AKKA

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

NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Attestation

Issued by: Akka Technologies, Inc.

Signed by: **Michael Nash**, Chief Information Security Officer (michael.nash@akka.io)

Date: April 20, 2026

Document Status: Active — Subject to Annual Review

Introduction

This document constitutes a formal attestation by Akka Technologies, Inc. ("Akka") of its alignment with NIST Special Publication 800-161 Revision 1 (NIST SP 800-161r1), "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," published by the National Institute of Standards and Technology (NIST).

NIST SP 800-161r1 provides comprehensive guidance for managing cybersecurity risks throughout the supply chain — including hardware, software, and services sourced from third-party suppliers. It is one of the most thorough supply chain risk management frameworks available, drawing from and integrating controls across multiple NIST publications. Akka has adopted this framework to ensure that its supply chain security practices meet the highest available standard of rigour.

Scope

This attestation covers all supply chain risk management activities conducted by Akka Technologies, Inc. in connection with the development, delivery, and operation of the Akka platform — including the SaaS offering and open-source SDK suite. The scope encompasses

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

Akka's relationships with hardware vendors, software component suppliers, cloud infrastructure providers, managed service providers, and all other third parties whose products or services are integrated into or support Akka's operations and product delivery.

Compliance Posture

Akka has mapped its supply chain risk management controls against all 304 controls defined in NIST SP 800-161r1. All 304 controls are fully Implemented.

This represents 100% implementation — one of the most comprehensive control coverage positions across any framework in Akka's compliance programme. Risk assessments across all controls indicate that 303 controls carry a Low residual risk rating and 1 control carries a Medium residual risk rating. This means 99.7% of controls are assessed at Low risk, reflecting the depth and effectiveness of Akka's supply chain risk management programme.

The breadth and depth of NIST SP 800-161r1 — spanning organisational policy, supplier assessment, software provenance, hardware integrity, contractual security requirements, and incident response for supply chain events — makes full implementation a significant undertaking. Akka's achievement of 100% implementation reflects a sustained, deliberate investment in supply chain security as a foundational element of its security programme.

Key Controls and Implementation Highlights

Supply Chain Risk Management Policy and Programme

Akka has established a formal Cybersecurity Supply Chain Risk Management (C-SCRM) policy that defines objectives, roles, responsibilities, and processes for managing supply chain risk. The programme is governed at the CISO level and integrated into Akka's broader ISMS

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

governance structure. Risk treatment decisions for supply chain risks are documented and tracked through the ISMS risk register.

Supplier Vetting and Risk Assessment

All third-party suppliers, cloud service providers, and managed service vendors undergo formal security vetting prior to onboarding. Vetting includes review of the supplier's security posture (SOC 2 reports, ISO certifications, penetration test results where available), assessment of data handling practices, and evaluation of business continuity capabilities. Suppliers are assigned a risk classification, and higher-risk suppliers are subject to enhanced due diligence and more frequent review.

Contractual Security Requirements

Akka's standard supplier agreements and data processing agreements include contractual security requirements aligned with NIST SP 800-161r1 expectations. These requirements cover data protection obligations, incident notification timelines, audit rights, subprocessor controls, and obligations to maintain security certifications. Security requirements are tailored to the supplier's risk classification and the nature of the services provided.

Software Component Analysis and Software Bill of Materials (SBOM)

Akka employs FOSSA for automated software composition analysis across all software components used in the Akka platform. FOSSA provides continuous visibility into open-source dependencies, licence obligations, and known vulnerabilities within the software supply chain. A Software Bill of Materials (SBOM) is maintained and updated as part of the software build process, providing traceability for all third-party software components incorporated into Akka's products. This capability directly supports hardware and software provenance tracking requirements within NIST SP 800-161r1.

AKKA

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

Hardware and Software Provenance Tracking

Akka maintains records of the provenance of hardware and software assets used in its infrastructure and product delivery. For cloud-hosted infrastructure, Akka relies on the infrastructure assurance programmes of its primary cloud providers (including Google Cloud Platform), which themselves maintain hardware supply chain integrity controls and publish attestations of their own compliance. For software, FOSSA-based SBOM management provides the primary provenance tracking capability.

Incident Response for Supply Chain Events

Akka's Incident Response Policy explicitly covers supply chain security incidents, including compromise of a third-party component, discovery of a malicious dependency, or notification from a supplier of a breach. The incident response procedure defines escalation paths, containment actions (including the ability to rapidly isolate or replace compromised components), customer notification obligations, and post-incident review requirements. Akka participates in relevant industry threat intelligence communities to receive early warning of supply chain threats.

Continuous Monitoring and Supplier Review

Approved suppliers are subject to ongoing monitoring. This includes automated vulnerability alerting for known CVEs affecting third-party components (via FOSSA and cloud provider security bulletins), periodic review of supplier security posture (at least annually for high-risk suppliers), and assessment of any changes to a supplier's ownership, certifications, or incident history that may affect their risk classification.

AKKA

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

Supporting Evidence

Akka's compliance with NIST SP 800-161r1 is supported by the following evidence:

- SOC 2 Type II Report: Akka's SOC 2 Type II report covers vendor management and third-party risk controls, providing independent validation of Akka's supplier oversight practices.

- ISO 27001-Aligned ISMS: Akka's ISMS includes supplier security controls aligned with ISO/IEC 27001:2022 Annex A.15 (Supplier Relationships), providing a documented and auditable supplier risk management framework.

- FOSSA SBOM Programme: Akka's use of FOSSA for continuous software composition analysis provides ongoing, automated evidence of software supply chain visibility and vulnerability management.

- Cloud Provider Assurance: Google Cloud Platform and other primary infrastructure providers hold SOC 2 Type II and ISO 27001 certifications, providing assurance that the infrastructure supply chain meets stringent security standards.

- Supplier Register: Akka maintains a formal supplier register documenting all approved third-party suppliers, their risk classifications, vetting status, and review history.

Conclusion

Akka Technologies, Inc. has achieved full implementation of all 304 controls defined in NIST SP 800-161r1, with 99.7% of controls assessed at Low residual risk. This represents one of the most comprehensive supply chain risk management postures available under any recognised framework. Akka's investment in supplier vetting, SBOM management via FOSSA, contractual security requirements, and integrated incident response for supply chain events demonstrates a mature, enterprise-grade approach to cybersecurity supply chain risk management.

AKKA

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

This attestation is made in good faith based on Akka's current information security programme as of the date of issuance. It is available to customers, prospects, and auditors upon request and is subject to annual review and renewal.

Signed,

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.

michael.nash@akka.io

April 20, 2026