SCIOPTA Middleware - CRA Compliance Overview

Abstract

This document is the **CRA Compliance Overview** for Sciopta Middleware.

Copyright

Copyright © 2026 by SCIOPTA Systems GmbH. All rights reserved. No part of this publication may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, optical, chemical or otherwise, without the prior written permission of SCIOPTA Systems GmbH. The Software described in this document is licensed under a software license agreement and maybe used only in accordance with the terms of this agreement.

Disclaimer

SCIOPTA Systems GmbH makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, SCIOPTA Systems GmbH reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Trademark

SCIOPTA is a registered trademark of SCIOPTA Systems GmbH.

Contact

Corporate Headquarters
SCIOPTA Systems GmbH
Hauptstrasse 293
79576 Weil am Rhein
Germany
Tel. +49 7621 940 919 0
Fax +49 7621 940 919 19
email: sales@sciopta.com
www.sciopta.com

Contents

Sciopta Middleware – CRA Compliance Overview . . . 1
1 Introduction . . . 1
2 Product Classification Impact . . . 1
3 CRA Requirements Summary . . . 2
4 How Sciopta Middleware Supports CRA Requirements . . . 2
4.1 Secure-by-Design Architecture . . . 2
4.2 Data Handling & Communication . . . 2
4.3 Secure Delivery, Integrity & Authenticity (via Sciopta Kernel) . . . 2
4.4 Resilience & Fault Containment . . . 2
4.5 Lifecycle Management . . . 3
4.6 Documentation and Compliance . . . 3
4.7 User Information & Guidance . . . 3
4.8 Certification & Assurance . . . 3
5 Summary Table – CRA Requirements vs Sciopta Middleware Features . . . 4
6 Conclusion . . . 4

Sciopta Middleware – CRA Compliance Overview

1 Introduction

The **EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847)** establishes mandatory cybersecurity requirements for products with digital elements.

Sciopta Middleware provides a **modular, safety-oriented software layer** that runs on the **Sciopta Kernel**, certified or non-certified. It includes network protocols, file systems, USB support, distributed messaging, and APIs, enabling **secure, predictable, and controlled communication between applications and system components**.

Sciopta Middleware is built to operate on the **Sciopta Kernel**, which provides a **secure execution foundation** aligned with CRA principles.

By providing **documented, modular middleware components and well-defined integration interfaces**, Sciopta Middleware supports manufacturers in **implementing CRA-aligned software architectures and reducing integration effort and compliance risk**.

2 Product Classification Impact

IMPORTANT	The CRA classifies **final products**, not individual components (Article 7). Sciopta provides a **software component** (the Kernel). It does not determine the classification of the integrator's final product.

A device using Sciopta components is classified based on its **core functionality** (e.g., making coffee, controlling a motor, securing a network), not on the presence of an RTOS or middleware.

Product Type	Core Functionality	Likely CRA Classification	Integrator's Conformity Path
Medical infusion pump	Delivering medication safely	Default	Module A (Self-assessment)
Industrial motor controller	Controlling a motor	Default	Module A (Self-assessment)
Network firewall appliance	Network security	Important (Class II)	Module B+C or H (Third-party)
Smart meter with remote shut-off	Energy metering and control	Critical	EUCC or Module B+C+H

Integrators remain fully responsible for determining their final product's classification and completing the appropriate conformity assessment. Sciopta's documentation supports all paths.

3 CRA Requirements Summary

Requirement Category	Description
Secure-by-Design Architecture	Components must minimize attack surfaces and follow secure design principles.
Data Handling & Communication	Messages and modules must behave predictably and avoid corruption.
Secure Delivery, Integrity & Authenticity	Updates must be delivered securely, with authenticity and integrity guarantees.
Vulnerability & Lifecycle Handling	Security issues must be tracked and mitigated throughout the lifecycle.
Documentation & Conformity Assessment	Technical documentation, risk assessment, and integration guides must be maintained.
User Information & Guidance	Instructions for installation, configuration, and safe operation must be clear.

4 How Sciopta Middleware Supports CRA Requirements

4.1 Secure-by-Design Architecture

- **IPS Stack & Applications:** Modular network services with well-defined interfaces.
- **CONNECTOR:** Provides controlled inter-node messaging and abstraction for distributed systems.
- **File Systems & USB Modules:** Provide safe, deterministic access paths to storage and USB devices.

✔ Supports CRA secure-by-design principles through modular architecture and controlled interfaces

4.2 Data Handling & Communication

- Middleware ensures **structured, predictable message flows**.
- Avoids uncontrolled shared memory or inter-component interference.
- Provides error reporting and monitoring of communication services.

✔ Aligns with CRA expectations for predictable and safe data handling

4.3 Secure Delivery, Integrity & Authenticity (via Sciopta Kernel)

Middleware components are distributed as part of the same secure delivery as the Sciopta Kernel:

- **Digitally signed delivery:** The entire delivery package (including middleware) is signed using PGP/GPG.
- **Secure download:** HTTPS with password delivered via signed email (S/MIME or PGP).
- **Integrity verification:** Each kernel files in the delivery includes a hash file that can be verified against the TÜV certification report, ensuring the kernel binary has not been tampered.

✔ Fully satisfies CRA requirements for secure delivery, integrity, and authenticity

4.4 Resilience & Fault Containment

- Middleware modules implement **error detection and service isolation**.
- Faults in one module (e.g., network stack, file system) do not propagate to other services.

- CONNECTOR provides robust multi-node communication management.

✔ Supports CRA resilience principles at the middleware level

4.5 Lifecycle Management

- Versioned middleware modules with clear maintenance documentation.
- Integration guides describe supported configurations and update practices.
- Lifecycle support is **module-based**, patching and updates follow documented processes.

✔ Supports CRA expectations for lifecycle and update management

4.6 Documentation and Compliance

- **Technical documentation** provides full architecture and integration guidance.
- Manuals describe configuration, supported platforms, and operational assumptions.
- Documentation can be referenced in CRA technical files.

✔ Supports CRA documentation obligations

4.7 User Information & Guidance

- Installation and configuration instructions are provided in manuals for all middleware modules.
- Usage guidance covers supported features, limits, and operational assumptions.

✔ Aligns with CRA user information requirements

4.8 Certification & Assurance

- Middleware components are not certified, but development follows the same principles as the certified SCIOPTA RTOS.

✔ Provides integration-level assurance when used with Sciopta Safety Certified Kernel

5 Summary Table – CRA Requirements vs Sciopta Middleware Features

CRA Requirement	Sciopta Middleware Support
Secure-by-Design Architecture	Modular services, controlled interfaces, IPS stack, SCAPI API, CONNECTOR, File/USB modules
Data Handling & Communication	Structured message flows, controlled inter-module communication
Secure Delivery, Integrity & Authenticity	PGP-signed packages, HTTPS, password via signed email, SHA256/MD5 hashes (independent TÜV reference)
Resilience & Fault Containment	Error detection, service isolation, fault containment
Vulnerability & Lifecycle Management	Versioning, maintenance guides, module updates
Documentation & Conformity Assessment	Manuals for IPS, CONNECTOR, SCAPI API, File/USB modules
User Information & Guidance	Installation, configuration, integration instructions
Certification & Assurance	Middleware follows SCIOPTA RTOS development principles; Kernel is TÜV-certified

6 Conclusion

Sciopta Middleware provides **modular, documented, and integration-ready software components** that complement the Sciopta Kernel.
The Kernel itself implements a **secure delivery and integrity** (PGP-signed packages, HTTPS distribution, independent SHA256/MD5 hash verification) that fully satisfies CRA requirements for secure distribution and authenticity.

These components help manufacturers **implement structured communication, modular services, and predictable system behavior**, supporting CRA principles at the middleware layer.