THALES
Building a future we can all trust

DORA drives DataSec

MARKUS HOFBAUER
Sales Engineer Manager

www.thalesgroup.com

Martin Gegenleitner

Pre-Sales Consultant

Digital Operational Resilience Act (DORA) Compliance

EUROPEAN UNION

THE EUROPEAN PARLIAMENT — THE COUNCIL

Brussels, 17 November 2022
(OR. en)

2020/0266(COD) — PE-CONS 41/22

Regulation of the European Parliament and council on digital operational resilience for the financial sector

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

PE-CONS 41/22 — MCA

ECOFIN — EN

Overall objective

The European Union's Digital Operational Resilience Act sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services. The DORA regulation was adopted on December 14, 2022, and will be enforced starting on January 17, 2025.

Applies to

Financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, payment processing, or insurance, and critical third parties, such as cloud platforms or data analytics services.

Penalties

Member States are granted discretion on penalties of up to EUR 10M or 2% of total worldwide turnover for the company that violates the law (whichever is higher).

Article 6 – Encryption and cryptographic controls (1/3)

1

As part of their ICT security policies, financial entities shall develop, document and implement a policy on encryption and cryptographic controls, with a view to preserve the availability, authenticity, integrity and confidentiality of data.

2

a)

Rules for the encryption of data at rest and in transit.

b)

Rules for the encryption of data in use, where necessary. Where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment or take other equivalent measures that ensure the confidentiality, integrity, authenticity and availability of data.

c)

Rules for the encryption of internal network connections and traffic with external parties.

d)

Provisions for cryptographic key management establishing the correct use, protection, and lifecycle of cryptographic keys in accordance with Article 7.

Source: JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

Article 6 – Encryption and cryptographic controls (2/3)

3

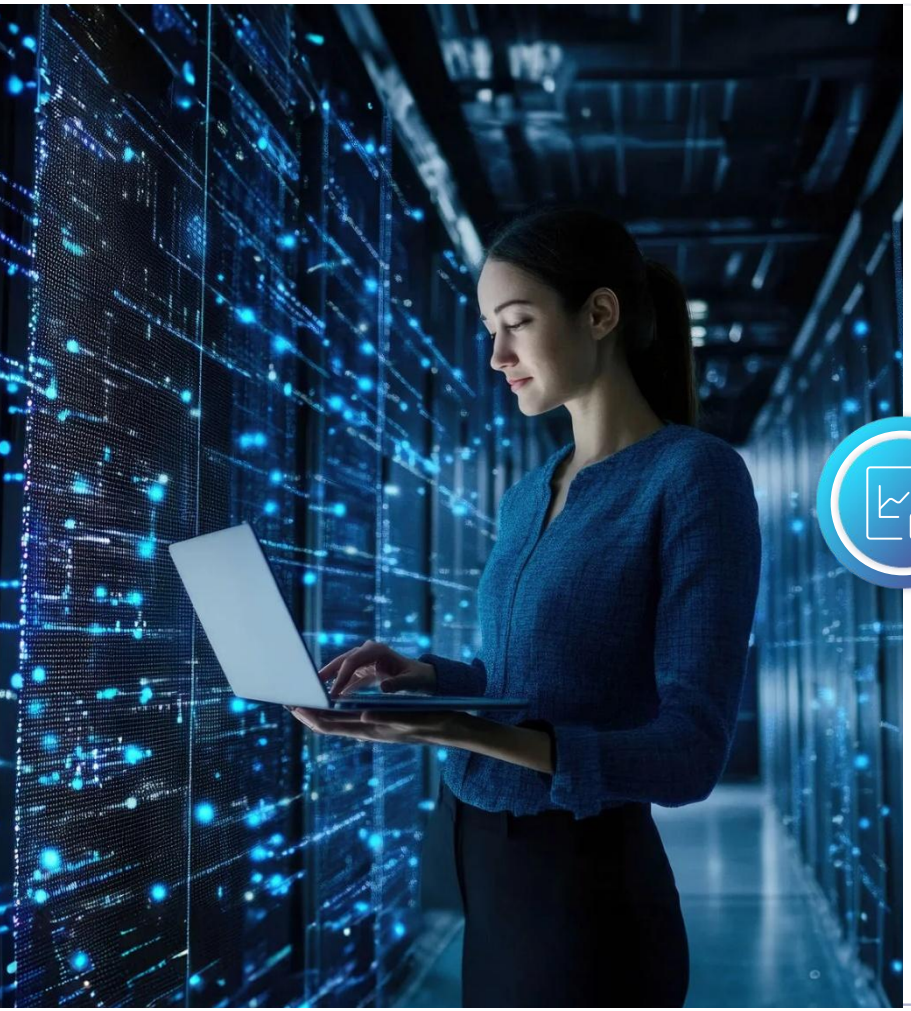
Financial entities shall include in the policy on encryption and cryptographic controls criteria to **select cryptographic techniques and use practices taking into account leading practices and standards**, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets established according to Article 8(1) of Regulation (EU) 2022/2554. Where the financial entity cannot adhere to the leading practices or use the most reliable techniques, it shall adopt mitigation and monitoring measures to ensure resiliency against cyber threats.

4

Financial entities shall include in the policy on encryption and cryptographic controls provisions to, where necessary, **on the basis of developments in cryptanalysis, update or change the cryptographic technology** to ensure they remain resilient against cyber threats and considering the information resources referred to in Article 10(2), point (a). Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats.

Source: JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

Article 6 – Encryption and cryptographic controls (3/3)



5

Financial entities shall include a requirement in the policy on encryption and cryptographic controls to **record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4** and to provide a reasoned explanation for doing so.

Source: JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

Article 7 – Cryptographic key management (1/2)

1

Financial entities shall lay out in the provisions on cryptographic key management referred to in Article 6(2) point (d), the requirements for managing cryptographic **keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys.**

2

Financial entities shall identify and **implement controls to protect cryptographic keys through their whole lifecycle** against loss, unauthorised access, disclosure and modification. The controls shall be designed taking into account the results of the approved data classification and the ICT risk assessment processes.

Source: JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

Article 7 – Cryptographic key management (2/2)

3

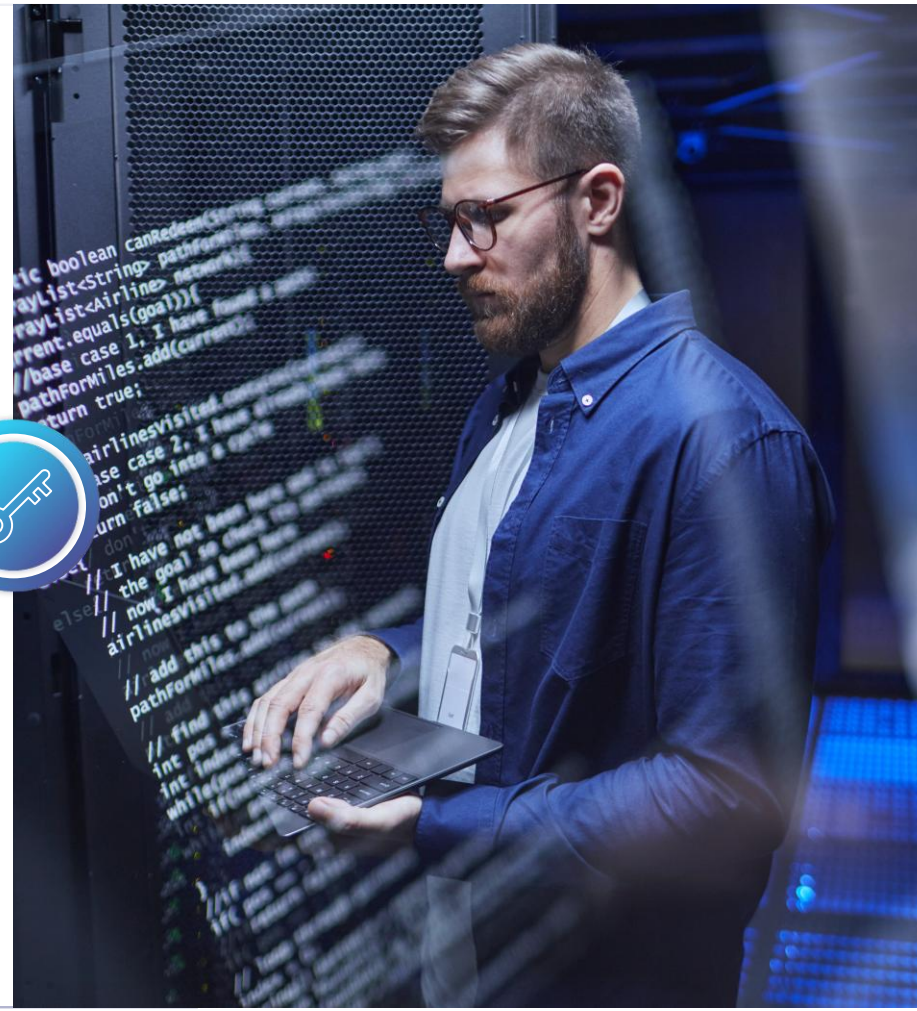
Financial entities shall develop and implement methods to **replace the cryptographic keys** in the case of lost, compromised or damaged keys.

4

Financial entities shall create and **maintain a register for all certificates and certificate storing devices** for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date.

5

Financial entities shall ensure the **prompt renewal of certificates in advance** of their expiration.

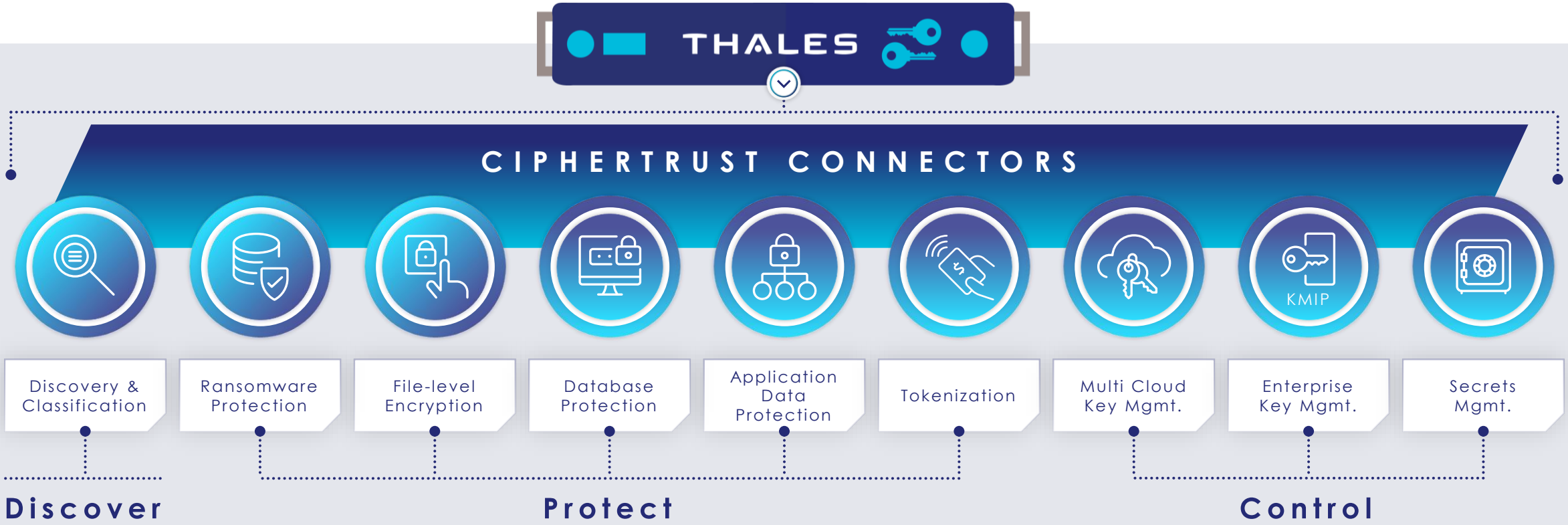


Source: JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework.pdf (europa.eu)

CipherTrust Data Security Platform

CipherTrust Manager

Key Management and Policies



Protect your sensitive data wherever it resides

Where

Protection Layer

- Network
- Application
- Database
- File System

How

CipherTrust Connectors

Data Protection Gateway for REST	Tokenization (Vaultless & Vaulted)	
Application Data Protection (SDKs)		
Database Protection	Application Key Management (for native TDE)	Batch Data Transformation
Transparent Encryption with Live Data Transformation	Transparent Encryption solutions for: - Amazon S3 - SAP HANA - Kubernetes - Teradata	

Solutions for each layer of the technology stack to match your security requirements and infrastructure.

CORE MESSAGE #1

You need to take care of crypto and encryption!

Customer success story #1 – Landing @ Insurance

Goal: Adjust InfoSec measures to fulfil DORA requirements

Gaps @ encryption and key management

CipherTrust to the rescue!

2-phased deployment in multiple European countries

Mix of virtual and physical appliances for resilience

Encryption targets

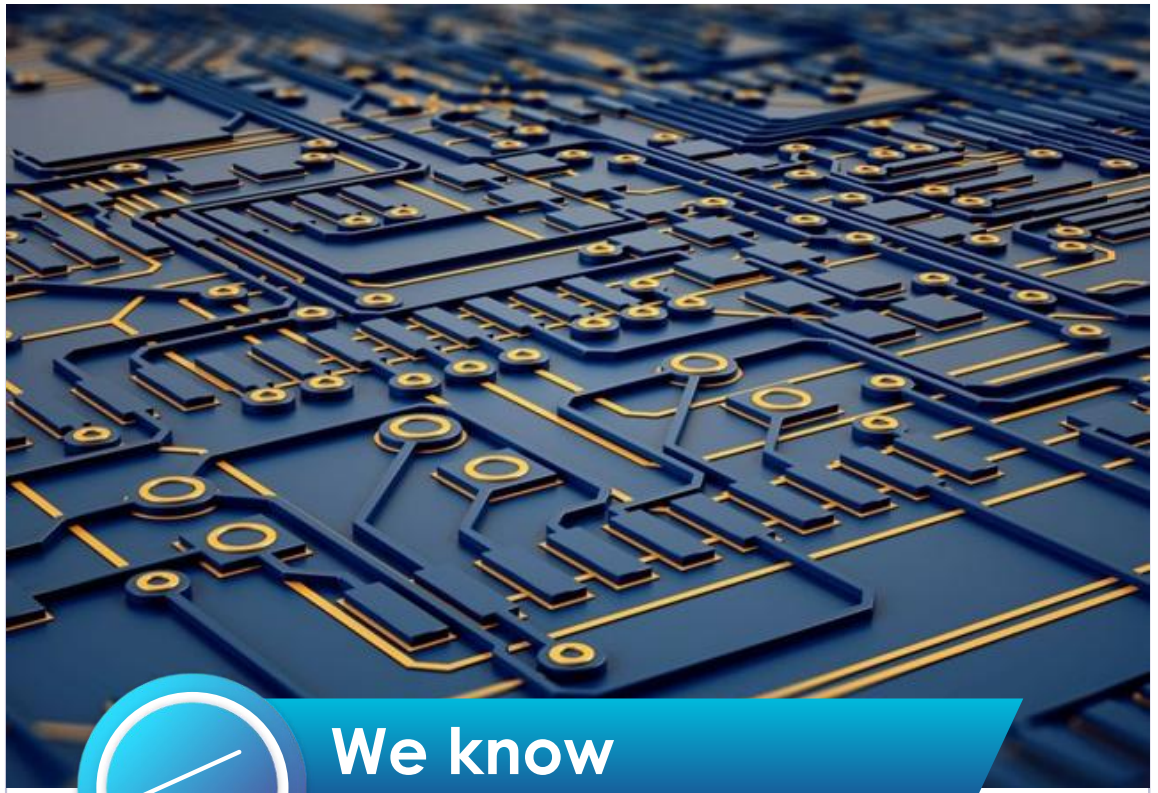
Databases

File servers

KMIP consumers

Teamwork makes the dream work!

Partner knows the customer



We know our products

Customer success story #2 – Expanding @ Banking

DORA as an additional driver for a resilience focused IT architecture redesign

Remove dependencies (especially on the network) = use physical appliances with built-in HSMs

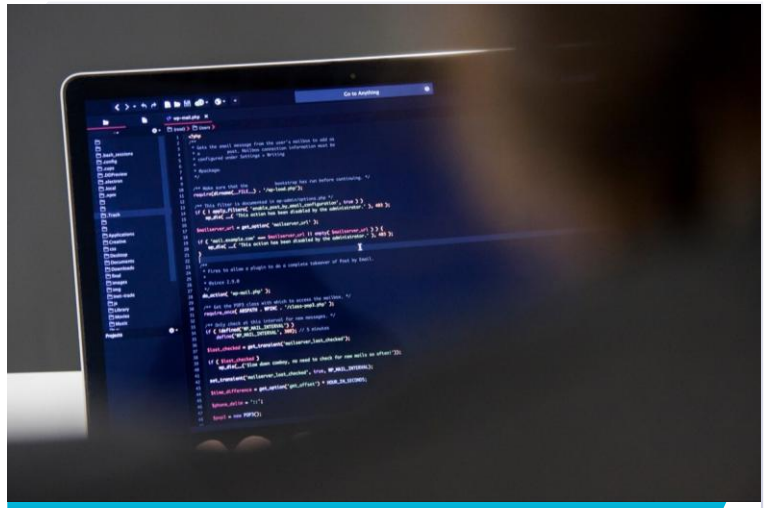
Provide CipherTrust Platform as an internal managed service

What did we sell?

Customer already runs on an Enterprise License Agreement

Existing service was used until this year exclusively by a single internal customer

Need for more CipherTrust clusters to separate their crypto consumers



Why CipherTrust?

Automation, automation, automation

Team size = 2,5 FTE to run 3 clusters with more than 600 installed connectors (and also other things like PKI, PAM, …)

Challenges solved with partner

Physical appliances providing services to multiple (35) VLANs

Partner provides networking know-how

Ensure fall back routines in case of (network) outages

We provide best practices

Ensure events are logged and monitored in an effective manner

Partner provides experience from other customers and also from other vendor solutions

Partner supports maintenance and operation of the internal service

CORE MESSAGE #2

We need you


THALES
Building a future we can all trust
Thank you
www.thalesgroup.com