cryptas

we establish trust.

Digital Operational Resilience Act DORA

HOW **CRYPTAS** CAN HELP YOU TO COMPLY WITH **REGULATION (EU) 2022/2554**.

WHAT IS DORA?

The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, addresses ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system.

Structure of the Regulation

As a "Regulation" it is immediately effective to all financial entities with the EU, without the need for an implementing act by the individual member states. On 17 January 2025, DORA will become effective. While the Regulation itself is stating the objectives and requirements on a rather abstract level, certain aspects have been further detailed in a Regulatory Technical Standards (RTS), which is available in its final draft from January 2025.

WHO IS AFFECTED?

DORA covers a wide array of financial service providers such as banks, credit institutions, payment institutions, e-money institutions, insurance companies, investment firms, and crypto-asset service providers, among others. Significantly, DORA delineates crucial ICT services offered to financial institutions. Should an entity provide critical ICT services to a financial institution, it will fall under direct regulatory supervision as outlined in the DORA framework. This encompasses services like cloud platforms and data analytics.

Entities found to be in violation of the Act's requirements could be subjected to fines up to 2% of their total annual worldwide revenue or, for individuals, a maximum fine of EUR 1,000,000.

This document connects the requirements of the DORA regulation and the related Regulatory Technical Standard to the contributions that CRYPTAS is able to provide to the affected financial entities, to meet such requirements.

HOW TO APPROACH THE CHALLENGE?

Financial institutions are **faced with a host of rules to comply with DORA**. Although data security and cryptography related topics are only a small portion of the overall DORA requirements, they are **still affecting all processes throughout the entire business**.

A holistic approach is advisable, by **providing corporate trust services** centrally to all organization units and to all business processes.

CRYPTAS provides assistance in **designing, implementing and operating** such **corporate trust services**.

Chapter	REQUIREMENT	CRYPTAS CONTRIBUTION
DORA ARTICLE 9 "PROTECTION AND PREVENTION"		
Art 9.4 (a)	*develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable*	Consulting and assistance in developing and documenting such policies and rules.
Art 9.4 (c)	*implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;*	Egofy converged Smartcard solution, with Legic and Mifare Desfire for physical access, combined with X.509 certificates, FIDO-2 and OTP for logical Multi-factor authentication. Intercede MyID for administration of policies and access rights.
Art 9.4 (d)	*implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys*	Authentication solution, including PKI and Credential Management systems
Art 15	*Further harmonisation of ICT risk management tools, methods, processes and policies*	see contributions relating to Draft RTS 2024-01/JC 2023 86 (below)
DRAFT RTS 2024-01/JC 2023 86 – ARTICLE 6 "ENCRYPTION AND CRYPTOGRAPHIC CONTROLS"		
Art 6.1	*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.*	Consulting on best practices, proportionate policies and implementation architecture. CRYPTAS also supports documenting and implementation of such policies.
Art 6.2 (a)	*rules for the encryption of data at rest and in transit;*	360° encryption solution (file & folder, volume encryption, transparent database encryption, cloud data encryption), e.g. Thales CiphterTrust Data Security Platform, Utimaco LANCrypt. The use of SMIME email encryption must also be discussed
Art 6.2 (c)	*rules for the encryption of internal network connections and traffic with external parties*	Solutions using SSL/TLS certificates. Internal connections and traffic protected through Enterprise PKI, e.g. Keyfactor EJBCA, Entrust Certificate Manager, MTG CARA, Cryptas primeID PKIaaS. An enterprise PKI always relies on an HSM solution to protect the keys. External traffic is protected with public trust certificates. Certificate Lifecycle Management becomes an important tool to manage this requirement
Art 6.2 (d) and Art 7.1	*provisions for cryptographic key management ...* *... managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys*	Enterprise Key Management solution, e.g. Thales CipherTrust Manager, Entrust KeyControl, MTG KMS. PKI and CLM for managing the lifecycle of certificates and related keys. An HSM solution is needed to secure the keys.

Chapter	REQUIREMENT	CRYPTAS CONTRIBUTION
DRAFT RTS 2024-01/JC 2023 86 – ARTICLE 7 "CRYPTOGRAPHIC KEY MANAGEMENT"		
Art 7.2 and Art 7.3	*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. Financial entities shall develop and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys*	Documented key management policies, to be implemented in each of the key-consuming ICT systems, and with the help of an Enterprise Key Management solution. An HSM solution is needed to secure the keys.
Art 7.4 and Art 7.5	*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. Financial entities shall ensure the prompt renewal of certificates in advance of their expiration.*	Certificate discovery. Certificate lifecycle management solution, e.g. Keyfactor Command, Entrust Certificate Hub, libC SwissPKI, MTG CLM, Cryptas primeID DISCOVER
DRAFT RTS 2024-01/JC 2023 86 – ARTICLE 8 "POLICIES AND PROCEDURES FOR ICT OPERATIONS"		
Art 8	*Policies and Procedures for ICT Operations, including:* - *Secure installation, maintenance* - *Backup-Restore* - *Audit trail , system log* - *Separation of production from dev + test* - *Support and escalation contacts* - *System restart, roll-back, recovery*	CRYPTAS supplied solutions and CRYPTAS managed services have been built, operated, and documented to the principles of Art 8 already before DORA was put in place