AKKA

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

Attestation de conformité au schéma européen de certification de cybersécurité EUCC (ENISA Common Criteria)

Introduction

Le schéma européen de certification de cybersécurité basé sur les Critères Communs (EUCC) est un cadre de certification établi par le Règlement (UE) 2019/881 — la Loi sur la cybersécurité de l'UE — et mis en œuvre par le Règlement d'exécution (UE) 2024/482 de la Commission. Il fournit un cadre européen standardisé pour l'évaluation et la certification de la sécurité des produits TIC, notamment les logiciels, les matériels et les composants, basé sur la norme internationale des Critères Communs (ISO/IEC 15408) et la Méthodologie commune d'évaluation de la sécurité des technologies de l'information (ISO/IEC 18045).

Le schéma EUCC est particulièrement pertinent pour Akka en tant que fournisseur de produits logiciels comportant des éléments numériques, notamment ses SDK open source et sa plateforme SaaS. Les clients de l'UE — en particulier ceux relevant de secteurs réglementés tels que les infrastructures critiques, les services financiers, la défense et les administrations publiques — demandent de plus en plus souvent des preuves que les composants logiciels qu'ils utilisent ont été développés et exploités conformément à des normes cohérentes avec l'EUCC. Par ailleurs, la conformité à l'EUCC est reconnue comme soutenant l'alignement avec le Règlement européen sur la cyber-résilience (EU CRA), qui impose des exigences de sécurité aux produits comportant des éléments numériques mis sur le marché de l'UE.

La présente attestation confirme l'alignement d'Akka avec les exigences de sécurité du schéma EUCC à la date indiquée ci-dessous. Il ne s'agit pas d'une certification EUCC formelle délivrée par un organisme d'évaluation de la conformité accrédité, mais d'une évaluation

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

interne par Akka de sa conformité aux exigences du schéma telles qu'appliquées à ses pratiques de développement logiciel et d'exploitation.

Périmètre

La présente attestation couvre le cycle de vie de développement logiciel, l'architecture de sécurité, la gestion des vulnérabilités et les pratiques de sécurité opérationnelle d'Akka Technologies, Inc. (« Akka ») tels qu'ils se rapportent au schéma EUCC. Les activités et systèmes entrant dans le périmètre comprennent :

Développement logiciel : les processus de développement, de test et de publication de la plateforme SaaS d'Akka et des composants SDK open source.

Architecture de sécurité : la conception et la documentation de l'architecture pertinente sur le plan de la sécurité pour la plateforme et les composants d'Akka.

Gestion des vulnérabilités : identification, évaluation et remédiation des vulnérabilités de sécurité dans les logiciels et l'infrastructure d'Akka.

Contrôles cryptographiques : sélection, mise en œuvre et gestion des mécanismes cryptographiques.

Gestion des accès et journalisation des audits : contrôles régissant les accès privilégiés, l'authentification et l'intégrité des enregistrements d'audit.

Situation de conformité

AKKA

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

Akka maintient 135 contrôles spécifiquement mappés à l'EUCC au sein de son Système de Management de la Sécurité de l'Information (SMSI). Les 135 contrôles sont au statut Mis en œuvre. La répartition des risques au sein du dispositif de contrôle est la suivante :

- 135 contrôles cotés Risque faible
- 0 contrôle coté Risque moyen
- 0 contrôle coté Risque élevé

La conformité globale à l'EUCC est évaluée comme Conforme. Le profil de risque uniformément faible sur l'ensemble des 135 contrôles témoigne de la maturité et de la profondeur des pratiques d'ingénierie de la sécurité d'Akka. L'approche d'Akka en matière de développement logiciel sécurisé, d'hygiène cryptographique et de gestion des vulnérabilités est ancrée dans sa culture d'ingénierie et s'appuie sur des outils automatisés, des processus formels et une amélioration continue.

Principaux contrôles mis en œuvre

Architecture de sécurité et documentation

Akka maintient une documentation formelle de son architecture de sécurité pour la plateforme SaaS, incluant les frontières de confiance, les flux de données, les modèles d'authentification et d'autorisation, les points de contrôle cryptographiques et la segmentation réseau. Des revues d'architecture de sécurité sont conduites lors des modifications substantielles de la conception, et un contrôle dédié à la revue de sécurité est intégré dans le cycle de vie de développement produit. La documentation de l'architecture est maintenue comme un artefact vivant et examinée périodiquement pour s'assurer qu'elle reflète fidèlement le système déployé.

AKKA

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

Cycle de vie de développement sécurisé

Les processus de développement logiciel d'Akka intègrent la sécurité à chaque phase du cycle de vie. Les exigences de sécurité sont définies conjointement avec les exigences fonctionnelles lors de la phase de conception. La modélisation des menaces est appliquée aux nouvelles fonctionnalités et composants pour identifier les surfaces d'attaque et concevoir des mesures d'atténuation avant la mise en œuvre. Les processus de revue de code intègrent des critères de revue axés sur la sécurité. Des outils d'analyse statique et d'analyse des dépendances sont intégrés dans le pipeline CI/CD pour détecter automatiquement les classes de vulnérabilités courantes et les dépendances présentant des vulnérabilités connues. Des tests de sécurité — notamment des tests d'intrusion — sont conduits régulièrement et après chaque version majeure.

Gestion des vulnérabilités et divulgation

Akka exploite un programme complet de gestion des vulnérabilités couvrant à la fois ses logiciels développés en interne et son infrastructure sous-jacente. Des analyses automatisées identifient en continu les vulnérabilités dans les dépendances tierces, les images de conteneurs et les configurations d'infrastructure. Les vulnérabilités identifiées font l'objet d'un triage selon une approche basée sur les risques, et des délais de remédiation sont définis en fonction de leur niveau de gravité. Akka maintient une politique de divulgation responsable (divulgation coordonnée des vulnérabilités), publiée sur trust.akka.io, permettant aux chercheurs en sécurité externes de signaler des vulnérabilités potentielles via un canal défini. Les vulnérabilités critiques sont traitées via un processus de correction d'urgence avec des délais de réponse définis.

Contrôles cryptographiques

Akka met en œuvre des contrôles cryptographiques sur l'ensemble de sa plateforme conformément aux meilleures pratiques actuelles et aux normes applicables. Le chiffrement est appliqué à toutes les données en transit via TLS 1.2 ou supérieur, avec imposition de

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

suites de chiffrement robustes. Les données au repos sont chiffrées en AES-256 ou équivalent. Des procédures de gestion des clés cryptographiques encadrent la génération, le stockage, la rotation, la révocation et la destruction des clés cryptographiques. Les algorithmes cryptographiques faibles ou obsolètes sont interdits par politique et imposés via des contrôles techniques. La politique cryptographique d'Akka est réexaminée annuellement pour intégrer les avancées des normes cryptographiques et faire face aux menaces émergentes.

Gestion des accès et moindre privilège

L'accès aux systèmes, à la plateforme et aux environnements de développement d'Akka est régi par une politique formelle de contrôle des accès fondée sur le principe du moindre privilège. Les droits d'accès sont attribués en fonction du rôle professionnel et examinés au moins trimestriellement. Les accès privilégiés sont soumis à des contrôles supplémentaires, notamment l'authentification multifacteur, des sessions limitées dans le temps et une journalisation d'audit renforcée. Les comptes de service et les identifiants applicatifs sont gérés via des outils de gestion des secrets, empêchant l'inscription en dur des identifiants. Les accès utilisateurs sont révoqués rapidement en cas de changement de statut professionnel ou de rôle.

Journalisation des audits et surveillance

Akka maintient une journalisation d'audit complète sur l'ensemble de sa plateforme et de son infrastructure, enregistrant les événements d'authentification, les actions privilégiées, les modifications de configuration et les appels API pertinents sur le plan de la sécurité. Les journaux sont conservés dans un système de journalisation centralisé et inviolable, avec des contrôles d'accès empêchant toute modification non autorisée. Les durées de conservation des journaux sont définies et appliquées. La surveillance de la sécurité opère en continu, avec des alertes sur les schémas de comportement anormal définis. L'examen des journaux et l'investigation des anomalies sont réalisés régulièrement par l'équipe de sécurité.

AKKA

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

Sécurité de la chaîne d'approvisionnement et des composants

Akka gère la sécurité des composants tiers — notamment les bibliothèques open source, les images de base de conteneurs et les services cloud — dans le cadre intégral de son programme de sécurité. Une nomenclature logicielle (SBOM) est maintenue pour les produits logiciels d'Akka, permettant une identification rapide des composants affectés lors de la divulgation de nouvelles vulnérabilités. Les dépendances tierces sont examinées et approuvées avant adoption, et la combinaison du verrouillage de version et de la surveillance automatisée des mises à jour garantit qu'Akka est rapidement informée des mises à jour pertinentes sur le plan de la sécurité. Les fournisseurs d'infrastructure cloud sont sélectionnés sur la base de leurs certifications de sécurité et de leur propre conformité aux normes applicables.

Éléments probants à l'appui

Les éléments probants suivants viennent à l'appui de la présente attestation :

- SMSI aligné sur la norme ISO 27001 avec 135 contrôles EUCC intégralement mis en œuvre, tous cotés Risque faible

- Rapport d'attestation SOC 2 Type II délivré par un auditeur indépendant (disponible sous accord de confidentialité sur demande)

- Cycle de vie de développement sécurisé (SDLC) documenté intégrant la modélisation des menaces, la revue de code sécurisée et les tests de sécurité

- Analyse SAST/SCA automatisée intégrée dans le pipeline CI/CD

- Politique de divulgation responsable publiée sur trust.akka.io

- Politique cryptographique examinée et approuvée dans les douze derniers mois

- Nomenclature logicielle (SBOM) maintenue pour les composants de la plateforme et des SDK

- Politique de contrôle des accès avec revues trimestrielles des accès et imposition de l'authentification multifacteur

- Journalisation d'audit centralisée avec stockage inviolable et durées de conservation définies

Conclusion

Akka Technologies, Inc. atteste qu'à la date du présent document, ses pratiques de développement logiciel, d'architecture de sécurité, de gestion des vulnérabilités et de sécurité opérationnelle sont alignées sur les exigences du schéma européen de certification de cybersécurité EUCC (ENISA Common Criteria) établi par le Règlement (UE) 2019/881 et le Règlement d'exécution (UE) 2024/482. Les 135 contrôles EUCC du SMSI d'Akka sont intégralement mis en œuvre, et l'ensemble des contrôles est coté au niveau de Risque faible.

Bien que ce document constitue une auto-évaluation interne plutôt qu'un certificat EUCC formel délivré par un organisme d'évaluation de la conformité accrédité, il témoigne de la profondeur et de la maturité des pratiques d'ingénierie de la sécurité d'Akka et de son engagement à satisfaire aux normes attendues d'un fournisseur de logiciels sur le marché de l'UE. Akka continue d'investir dans son programme de sécurité et de suivre les évolutions du schéma EUCC et du cadre plus large de la Loi sur la cybersécurité de l'UE.

La présente attestation est réexaminée annuellement ou lors de modifications substantielles des logiciels, de l'architecture d'Akka ou du cadre réglementaire applicable. Elle est disponible sur demande auprès des clients, prospects et autorités compétentes.

Michael Nash

Directeur de la Sécurité des Systèmes d'Information (CISO)

Akka Technologies, Inc.

michael.nash@akka.io

AKKA

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

Date : 20 avril 2026