Ensuring Operational Resilience:

A Guide to Securing Data in Transit for DORA Compliance

As cybersecurity risks and threats continue to evolve, the financial sector is just one of many industries that remain a key target for cybercriminals looking to exploit vulnerabilities. To address these challenges head-on, the European Union's Digital Operational Resilience Act (DORA) aims to improve the resilience of financial organisations against these threats. Set to come into effect in January 2025, the new regulation addresses multiple elements of digital resilience, including protecting data in transit.

This whitepaper outlines the importance of safeguarding data in transit, explains how it fits into the broader objectives of DORA, and offers practical strategies for financial institutions to ensure compliance.

With a focus on technologies like Certes DPRM, this paper highlights how organizations can secure their data flows, mitigate third-party risks, and build a more resilient digital infrastructure.

> **Protecting data in transit is no longer a best practice—it's a regulatory mandate that directly impacts business continuity and customer trust.**
>
> *Paul German– CEO, Certes*

The Impact of DORA on Financial Institutions

The introduction of DORA's regulatory framework requires financial institutions to confidently withstand and recover from IT disruption like cyberattacks. From banks to investment firms, insurers and payment providers, financial entities that operate in the EU will need to comply with regulations to strengthen their operational resilience and ensure financial stability is not affected by cyber attacks.

As with other regulations, the penalties for non-compliance include substantial fines of up to 2% of annual turnover, temporary business shutdowns, and legal action. But ultimately, the most significant consequence is increased vulnerability to cyberattacks. Without the necessary security precautions in place, financial institutions are exposing themselves to the risk of data breaches and financial fraud, leading to loss of business, reputation, and trust.

What are the Key Components of DORA?

Risk Management: Institutions must identify potential cyber risks and establish systems to manage those risks. This involves not just identifying threats but also implementing controls to safeguard critical systems and data.

Incident Reporting: Organizations must report major cyber incidents to the appropriate regulatory authorities. This ensures that incidents are tracked and addressed quickly, preventing large-scale impacts.

Third-Party Risk Management: Given that many financial institutions rely on third-party services, DORA requires strict oversight of these external vendors, ensuring they meet the same resilience standards.

Testing and Audits: Regular testing, such as penetration testing, is required to ensure that cybersecurity measures remain effective over time, even as threats evolve.

A significant part of achieving compliance with DORA is ensuring that data in transit remains secure, minimizing the risk of data breaches and cyberattacks during its transmission.

Why is Securing Data in Transit Essential for DORA Compliance?

Securing data in transit means safeguarding sensitive information as it moves through networks and between systems. For financial institutions, this can include anything from internal data exchanges to external transfers with clients and third-party partners. Data in transit is especially vulnerable to interception, as it travels across potentially unsecured or less-controlled networks, which makes it a primary target for attacks.

> **The financial sector's heavy reliance on third-party services creates additional vulnerabilities. DORA's focus on third-party risk management underscores the need for institutions to have strict protocols for data in transit, reducing potential weak points in the digital supply chain.**
>
> *Simon Pamplin – CTO, Certes*

Protecting Confidentiality of Financial Data

Financial data often includes personally identifiable information (PII), account details, and transaction data. DORA states that this data should remain confidential during transit to protect consumers' privacy and trust. Data protection ensures that even if data is intercepted, it cannot be easily read or exploited.

Mitigating Risks of Man-in-the-Middle (MITM) Attacks:

MITM attacks exploit vulnerabilities during data transmission by intercepting and potentially altering the information exchanged between two parties. In financial settings, MITM attacks could lead to unauthorized access or data manipulation. Certes DPRM reduces these risks through frequent key rotation and advanced encryption to render intercepted data unreadable.

Certes DPRM offers advanced key management, changing encryption keys hourly to reduce the risks of interception. Even if data is intercepted, it cannot be read or manipulated by unauthorised users.

Addressing Third-Party Risks

Financial institutions often integrate third-party services, such as cloud providers, payment processors, and data storage solutions, which can introduce additional vulnerabilities. DORA mandates that institutions conduct due diligence on third-party service providers, ensuring they adhere to the same resilience standards.

- **Secure API Gateways:** Secure APIs ensure that data exchanged between the institution and third parties is encrypted and authenticated. Certes DPRM supports encryption over APIs, ensuring secure connections between internal systems and external partners.
- **Zero Trust Network Access:** Implementing a Zero Trust model means no user or device is trusted by default, even those inside the network. Access is granted based on verification, ensuring that only authorized parties can access data.

> **Data in transit is a prime target for interception, especially during transmission across unsecured networks. Solutions like Certes DPRM, with advanced encryption and automated key management, fortify data as it travels, aligning with DORA's emphasis on secure communications.**
>
> *Simon Pamplin – CTO, Certes*

Maintaining Regulatory Compliance

DORA's requirements align with other regulations such as GDPR, MiFID II, and PSD2, which emphasize data protection during transmission. A unified approach to data protection and monitoring not only ensures DORA compliance but also simplifies adherence to other regulatory standards.

- **Encryption-at-Rest and In-Transit:** While DORA emphasizes data in transit, it's equally important to ensure that data is protected when at rest (stored data). Combining protection for both helps ensure complete data security.
- **Incident Response Plans:** Institutions must have incident response protocols that include specific steps for handling breaches related to data in transit. This can include rapid key revocation and enhanced monitoring during incidents.

How to Secure Data in Transit to Meet DORA Requirements

Financial institutions must deploy specific measures to secure their data in transit, ensuring compliance with DORA's expectations. Financial institutions should adopt the following best practices for securing data in transit:

Implement Advanced Encryption Techniques: Encryption remains the first line of defense in securing data in transit. Certes DPRM applies robust, quantum-safe encryption protocols, protecting each data flow individually. The hourly rotation of encryption keys further mitigates the risk of unauthorized decryption.

End-to-End Encryption (E2EE): Certes DPRM supports E2EE by ensuring data protection from source to destination, even across physical, virtual, or cloud-based infrastructure. This comprehensive data protection ensures data is secure from one endpoint to another, regardless of the transmission medium.

Real-Time Monitoring and Data Flow Recording: Continuous monitoring helps detect and respond to anomalous activity during data transmission. Certes DPRM provides real-time visibility into data flows, allowing financial institutions to respond proactively to threats and maintain compliance.

Adopt Secure Data-Sharing Protocols with Third Parties: Since many financial institutions rely on external vendors, adopting secure data-sharing protocols is essential. Certes DPRM provides a Zero Trust architecture for data in transit, where only authenticated parties can access data, minimizing the risks of unauthorized access through third parties.

CERTES

How Certes DPRM Supports DORA Compliance

Certes Data Protection and Risk Mitigation (DPRM) is a comprehensive solution for securing data in transit, with granular security controls enabling financial institutions to comply with the demands of DORA.

Key features include:

- **Granular Data Flow Security:** DPRM's granular security controls allow financial institutions to apply tailored data protection and access protocols, addressing DORA's strict requirements for data security.

- **Automated Key Management:** Certes DPRM automates key rotation hourly, reducing the chance of decryption by unauthorized parties and enhancing data protection during transmission.

- **Zero Trust Data Access:** Certes implements a Zero Trust model, ensuring that every access request is authenticated and verified, supporting DORA's mandates on stringent access control and third-party risk management.

- **Continuous Monitoring and Threat Detection:** With real-time monitoring, DPRM alerts institutions to any anomalies, helping to prevent and respond to potential incidents in line with DORA's incident response requirements.

- **Secure APIs and Data Transmission Protocols:** Secure API management and encryption over data-sharing protocols minimize vulnerabilities when interacting with third parties, in compliance with DORA's guidelines for managing third-party risks.

Building a Resilient Data Protection Strategy for DORA Compliance

With the implementation of DORA on the horizon, protecting data in transit must be a priority for financial organisations. By adopting advanced data protection, ensuring secure communication with third parties, and leveraging solutions like Certes DPRM, organizations can secure their sensitive financial data, and comply with regulations. Certes is committed to helping financial institutions navigate these challenges, offering tools and expertise that make achieving DORA compliance straightforward and effective.

For financial institutions operating within the EU, now is the time to assess your data protection strategies and prioritize securing data in transit as a key component of your DORA compliance efforts.

> **"Ensuring the confidentiality of financial data in transit is essential to meet DORA's compliance standards. Implementing end-to-end encryption and Zero Trust models not only protect sensitive information but also solidify customer confidence in an increasingly cyber-threatened landscape."**
>
> *Simon Pamplin – CTO, Certes*

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai