

# ENISA European Union Common Criteria for Cybersecurity Certification Compliance Attestation

## Introduction

The ENISA European Union Common Criteria (EUCC) scheme is a cybersecurity certification framework established under Regulation (EU) 2019/881 — the EU Cybersecurity Act — and operationalised through Commission Implementing Regulation (EU) 2024/482. It provides a standardised, EU-wide framework for the security evaluation and certification of ICT products, including software, hardware, and components, based on the international Common Criteria standard (ISO/IEC 15408) and the Common Methodology for IT Security Evaluation (ISO/IEC 18045).

The EUCC scheme is particularly relevant to Akka as a provider of software products with digital elements, including its open-source SDKs and SaaS platform. EU customers — particularly those in regulated sectors such as critical infrastructure, financial services, defence, and government — increasingly require evidence that the software components they use have been developed and operated to standards consistent with the EUCC. Furthermore, compliance with the EUCC is recognised as supporting alignment with the EU Cyber Resilience Act (EU CRA), which mandates security requirements for products with digital elements placed on the EU market.

This attestation confirms Akka's alignment with the security requirements of the EUCC scheme as of the date stated below. It is not a formal EUCC certification issued by an accredited conformity assessment body, but represents Akka's internal assessment of its compliance with the scheme's requirements as applied to its software development and operations practices.

## Scope

This attestation covers Akka Technologies, Inc.'s ("Akka") software development lifecycle, security architecture, vulnerability management, and operational security practices as they pertain to the EUCC scheme. In-scope activities and systems include:

Software development: the development, testing, and release processes for Akka's SaaS platform and open-source SDK components.

Security architecture: the design and documentation of security-relevant architecture for Akka's platform and components.

Vulnerability management: identification, assessment, and remediation of security vulnerabilities in Akka's software and infrastructure.

Cryptographic controls: the selection, implementation, and management of cryptographic mechanisms.

Access management and audit logging: controls governing privileged access, authentication, and the integrity of audit records.

## Compliance Posture

Akka maintains 135 controls specifically mapped to the EUCC within its Information Security Management System (ISMS). All 135 controls are in Implemented status. Risk distribution across the control set is as follows:

- 135 controls rated Low risk
- 0 controls rated Medium risk
- 0 controls rated High risk

Overall EUCS compliance is assessed as Compliant. The uniformly Low risk profile across all 135 controls reflects the maturity and depth of Akka's security engineering practices. Akka's approach to secure software development, cryptographic hygiene, and vulnerability management is embedded in its engineering culture and supported by automated tooling, formal processes, and continuous improvement.

## Key Controls Implemented

### Security Architecture and Documentation

Akka maintains formal documentation of its security architecture for the SaaS platform, including trust boundaries, data flows, authentication and authorisation models, cryptographic control points, and network segmentation. Security architecture reviews are conducted as part of significant design changes, and a dedicated security review gate is included in the product development lifecycle. Architecture documentation is maintained as a living artefact and reviewed periodically to ensure it accurately reflects the deployed system.

### Secure Development Lifecycle

Akka's software development processes incorporate security at every phase of the lifecycle. Security requirements are defined alongside functional requirements at the design stage. Threat modelling is applied to new features and components to identify attack surfaces and design mitigations before implementation. Code review processes include security-focused review criteria. Static analysis and dependency scanning tools are integrated into the CI/CD pipeline to detect common vulnerability classes and known-vulnerable dependencies

automatically. Security testing — including penetration testing — is conducted on a regular basis and following major releases.

## Vulnerability Management and Disclosure

Akka operates a comprehensive vulnerability management programme covering both its developed software and its supporting infrastructure. Automated scanning identifies vulnerabilities in third-party dependencies, container images, and infrastructure configurations on a continuous basis. Identified vulnerabilities are triaged using a risk-based approach, and remediation timelines are defined by severity. Akka maintains a responsible disclosure (coordinated vulnerability disclosure) policy, published at [trust.akka.io](https://trust.akka.io), that enables external security researchers to report potential vulnerabilities through a defined channel. Critical vulnerabilities are addressed through an emergency patching process with defined response timelines.

## Cryptographic Controls

Akka implements cryptographic controls across its platform in accordance with current best practice and applicable standards. Encryption is applied to all data in transit using TLS 1.2 or higher, with strong cipher suites enforced. Data at rest is encrypted using AES-256 or equivalent. Cryptographic key management procedures govern the generation, storage, rotation, revocation, and destruction of cryptographic keys. Weak or deprecated cryptographic algorithms are prohibited by policy and enforced through technical controls. Akka's cryptography policy is reviewed annually to incorporate advances in cryptographic standards and to address emerging threats.

## Access Management and Least Privilege

Access to Akka's systems, platform, and development environments is governed by a formal access control policy based on the principle of least privilege. Access rights are assigned

based on job role and reviewed at least quarterly. Privileged access is subject to additional controls including multi-factor authentication, time-limited sessions, and enhanced audit logging. Service accounts and application credentials are managed through secrets management tooling, preventing hard-coded credentials. User access is promptly revoked upon changes in employment status or role.

## Audit Logging and Monitoring

Akka maintains comprehensive audit logging across its platform and infrastructure, capturing authentication events, privileged actions, configuration changes, and security-relevant API calls. Logs are stored in a centralised, tamper-resistant logging system with access controls preventing unauthorised modification. Log retention periods are defined and enforced. Security monitoring operates continuously, with alerting on defined anomalous behaviour patterns. Log review and anomaly investigation are performed on a regular basis by the security team.

## Supply Chain and Component Security

Akka manages the security of third-party components — including open-source libraries, container base images, and cloud services — as an integral part of its security programme. A software bill of materials (SBOM) is maintained for Akka's software products, enabling rapid identification of affected components when new vulnerabilities are disclosed. Third-party dependencies are reviewed and approved before adoption, and version pinning combined with automated update monitoring ensures that Akka is notified of security-relevant updates promptly. Cloud infrastructure providers are selected based on their security certifications and their own compliance with relevant standards.

## Supporting Evidence

The following evidence supports this attestation:

- ISO 27001-aligned ISMS with 135 fully implemented EUCC controls, all rated Low risk
- SOC 2 Type II attestation report from an independent auditor (available under NDA on request)
- Documented secure development lifecycle (SDLC) incorporating threat modelling, security code review, and security testing
- Automated SAST/SCA scanning integrated into CI/CD pipeline
- Responsible disclosure policy published at trust.akka.io
- Cryptography policy reviewed and approved within the last twelve months
- Software bill of materials (SBOM) maintained for platform and SDK components
- Access control policy with quarterly access reviews and MFA enforcement
- Centralised audit logging with tamper-resistant storage and defined retention periods

## Conclusion

Akka Technologies, Inc. attests that, as of the date of this document, its software development, security architecture, vulnerability management, and operational security practices align with the requirements of the ENISA European Union Common Criteria (EUCC) cybersecurity certification scheme established under Regulation (EU) 2019/881 and Implementing Regulation (EU) 2024/482. All 135 EUCC controls in Akka's ISMS are fully implemented, and all controls are rated at Low risk.

While this document constitutes an internal self-assessment rather than a formal EUCC certificate issued by an accredited conformity assessment body, it demonstrates the depth and maturity of Akka's security engineering practices and its commitment to meeting the standards expected of a software provider in the EU market. Akka continues to invest in its security programme and to track developments in the EUCC scheme and the broader EU Cybersecurity Act framework.



Akka.io | info@akka.io | 1-877-989-7372  
580 California St, #1231 San Francisco, CA 94104

This attestation is reviewed annually or upon material changes to Akka's software, architecture, or the applicable regulatory framework. It is available to customers, prospects, and competent authorities on request.

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.

michael.nash@akka.io

Date: 20 April 2026