AKKA

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

Payment Card Industry Data Security Standard v4.0 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 the Payment Card Industry Data Security Standard version 4.0 (PCI-DSS v4.0), published by the PCI Security Standards Council (PCI SSC).

PCI-DSS v4.0 establishes security requirements for entities that store, process, or transmit cardholder data (CHD) or that could impact the security of a cardholder data environment (CDE). It is important to note at the outset that Akka itself does not store, process, or transmit cardholder data. Akka is a platform and SDK provider: its Akka platform provides infrastructure for building reactive microservices and distributed systems, and some customers may choose to build payment-adjacent applications using the Akka platform. Akka does not operate a cardholder data environment and is not a payment processor.

Nonetheless, Akka has adopted PCI-DSS v4.0 as a framework to ensure that its platform's security posture does not introduce weaknesses that could undermine the security of customers who build or operate payment applications on top of Akka, and to demonstrate to such customers that Akka's own security practices meet PCI-DSS expectations for a technology service provider.

AKKA

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

Scope

This attestation covers the information security management programme and platform security controls operated by Akka Technologies, Inc. in support of its Akka platform — a cloud-hosted SaaS offering and open-source SDK suite. The scope reflects Akka's role as a platform/SDK provider rather than as a party that directly handles cardholder data. Controls are implemented in respect of Akka's own systems, infrastructure, development practices, and supplier relationships. Akka's customers are responsible for their own PCI-DSS compliance when building cardholder data environments on or alongside the Akka platform.

Compliance Posture

Akka has mapped its internal controls against all 91 controls within Akka's PCI-DSS v4.0 implementation framework. All 91 controls are fully Implemented.

Risk assessments across these controls indicate that 34 controls carry a Low residual risk rating and 57 carry a Medium residual risk rating. No controls carry a High residual risk rating. The concentration of Medium-rated controls reflects the nature of PCI-DSS requirements — particularly those relating to network security, data protection, and third-party service provider oversight — which demand sustained operational vigilance even when well-implemented.

Key Controls and Implementation Highlights

Network Security

Akka maintains documented network security architecture for its cloud infrastructure, including network segmentation, firewall configuration standards, and controls over inbound and

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

outbound traffic. Network security configurations are reviewed periodically and following any significant infrastructure change. Akka's cloud infrastructure is hosted on Google Cloud Platform, which provides underlying network security capabilities and holds its own PCI-DSS compliance certifications.

Access Control

Access to Akka's systems is governed by a formal access control policy. User accounts are provisioned on the basis of least privilege and role-based access control. Unique user IDs are required; shared accounts are prohibited for privileged access. Multi-factor authentication (MFA) is mandatory for all access to cloud infrastructure and production systems. Password and authentication policies meet or exceed PCI-DSS v4.0 requirements. Access rights are reviewed regularly, and privileged access is subject to enhanced controls and periodic recertification.

Vulnerability Management

Akka operates a formal vulnerability management programme covering infrastructure, platform components, and software dependencies. Regular vulnerability scanning is conducted across Akka's cloud environment, with results tracked to remediation within defined SLAs based on severity. Software composition analysis is performed using FOSSA, providing continuous visibility into vulnerabilities in open-source dependencies. Penetration testing is commissioned regularly, with findings tracked to closure. Critical and high-severity vulnerabilities are prioritised for rapid remediation in line with PCI-DSS requirements.

Monitoring, Logging, and Alerting

Akka implements comprehensive logging and monitoring across its infrastructure and platform components. Security-relevant events are logged, centralised, and retained in accordance with Akka's data retention policy. Monitoring and alerting are configured to detect anomalous

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

activity, unauthorised access attempts, and potential indicators of compromise. Log integrity controls prevent tampering with audit trails. Security event reviews are conducted as part of regular operational processes.

Data Protection

As noted above, Akka does not store, process, or transmit cardholder data. Data protection controls within Akka's programme focus on the protection of Akka's own business data and customer data entrusted to Akka in the course of service delivery. Data classification and handling procedures are in place. Data is encrypted in transit using TLS and at rest using industry-standard encryption. Data retention and disposal procedures are documented and followed.

Secure Development

Akka embeds security into its software development lifecycle. Secure coding standards are documented and applied. Static application security testing (SAST), software composition analysis, and peer code review are incorporated into the development process. Security requirements are defined for new features, and security testing is conducted before significant releases. Developers receive security training appropriate to their role. These practices ensure that the Akka platform does not introduce vulnerabilities that could affect customers who build payment-adjacent applications on top of it.

Third-Party Service Provider Security

Akka maintains a formal supplier management programme. Third-party service providers — including cloud infrastructure providers, managed service vendors, and software suppliers — undergo risk-based security assessment prior to onboarding. Supplier agreements include security obligations, incident notification requirements, and audit rights. Critical suppliers are

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

reviewed at least annually. Akka maintains a list of all third-party service providers with access to Akka's environment or systems.

Incident Response

Akka maintains a documented Incident Response Policy and Procedure covering detection, containment, eradication, recovery, and post-incident review. The incident response process includes provisions for customer notification in the event of a security incident that could affect their environments. Tabletop exercises are conducted regularly to test and improve response capability.

Supporting Evidence

Akka's compliance with PCI-DSS v4.0 is supported by the following evidence:

- SOC 2 Type II Report: Akka's SOC 2 Type II report provides independent third-party validation of Akka's security controls across availability, security, and confidentiality — covering substantial portions of PCI-DSS requirements.

- ISO 27001-Aligned ISMS: Akka's ISMS, aligned with ISO/IEC 27001:2022, provides the governance framework for Akka's security programme and maps to PCI-DSS requirements for risk management, access control, vulnerability management, and incident response.

- Google Cloud Platform PCI-DSS Compliance: Akka's primary cloud infrastructure provider (Google Cloud Platform) is a PCI-DSS compliant service provider. This provides assurance that the underlying infrastructure layer meets PCI-DSS requirements, supporting Akka's overall posture.

- FOSSA Software Composition Analysis: Automated dependency scanning supports PCI-DSS vulnerability management requirements for third-party software components.

AKKA

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

Conclusion

Akka Technologies, Inc. has implemented all 91 controls within its PCI-DSS v4.0 alignment framework, with no High residual risk gaps. As a platform and SDK provider — not a payment processor or cardholder data handler — Akka's PCI-DSS compliance programme is focused on ensuring that Akka's own systems, infrastructure, and development practices do not introduce security weaknesses that could affect customers building payment-adjacent applications on the Akka platform.

Akka's SOC 2 Type II report, ISO 27001-aligned ISMS, and Google Cloud Platform's PCI-DSS compliance certification together provide a strong foundation of independent evidence supporting this attestation.

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