THALES
Building a future we can all trust

How Thales accelerates NIS2 compliance

NIS2 Directive and beyond - Cybersecurity legislation in the EU

Ignacio BERROZPE
PreSales Manager

Thales Cloud Protection and Licensing
www.thalesgroup.com

DATA PROTECTION IS A QUESTION OF RESPONSIBILITY

Users need control to be accountable

"Digital sovereignty refers to the ability to
control your own digital destiny
– the data, hardware, and software
that you rely on and create."

World Economic Forum

Cloud adoption

Cloud SP

Responsibility
Security OF the cloud

Cloud Users

Responsibility
Security IN the cloud

… complexifies the question of responsibility

- **Impacts of Cloud Adoption:**

Cloud = somebody else computer

□ Loss of **direct control** (outsourcing)

□ Multinational **law enforcement**

The EU constantly adapts the compliance framework to take these new challenges into account

Data Protection compliance: multiple laws, recurrent patterns

- **Responsibility**
  - What industry/sector?
  - What asset/data?
  - Self + supply chain?

- **Assessment**
  - Risks vs Responsibility

- **Obligations**
  - Mitigation tools
    - Technical & organisational measures
  - Reporting
    - Supervisory, penalties

EU Data Protection legislation - Illustrations

GDPR

- Responsibility: personal data
- Assessment: Art 35; Art 30
- Mitigation: Art 24&32 (encryption, key management), Art 45/46& EDPB (transfer outside EU)

NIS2

- Responsibility : *Essential* and *Important* entities (multi-sectors, ICT)
- Assessment: cyber risk, supply chain risks
- Mitigation: Art 21 (encryption, cryptography, authentication)

DORA

- Responsibility: Financial Entities (banks, insurance, FS, ICT)
- Assessment: cyber risks, supply chain risks
- Mitigation: Art 9 (encryption, key management, authentication), Art 28 (supply chain contingency measures

Focus point: GDPR – General Data Protection Regulation

Published: 2016, Applicable: May 2018

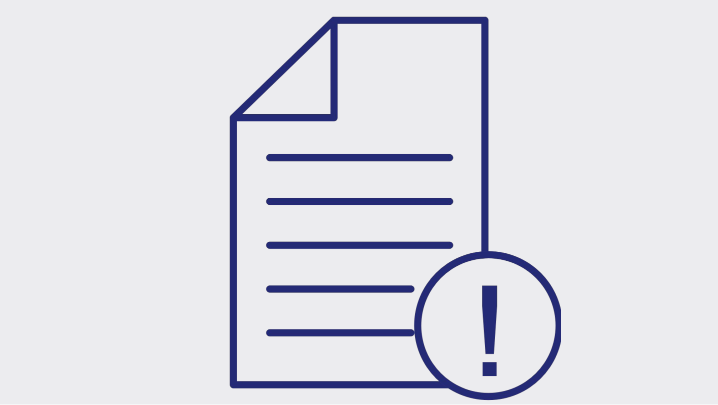
- **Scope & Responsibility**
  - Any organisations
  - Focus on the protection of personal data

- **Risk on cyber (Art 32)**
  - Organisations "shall implement appropriate technical and organisational measures including encryption of personal data;"
  - Personal data is protected by the "use of additional information [Keys], kept separately and subject to technical and organisational measures"

- **Risk on supply chain (EDPB recommendation 01/2020)**
  - "the personal data is processed using strong encryption"
  - "the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked)"
  - "the keys are retained solely under the control of the data exporter"

Data Privacy Framework

Applicable: 10 July 2023



What is DPF?

- A new legal instrument to transfer data to US or US International Organisations (EU, UK Extension, Swiss extension)
- Oct22: EO 14086 ("Enhanced Safeguards for US Signals Intelligence Activities")
- Jul23: adequacy for US DPF-certified sector (self-certified commercial organisations, for a given scope)

Residual issues

- EU Parliament, EDPB, NOYB: "Privacy Shield issues are not solved by DPF" + EO-based
- Self-certification and limited scope
  - DPF: only US specified scope
  - Not all US as a country, no other countries
  - Cloud SPs: only cover Service Data!

Impact of residual issues

- Uncertainty for businesses
- CJEU invalidation of DPF adequacy
- **CSP DPF: not for Customer Data**

Besides…

- Article32 not linked to data transfers
- DORA, NIS2: not linked to DPF

Focus point: DORA – Digital Operational Resilience Act

Published: 27 Dec 2022, Enforced: 16 Jan 2023, Applicable: 17 Jan 2025

Scope & Responsibility

- Financial entities
- Banks and payment services
- Insurance and pension services
- Trading and other FS services
- Supporting ICT service providers

Risk on cyber (Art 9)

- "Financial entities shall implement
  - strong **authentication** mechanisms
  - dedicated control system to protect **cryptographic keys** & **data encryption**
  - **data classification**"

Risk on supply chain (Art 28)

- "Financial entities shall put in place exit strategies.
  - "remove securely and integrally transfer data" [**cyber shredding**]
  - "shall have appropriate **contingency measures in place**"

THALES
Building a future we can all trust

Focus point: NIS2 – Network and Information Security

Published: 27 Dec 2022, Transposable: 17 Oct 2024.

- **Scope & Responsibility**
  - **Essential** and **Important** entities
  - Include organisations and their ICT supply chain/subcontractors

- **Obligations from NIS2**
  - Chapter II: Obligations on Member States
    - to adopt cyber strategies, authorities
  - Chapter III: Union level coordination
  - Chapter III & IV: Obligations on Regulated entities
    - Cybersecurity risk management: assessment, mitigation, reporting
    - Information sharing
  - Supervisory and enforcement

- **Cyber Risk measures (Art 21)**
  - Entities shall take technical, operational and organisational measures to manage risks including
    - **Supply chain**
    - **Cryptography, encryption**
    - **Access control, MFA**

NIS2 Directive and beyond
-Cybersecurity legislation in the EU

Synopsis

www.thalesgroup.com

NIS2, Network and Information Security, is a new Directive that lays down measures that aim to achieve a high common level of cybersecurity across the European Union.

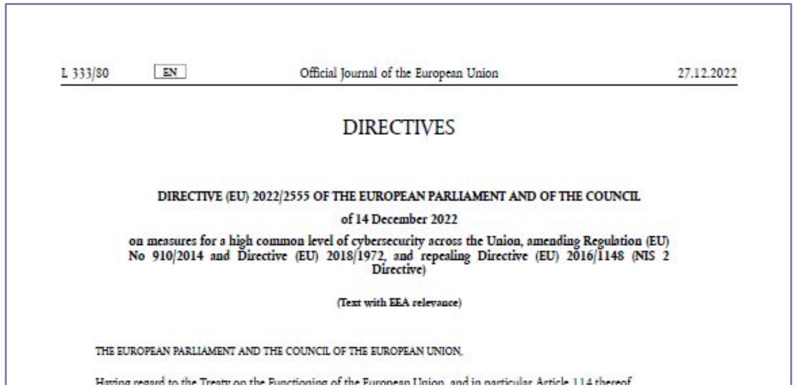
In this session, we will explore some of the obligations NIS2 defines for Member States and a large number of regulated sectors, and actionable strategies to reach compliance.

NIS2 – Network and Information Security Directive

- **Overall objective**

- "This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union."
- Decision is to improve the initial NIS adopted in 2016 (Directive 2016/1148)
- NIS2 is to be transposed by nation states by 17 Oct 2024 (NIS2, Article 41)

Source:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1693235799670



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

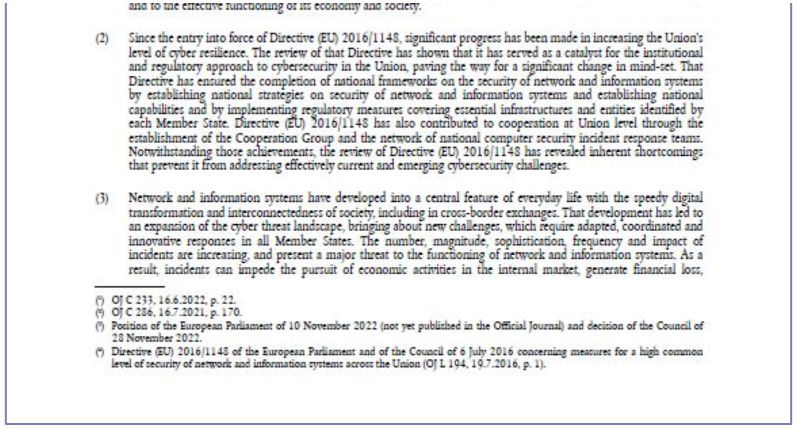
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on measures for a high common level of cybersecurity across the Union



and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

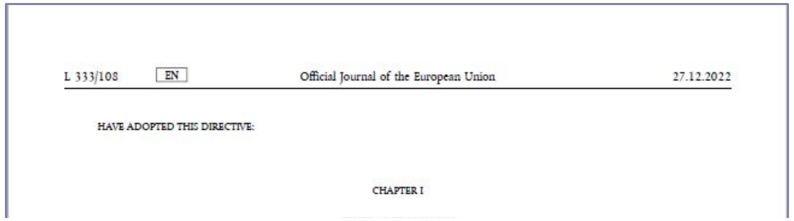
[1] OJ C 233, 16.6.2022, p. 22.
[2] OJ C 286, 16.7.2021, p. 170.
[3] Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.
[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

NIS2 – Subject Matter (Article 1)

- **"NIS2 Directive lays down**

- cybersecurity **risk management and reporting** obligations for regulated entities
  - **Article 21: mitigation**
  - **Article 23: reporting**

- supervisory and **enforcement obligations** on Member States"



L 333/108 EN Official Journal of the European Union 27.12.2022

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

Article 1
Subject matter

"This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market."

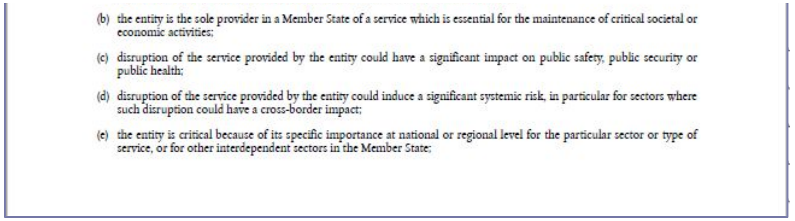
"2. To that end, this Directive lays down:

a) obligations that require **Member States** to adopt national cybersecurity strategies

b) **cybersecurity risk-management measures** and **reporting obligations for entities**;

c) rules and obligations on cybersecurity **information sharing**;

d) **supervisory and enforcement** obligations on Member States."



(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

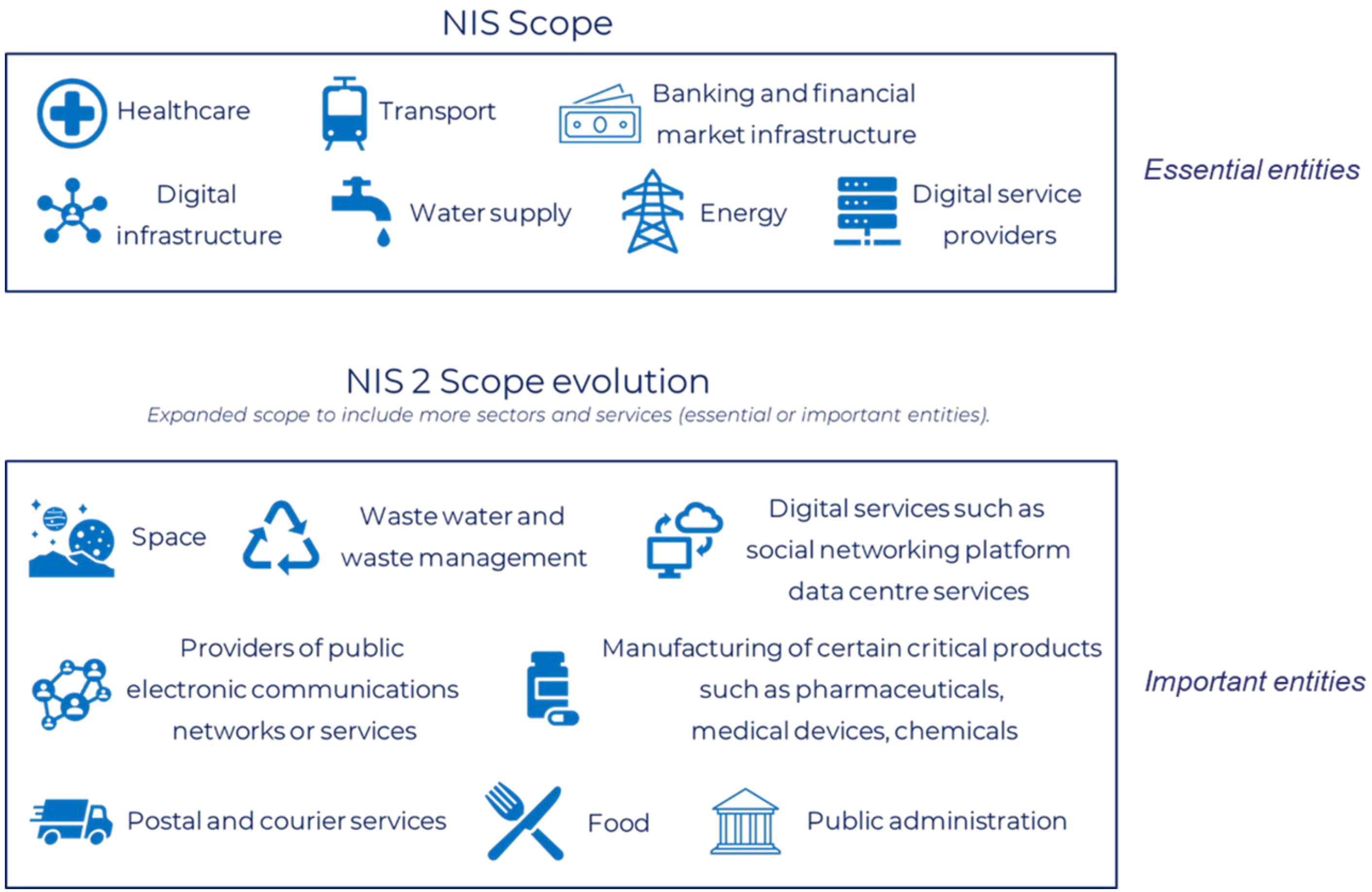
(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

NIS2 – Regulated Sectors (Article 2)

“NIS2 Directive lays down cybersecurity risk management and reporting obligations for **Essential Entities** and **Important Entities**”



NIS Scope

Healthcare

Transport

Banking and financial market infrastructure

Digital infrastructure

Water supply

Energy

Digital service providers

Essential entities

NIS 2 Scope evolution

Expanded scope to include more sectors and services (essential or important entities).

Space

Waste water and waste management

Digital services such as social networking platform data centre services

Providers of public electronic communications networks or services

Manufacturing of certain critical products such as pharmaceuticals, medical devices, chemicals

Postal and courier services

Food

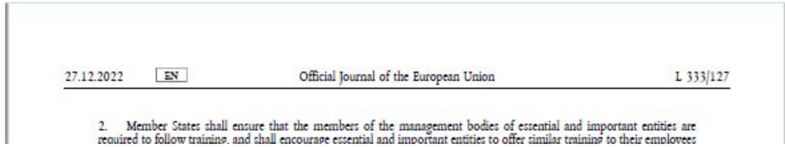
Public administration

Important entities

Cybersecurity measures (Article 21)

- **Risk-management measures mandated by NIS2**

- **Technical Measures**
  - **Cryptography, Encryption**
- **Organisational Measures**
  - **Supply chain risk mitigation: resilience vs 3rd party service providers**



27.12.2022 EN Official Journal of the European Union L 333/127

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees

Article 21
Cybersecurity risk-management measures

"Essential and Important Entities take appropriate and proportionate technical, operational and organisational measures to manage the risks"

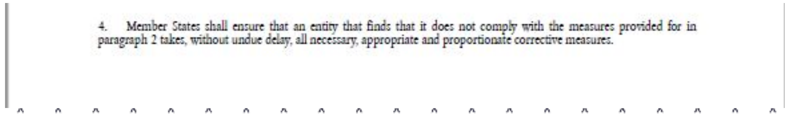
"Measures shall include at least:

d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

h) policies and procedures regarding the **use of cryptography** and, where appropriate, **encryption**;

i) human resources security, **access control policies** and **asset management**;

j) the use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate."



4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

Concept of Technical & Organisational Measures

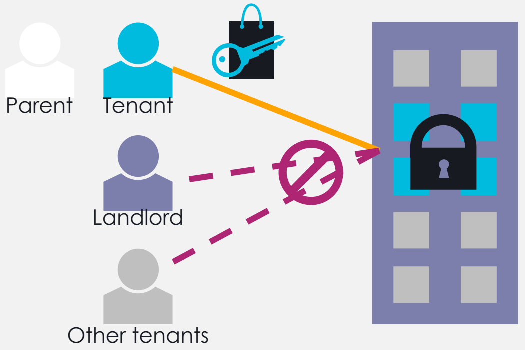
Physical world

Technical measures:

- Lock your apartment to refrain access from neighbours, landlord
- Keep your key in a purse, not on the door's lock!

Organisational measures:

- Keep the keys/purse with you
- Possibly share with a trusted relative



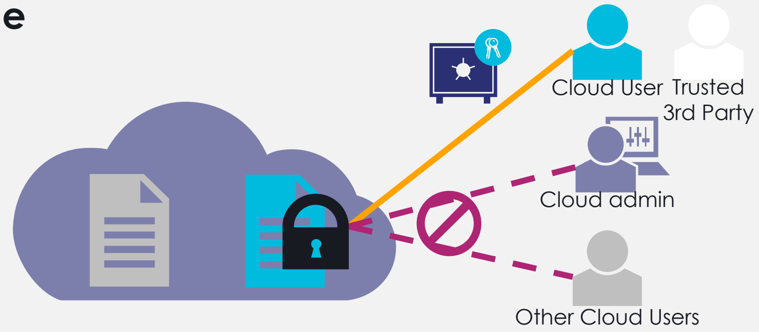
Digital space

Technical measures:

- Encrypt your data to refrain unauthorised access
- Put your key in a dedicated key management system, not on the data server

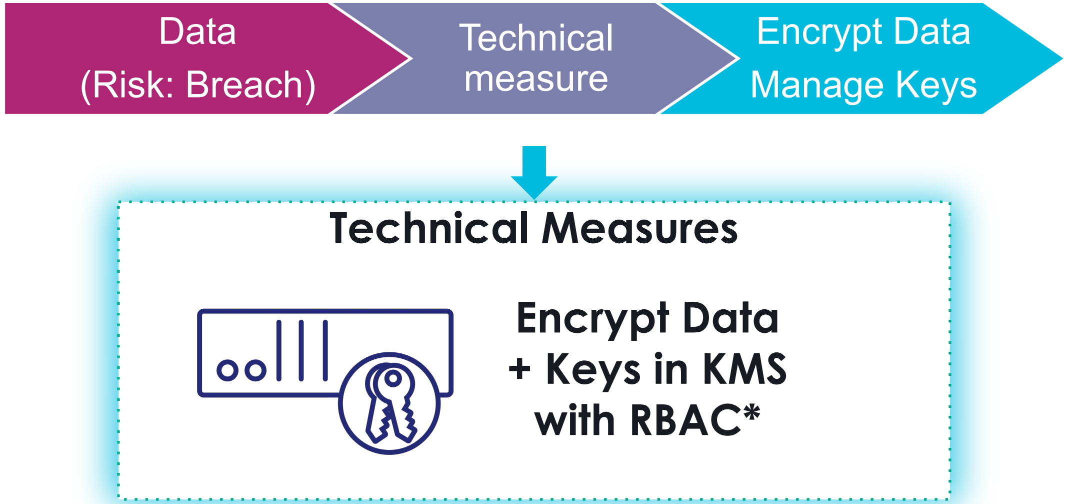
Organisational measures:

- Manage your own keys, bring your own KMS
- Possibly outsource to trusted security SP



Sovereign Control: Role of Encryption and Key Management

- Risk on cybersecurity

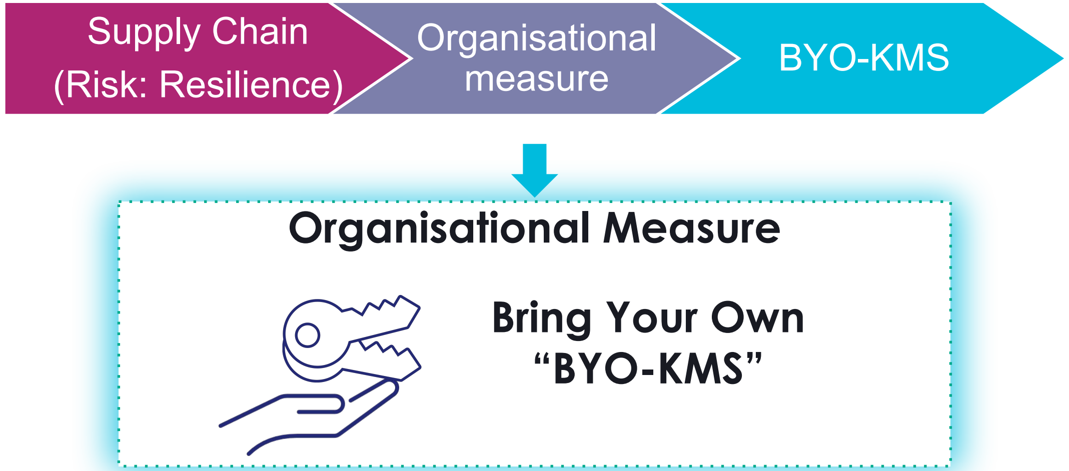


Data (Risk: Breach) → Technical measure → Encrypt Data Manage Keys

Technical Measures

Encrypt Data + Keys in KMS with RBAC*

- Risk on supply chain



Supply Chain (Risk: Resilience) → Organisational measure → BYO-KMS

Organisational Measure

Bring Your Own "BYO-KMS"

***KMS:** Key management System
RBAC: Role Based Access Control

What can Thales do for you? Technical Measures

What can Thales do for you?

Protect anything

- Big data
- Intellectual Property
- Financial data
- Enterprise data
- Identities of things
- Payments & digital transactions

Protect anywhere

- Applications
- Data centers
- Containers
- Networks
- Virtual
- Clouds

Delivered any way

- On-premises hardware or software
- Hybrid cloud & on-premises
- as-a-Service

What can Thales do for you? – Technical measures: data at rest

Secure sensitive data wherever it resides to meet compliance requirements with minimal disruption, effort and cost

Transparent Encryption

Encrypt data and define privileged user access controls without changes to infrastructure, applications or workflow

Live Data Transformation

Zero-downtime deployment and seamless key rotation

Advanced data protection solution integrations

Windows
aws
hadoop
Red Hat Enterprise Linux
SUSE
teradata.
ORACLE
Ubuntu
UNIX
Microsoft SQL Server
SAP HANA

…and more

What can Thales do for you? – Technical measures: databases

Protect sensitive information in databases across distributed systems

Database Protection

Transparently encrypt sensitive column-level data in databases

Application Key Management

ORACLE

Microsoft SQL Server

External key management for
Oracle TDE and
Microsoft SQL Server EKM

Batch Data Transformation

Protect vast quantities of data quickly

What can Thales do for you? – Technical measures: applications

Protect sensitive information in cloud native and legacy applications

Application Data Protection

Add data protection to applications using best in class encryption libraries

Application layer

Data Protection Gateway for REST

Add data protection to applications without modifying code

Network layer

RESTful Tokenization Service

Tokenize data using vaultless and vaulted solutions

Network layer

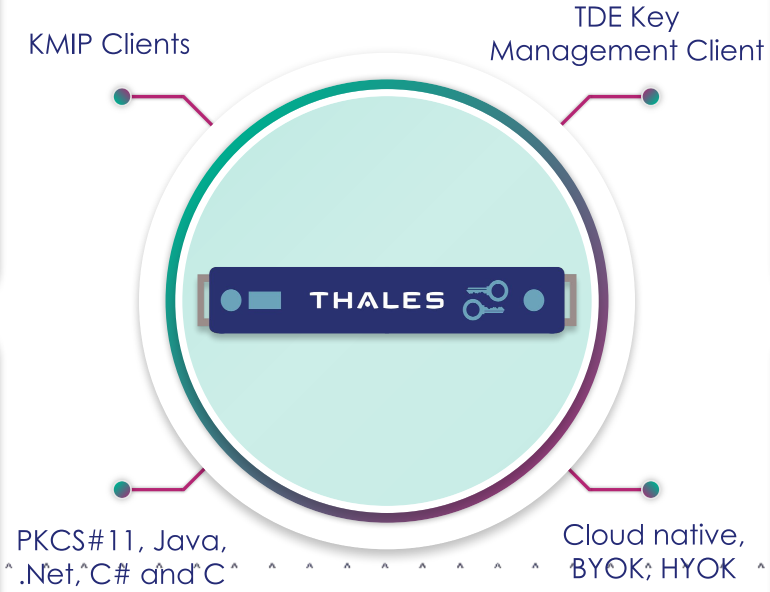
What can Thales do for you? Organisational Measures

What can Thales do for you? – Organisational measures: key management

Extensive partner integrations with leading enterprise storage, server, database, cloud and SaaS vendors

Data storage vendors, big data

PURESTORAGE
NUTANIX
vmware READY vSAN
mongoDB.
Hewlett Packard Enterprise
IBM.
DELLEMC
NetApp



Database (TDE) Key Management

ORACLE EXADATA
Microsoft SQL Server
ORACLE

Home-grown apps, web servers

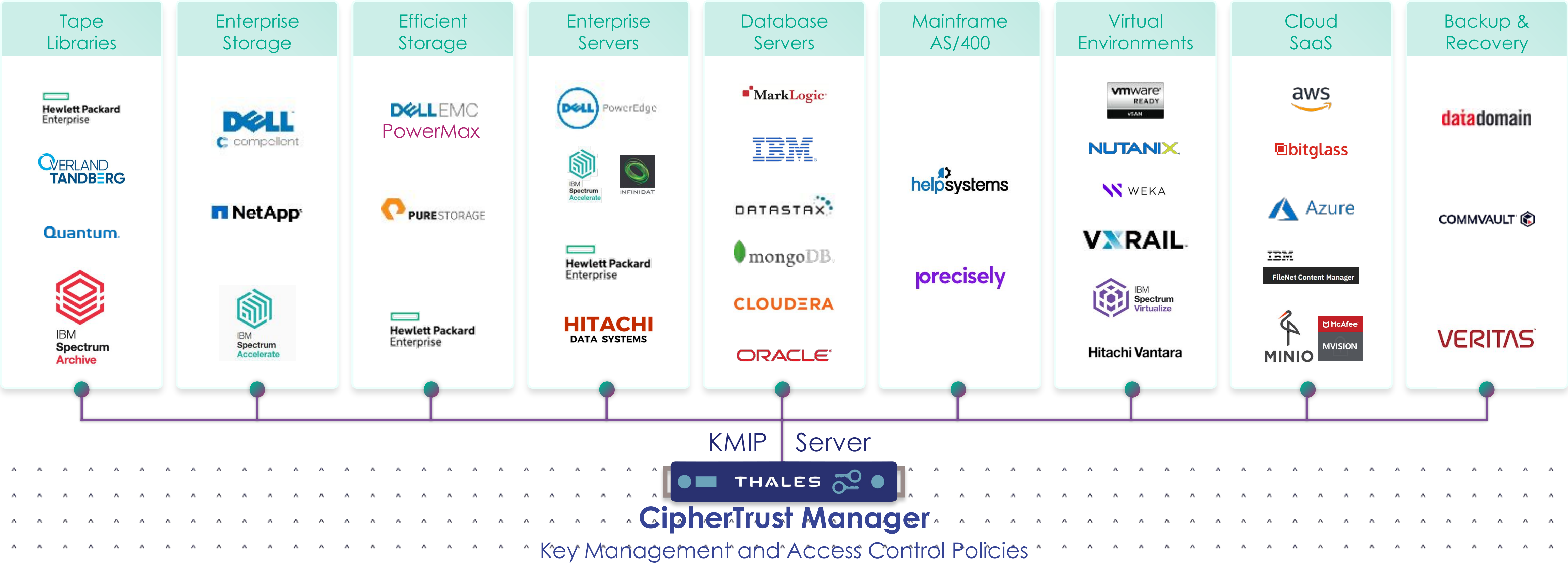
Microsoft
HashiCorp
NGINX
THE APACHE SOFTWARE FOUNDATION
ORACLE

Cloud Key Management

Azure
Microsoft 365
Google Cloud
Google Workspace
aws
ORACLE
SAP
salesforce

What can Thales do for you? – Org measures: key management KMIP

CipherTrust Manager works with a range of data storage, cloud/SaaS, and virtual environments using key management interoperability protocol (KMIP)



Tape Libraries
- Hewlett Packard Enterprise
- OVERLAND TANDBERG
- Quantum.
- IBM Spectrum Archive

Enterprise Storage
- DELL compellent
- NetApp
- IBM Spectrum Accelerate

Efficient Storage
- DELLEMC PowerMax
- PURESTORAGE
- Hewlett Packard Enterprise

Enterprise Servers
- DELL PowerEdge
- IBM Spectrum Accelerate
- INFINIDAT
- Hewlett Packard Enterprise
- HITACHI DATA SYSTEMS

Database Servers
- MarkLogic
- IBM
- DATASTAX
- mongoDB
- CLOUDERA
- ORACLE

Mainframe AS/400
- helpsystems
- precisely

Virtual Environments
- vmware READY vSAN
- NUTANIX
- WEKA
- VXRAIL
- IBM Spectrum Virtualize
- Hitachi Vantara

Cloud SaaS
- aws
- bitglass
- Azure
- IBM FileNet Content Manager
- MINIO
- McAfee MVISION

Backup & Recovery
- datadomain
- COMMVAULT
- VERITAS

KMIP | Server

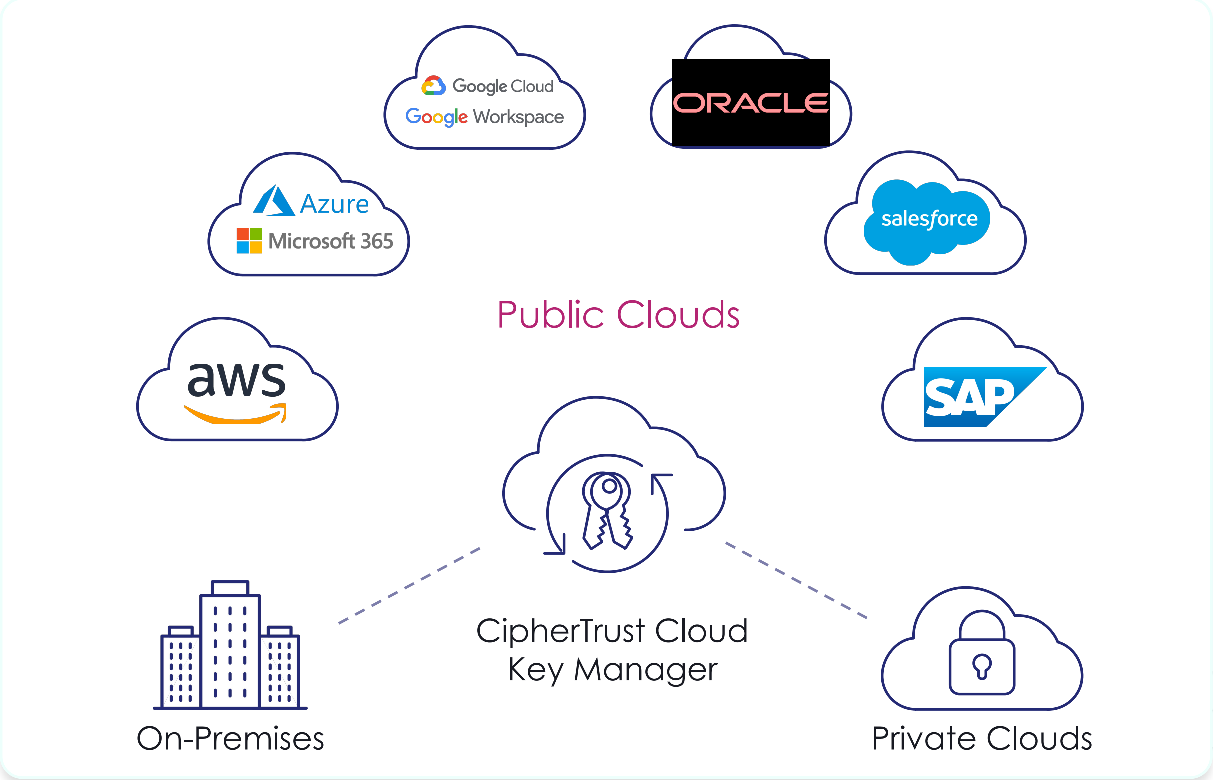
THALES

CipherTrust Manager

Key Management and Access Control Policies

What can Thales do for you? – Org measures: Cloud Key Management

Mitigate data security and privacy risks with separation of duty between your data and your cloud provider



Centralize multi cloud key management for BYOK, HYOK and cloud native encryption keys across any combination of clouds and on-premises with single UI

Increase efficiency with a single pane of glass view across regions, and automated key lifecycle management with a common set of APIs

Demonstrate compliance with data sovereignty laws and privacy regulations

What can Thales do for you? – Org measures: Secrets Management

Securing Secrets at Scale

CipherTrust Secrets Management*

Automate access to

- Secrets
- Credentials
- Certificates
- API keys
- Tokens

- Centralized management for all secret types
- Easy to use for DevSecOps
- SaaS (Software as a Service) scalability for hybrid and multi-cloud environments

Automate processes for

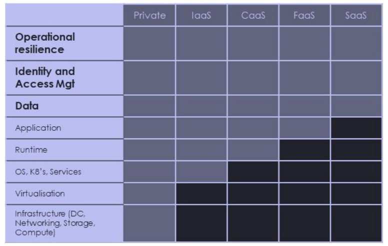
- Creating
- Storing
- Rotating
- removing

*Powered by Akeyless Vault

Conclusion

- Cloud adoption challenges the responsibilities of organisations, and comes with new risks (cyber, supply chain)
- Cloud security is not only about the security OF the cloud, but also the security IN the cloud
- Regulations and the state-of-the-art (IT Security) evolve to assess and mitigate these new risks
- Data encryption and multi-cloud key management are essential mitigation measures in an efficient cloud strategy

Governance



	Private	IaaS	CaaS	FaaS	SaaS
Operational resilience	▨	▨	▨	▨	▨
Identity and Access Mgt	▨	▨	▨	▨	▨
Data	▨	▨	▨	▨	▨
Application	▨	▨	▨	▨	■
Runtime	▨	▨	▨	■	■
OS, K8's, Services	▨	▨	■	■	■
Virtualisation	▨	■	■	■	■
Infrastructure (DC, Networking, Storage, Compute)	▨	■	■	■	■

Cyber risks

> Through 2025, more than **99 percent** of cloud breaches will have a root cause of a customer misconfiguration or mistake
>
> *Gartner, Outlook for Cloud Security*

Compliance

THALES
Building a future we can all trust

Cloud security
& sovereignty

Data protection
& security

DevSecOps &
application security

Thank You

Ignacio BERROZPE

Presales Manager

☎ +31 6 1552 1632

✉ Ignacio.berrozpe@ThalesGroup.com

THALES
Building a future we can all trust
= new options for
multi-clouds
Data Control

aws
salesforce
SAP
ORACLE

NIS2 – Regulated Sectors (Article 2)

- **Essential entities**
- **“digital infrastructure; ICT SPs”**

- Internet Exchange Point providers
- DNS service providers, excl root name servers
- TLD name registries
- *Cloud computing service providers*
- *Data centre service providers*
- *Content delivery network providers*
- *Trust service providers*
- *Providers of public electronic comm networks*
- *Providers of publicly available electronic communications services*

- ***Important entities***
- **“digital providers”**

- Providers of online marketplaces
- Providers of online search engines
- Providers of social networking services platforms

Italic: new from NIS1