AKKA

Lightbend Inc, d.b.a Akka

Akka Federation Plane SLA Policy

2026-04-13

Version 1

Contents

1.1. Introduction

This policy defines the level of service with respect to the Akka Federated Plane. It contains the measurement parameters of this service and the solutions if the service levels are not met.

1.2. Scope

This Akka Federated Plane SLA is a policy that applies to the Akka Federated Plane that is accessible by each Akka Region and Customer user accounts through Akka.io.

This SLA applies only to Akka-hosted products for customers with paid Subscriptions and does not apply to any other product offered by Akka, including any Free Trial or other similar free products and services. Akka will provide at least ninety (90) days advance notice for adverse changes to this SLA.

1.3. Referenced Policies

1. Resilience Guarantee Policy - Akka's policy that guarantees Your Applications will never experience a data loss caused by Akka.

1.4. Referenced Frameworks and Standards

1. Akka's Internal Assurance Framework

1.5. Akka Federated Plane SLA

Our service-level agreements around our hosted services.

1.5.1. Uptime Target

Akka will use commercially reasonable efforts to make Akka-hosted products available with an uptime percentage of at least 99.9% within a single calendar month.

"**Uptime**" is defined as the system being responsive and operational.

1.5.2. Latency Target

Latency in this context refers to the time between an Akka application receiving a request and the time a response to this request is sent back to the caller. Specifically, Akka measures the time from the completion of receipt of a request (e.g. the request has been fully received), to the time the response is fully sent back to the caller.

This time is inclusive of:

1. Serialization and deserialization, if applicable
2. All API operations that are part of the Akka platform
3. Any persistence as a part of handling the request.

This time is exclusive of:

1. Time Your Application Services spends processing the request once the Akka API calls Your Application Services.
2. Any calls to external systems or services not a part of the Akka system.

Akka guarantees that the core platform and infrastructure will maintain a P90 response latency of 10 milliseconds.

The foregoing does not include latency resulting from Customers' own application logic, processing time, or any third-party integrations or services used by Customers application.

Should the included latency exceed the specified threshold due to infrastructure or service issues, Akka will issue Service Credit for the period affected.

Latency in this context is distinct from the Resilience Guarantee.

1.5.3. Service Credits

If Akka fails to meet the uptime commitment or the latency commitment as defined Akka will credit back to Customer a **"Service Credit"** for the period affected.

The Service Credit is a percentage of the applicable fees for the affected period to be credited to Customer, if Akka approves the claim, as set forth in the table below.

Monthly Uptime Percentage	Service Credit Percentage
99.8% - < 99.00%	25%
< 99.00%	50%

Latency Percentile	Service Credit Percentage
80% - 90%	25%
<80%	50%

1.5.4. Scheduled Downtime

Akka prides itself on never having any scheduled downtime periods. In the event a scheduled service or emergency downtime period is needed, Akka shall notify Customer of the scheduled downtime. This notification must specify the date and time of the system maintenance, expected duration, and anticipated system or service resumption time. Scheduled and emergency downtime periods are excluded from availability calculations.

1.5.5. Customer Obligations

In order to be eligible for any Service Credits, Customer must:

1. Log a support ticket in the Support Portal within twenty-four (24) hours of first becoming aware of an event that impacts service availability.
2. Submit a claim and all required information by the end of the month immediately following the month in which the downtime occurred.
3. Include all information necessary for Akka to validate the claim, including:
    a) A detailed description of the events resulting in downtime, including the request logs that document the errors and corroborate the claimed outage (with any confidential or sensitive information in the logs removed or replaced with asterisks);
    b) Information regarding the time and duration of the downtime;
    c) The number and location(s) of affected users (if applicable); and
    d) Descriptions of attempts to resolve the downtime at the time of occurrence.
4. Reasonably assist Akka in investigating the cause of the downtime and processing the claim.

1.5.6. Exclusions

This SLA does not apply to any unavailability, suspension or termination of Akka issues, directly or indirectly:

- Caused by factors outside of Akka's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Akka;
- That result from any actions or inactions of the customer, including failure to acknowledge a recovery volume or respond to resource health concerns;
- That result from equipment, software or other technology not supplied by Akka;
- Use of any pre-release of the Software such as Beta or Milestone releases, except for Developer Support and agreed to by Akka in an applicable Order Form;
- Use of software not obtained from Akka under the Support Agreement; or
- Use of a version of Akka's product where a known issue has been resolved in a subsequent version.

1.6. Compliance

For Akka employees, failure to comply with this policy may result in progressive discipline up to and including dismissal. For non-Akka employees and contractors, failure to comply may result in removal of the individual's ability to access and use Akka data and systems. Employers of non-Akka employees will be notified of any violations.

Glossary

EEA States The EU Member States as well as Iceland, Liechtenstein and Norway.. *see* EEA & EU

AAO Akka Automated Operations - a managed platform deployed within a customer VPC that fully automates and supports production-grade, self-clustering and elastic agentic services built with the Akka SDK.. *see* Akka SDK & VPC

AI Risk Management Framework A structured approach to identifying, assessing, and mitigating risks associated with AI systems, as outlined by the NIST.. *see* AI & NIST

Akka Application An application that is built using the Akka SDK. Akka applications contain APIs, workflows, streaming consumers, timers, and views for querying data. They are packed into Docker images and deployed as microservice instances within an Akka operating environment. Akka applications act as their own in-memory, durable database. They take responsibility for persisting their own state. Akka apps also cluster from within, creating a runtime cluster with other instances that handle balancing traffic, sharding data, and replicating their data to instances running within another region. Akka applications can be replicated between regions in different Akka Application Planes if needed.. *see* Akka Application Plane, Akka SDK & API

Akka Application Plane The runtime environment for hosting Akka applications within one or more regions. The Akka application plane provides compute, storage, and I/O to execute Akka apps. It also provides automation to increase or decrease application instance capacity, observability for monitoring and debugging application behavior, and infrastructure management. The application plane is responsible for ensuring an Akka application meets its SLA by managing the Akka application and the underlying infrastructure. Data in this plane does not leave your VPC nor does it interact with our Akka Federation Plane.. *see* Akka Federation Plane, SLA & VPC

Akka CLI The CLI for developers, operators, and InfoSec teams to interface with various Akka environments. The Akka CLI provides utilities for building, testing, packing, and deploying Akka applications. It also provides utilities for observability, secrets management, service scaling, and account management.. *see* CLI

Akka Federated Plane The Akka Federated Plane is an online service to coordinate between Akka regions, providing maintenance and administrative operations to and between such regions.. 1

Akka SDK SDK with support for programming components, a local debugging console, and a test kit for building, testing, and packing Akka applications.. *see* SDK

ALC-DVS.1.1.1C In the context of the EUCC standard, ALC-DVS.1.1.1C is a specific assurance component within the Common Criteria framework. It falls under the ALC class, specifically the DVS family.. *see* ALC, DVS & EUCC

ALC-DVS.2 A component of the ALC class within the CC framework (EUCC), specifically under the DVS family. This component requires that security measures in place during the development of the TOE are sufficient to protect the TOE and its associated assets. It aims to ensure that the development environment is secure and that the measures are adequate to maintain the confidentiality and integrity of the TOE throughout its development.. *see* ALC, CC, DVS, EUCC & TOE

Assets Entities that the owner of the TOE presumably places value upon. In the context of a DSS, assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code and data provided to produce the TOE. *see* DSS & TOE

Authentic Data In the context of the EU DORA, data from a statutory public register, the dissemination and/or processing of which is subject to statutory requirements and which are disclosed by the customer to third parties in connection with the performance of a contract.. *see* EU DORA

Business Continuity Planning See Business Continuity Planning. *see* Business Continuity Planning

Business Operations General term for the entirety of operations performed by the developer related to the TOE, e.g. "personalization is part of Business Operations.. *see* TOE

BYOD Abbreviation for **B**ring **Y**our **O**wn **D**evice, a corporate IT policy that permits employees to use their personal smartphones, laptops, or tablets to access company data and perform work tasks rather than relying on employer-provided hardware. See personal-device.. *see* IT

Consent Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.. *see* Data Subject

Consumer In the context of the CCPA, A natural person who is a California resident.. *see* CCPA

Critical or Important Function In the context of the EU DORA, a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.. *see* EU DORA

CSF The NIST Cyber Security Framework (v2.0). *see* NIST

Data Subject Request A request made by an individual or an individual's legal representative to request Akka to do something which falls under one of the rights granted to EU-based individuals by the GDPR.. *see* EU & GDPR

Data Subjects See Data Subject.. *see* Data Subject

Deployer Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. *see* AI

Development environment Environment in which the TOE is developed; development includes the production of the TOE.. *see* TOE

DORA The EU Digital Operational Resilience Act, or DORA Regulation. *see* DORA Regulation & EU

DORA CO DORA **C**ontractural **O**bligations - specific contractural obligations required to be in place by the EU DORA for regulated industries and their ICT suppliers.. *see* DORA, EU DORA & ICT

DR **D**isaster **R**ecovery is a set of policies, tools, and procedures used to regain access and functionality to IT infrastructure following a catastrophic event. While HA focuses on surviving small hardware failures, DR is the "Plan B" for major disasterssuch as fires, floods, cyberattacks (like ransomware), or massive regional power outages.. *see* HA & IT

DSAR **D**ata **S**ubject **A**ccess **R**equest - A request by an individual under data protection law (e.g. GDPR) to obtain a copy of the personal data an organisation holds about them, along with information about how it is processed.. *see* GDPR

DSD Development Security Documentation, in the context of the EU CRA. *see* EU CRA

DSS Development Security System, in the context of the EU CRA. *see* EU CRA

EKS Amazon's **E**lastic **K**ubernetes **S**ervice - A managed service that automates the deployment, scaling, and management of **K**ubernetes control planes and infrastructure on AWS.. *see* AWS

EU CRA EU **C**yber **R**esiliency **A**ct: The goal of the CRA is to protect consumers and strengthen the EU's overall level of resilience. This means reducing the risks for all users of digital products, whether private individuals or public entities (corporations, hospitals, banks, utilities, postal services and so on). The CRA is mandatory, and compliance is required for CE Marking of regulated products, as well as for distribution in the European market. The CRA includes some strict, coercive measures such as heavy fines.. *see* CE Marking & EU

EU DORA See DORA. *see* DORA

EU GDPR Specifically the EU version of the GDPR.. *see* EU & GDPR

EUCC **E**uropean **U**nion **C**ommon **C**riteria, a standard for evaluating the security of information technology products and systems, ensuring they meet defined security requirements and specifications. The EUCC framework is derived from the SOG-IS Common Criteria which in turn is based on the ISO/IEC 15408-1 Common Criteria standard for Information Technology Security Evaluation. However, the SOG-IS adds an additional layer of mutual recognition among European countries. This means that a product evaluated and certified in one member state under SOG-IS is recognized by other member states, reducing the need for multiple evaluations.. *see* IEC & ISO

High Security Area Area where TOE related data or material classified critical or very critical is accessible, and Security Control areas (access control and intrusion detection) where applicable.. *see* TOE

ICT Asset In the context of the EU DORA, a software or hardware asset in the network and information systems used by the financial entity.. *see* EU DORA

ICT Risk In the context of the EU DORA, any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.. *see* EU DORA

ICT Services In the context of the EU DORA, digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.. *see* EU DORA & ICT

ICT Third-Party Risk An ICT risk that may arise for a financial entity in relation to its use of ICT services provided by ICT third-party service providers or by subcontractors of the latter, including through outsourcing arrangements.. *see* ICT

ICT Third-Party Service Provider Any company (whether independent or part of a financial group) providing ICT Services to financial entities. *see* ICT Services

ICT-Related Incident In the context of the EU DORA, a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity.. *see* EU DORA

IS Incident An IS incident. A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.. *see* IS

ISO/IEC 27701 Security techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and Guidelines. *see* IEC & ISO

ITSEF **I**nformation **T**echnology **S**ecurity **E**valuation **F**acility. It is an accredited laboratory responsible for conducting security evaluations of IT products and systems according to the Common Criteria standards. *see* IT

Major ICT-Related Incident In the context of the EU DORA, an ICT-Related Incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity.. *see* EU DORA & ICT-Related Incident

Network and Information System In the context of the EU DORA, An electronic communications network as defined in Article 2(1) of Directive (EU) 2018/1972; Any device or group of devices connected or associated with each other, one or more of which carry out automated processing of digital data based on a programme; or Digital data stored, processed, retrieved or transmitted by the elements specified for the purpose of their operation, use, protection and maintenance.. *see* EU DORA

P90 A statistical measure used to describe the performance of a system (usually latency or response time). If an SLA specifies a P90 of 500ms, it means that 90 percent of all requests are completed in 500ms or less.. 2, *see* SLA

Personal Device A device not owned by Akka, but owned by a User. Examples include personal cell phones, tablets, smart watches and so forth. See BYOD.. *see* BYOD

PII **P**ersonally **I**dentifiable **I**nformation is any data that can be used on its own or with other relevant information to identify, contact, or locate a single person. See Personal Information.. *see* Personal Information

Privileged Users In the context of the EU DORA, Privileged users: system administrators and operators who supervise the operation of the system as a whole. In addition, there may also be users with privileged user rights or user rights with advanced functionality in a specific IT system (e.g. they may grant users read/write permissions).. *see* EU DORA

Resilience Guarantee Akka's Resilience Guarantee Policy.. 2

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

RoPA **R**ecord **o**f **P**rocessing **A**ctivities - A mandatory documentation requirement under Article 30 of the GDPR that organisations must maintain, listing all personal data processing activities, their purposes, data categories, retention periods, and technical/organisational safeguards.. *see* GDPR

SCC **S**tandard **C**ontractual **C**lauses - Pre-approved contractual clauses issued by the European Commission that provide a legal mechanism for transferring personal data from the EEA to third countries that have not been deemed to offer an adequate level of data protection.. *see* EEA

Service Credit A financial credit applied to future purchases granted against a period of delay or outage that Akka guaranteed against.. 2

Significant Cyber Threat In the context of the EU DORA, a cyber threat the technical characteristics of which indicate that it could have the potential to result in a major ICT-Related Incident or a major operational or security payment-related incident.. *see* EU DORA & ICT-Related Incident

SLA A **S**ervice **L**evel **A**greement is a legal or formal commitment between a service provider and a customer. It defines the minimum level of service expected and, crucially, the penalties (such as service credits or refunds) if those levels aren't met.. 1, 3

SLO A **S**ervice **L**evel **O**bjective is a specific target or goal within an SLA. It is the technical benchmark that the team aims to hit to keep the customer happy. SLOs are usually more stringent than the SLA to provide a "safety buffer.". *see* SLA

SOC **S**ystem and **O**rganization **C**ontrols - A suite of audit reports produced by an independent third-party auditor (CPA firm) under the AICPA Trust Services Criteria, assessing the controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type II reports cover a defined period and provide evidence of the operating effectiveness of controls.. *see* AICPA

Support Portal Akka's online support ticketing/issue system.. 2

Third Country In the context of the EU and EU customers, any State that is not a member of the EEA.. *see* EEA & EU

Threat-Led Penetration Testing In the context of the EU DORA, a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.. *see* EU DORA

Trade Secret In the context of the EU DORA, a fact, information, other data or an assembly thereof, connected to an economic activity, which is secret in the sense that it is not, as a body or as the assembly of its components, generally known or readily accessible to persons dealing with the affected economic activity and therefore it has pecuniary value, and which is subject to steps made with the care that is generally expected under the given circumstances, by the person lawfully in control of the information, to keep it secret. Protected knowledge (know-how), technical, economic or organisational knowledge, solution, experience or the assembly thereof that are classified as trade secret and recorded in an identifiable manner also constitute trade secrets.. *see* EU DORA

TSC The **T**rust **S**ervices **C**riteria are a set of control criteria developed by the AICPA to evaluate and report on the suitability of the design and operating effectiveness of controls at a service organization relevant to the Security (the only required criterion), Availability, Processing Integrity, Confidentiality, or Privacy of the information and systems used to process user data.. *see* AICPA

UK **U**nited **K**ingdom - The sovereign state comprising England, Scotland, Wales, and Northern Ireland. Following its departure from the EU, the UK maintains its own data protection regime under the UK GDPR and the Data Protection Act 2018.. *see* EU & GDPR

Your Application Services In the context of Akka's policies, Your Application Services refers to application components or services developed by the customer to implement their business logic.. 1

Index