
Dossier 01 — Constructeurs et développeurs

Public : les équipes qui construisent une application d'IA (produit grand public, outil interne, plateforme) et qui veulent y intégrer une couche éthique sans changer de modèle.

Identité : ELYSÉA est une infrastructure cognitive éthique embarquable par SDK, un cerveau généraliste. Elle ne parle pas à l'utilisateur : c'est l'application du constructeur qui parle. ELYSÉA n'est ni compagnon, ni chatbot, ni coach, ni thérapeute, ni produit de bien-être, ni dispositif médical.

Statut au 01/10/2026 : ventes fermées tant que l'entité n'est pas inscrite (`elysea-web:src/lib/publicFacts.ts:69@-00c9c89`). Aucun résultat de campagne : chaque chiffre de performance est à mesurer — campagne en cours.

I. Son problème

- **Il doit prouver la sécurité de ce qu'il livre, pas seulement l'affirmer.** Les éditeurs de modèles publient désormais des fiches datées par version avec leurs évaluations de sécurité [S-PLT-05] [S-PLT-06]. Un constructeur qui bâtit au-dessus d'un modèle hérite de cette attente sans en avoir les moyens.
- **Ses clients et leurs assureurs demandent des traces.** Les assureurs excluent l'IA générative de leurs polices parce qu'ils ne voient pas quels modèles leurs assurés font tourner, ni pour quelles applications : « Carriers cannot see which models their insureds are running and for what applications » [S-ASS-01].
- **Un garde-fou coûte à chaque requête.** « A guardrail is a tax on every request » : un garde-fou se juge sur trois axes, sécurité, sur-refus et latence [S-MES-11].
- **Les lois visent maintenant le comportement conversationnel.** En Californie, SB 243 impose aux opérateurs d'applications relationnelles un protocole de crise publié et des rapports annuels [S-EDU-05]. Dans l'UE, l'art. 50 de l'AI Act impose d'informer la personne qu'elle interagit avec une IA [S-DRT-01].

2. Ce qu'il doit comprendre, prouver et utiliser (état de l'art)

Il doit...	Ce que dit l'état de l'art	Source
Comprendre qu'une mesure se lit avec son incertitude	Statistiques « reported with estimated uncertainties » ; différences appariées	[S-MES-01] [S-MES-10]
Exiger des juges validés contre l'humain	Comparer à l'annotation humaine, plusieurs juges, accord inter-juges	[S-MES-01] [S-MES-08]
Exiger des taux corrigés du biais du juge	Correction par sensibilité et spécificité mesurées	[S-MES-09]
Regarder le sur-refus autant que la sécurité	Spécificité mesurée à côté du F1 et de la latence	[S-MES-11]
Attendre d'une infrastructure les standards d'une plateforme	API versionnée sans rupture non annoncée, journal des changements, journaux d'audit exportables, responsabilités écrites, canal de signalement des failles	[S-PLT-01] [S-PLT-02] [S-PLT-04] [S-PLT-07]

3. Objections fréquentes et réponses

Objection	Réponse	Pièce
Je suis lié à mon modèle.	Le cerveau route vers quatre familles de fournisseurs.	elysea-core:functions/src/core/byok/-byokAllowList.ts:10-15@a5b9780e
Je veux ma propre clé.	Le code de résolution de la clé du constructeur existe. Son activation n'est pas câblée : BYOK n'est pas disponible aujourd'hui et ne sera annoncé qu'une fois prouvé sur le déployé.	elysea-core:functions/src/core/byok/-byokKeyService.ts:2@a5b9780e · elysea-web:src/lib/publicFacts.ts:66-67@-00c9c89
Un client pourra-t-il désactiver la sécurité ?	Non. Un constructeur peut durcir, jamais affaiblir : toute tentative reçoit un refus 400.	elysea-core:functions/src/endpoints/-sdkSurface.ts:139@a5b9780e · elysea-sdk:GUIDE_INTEGRATION_CONSTRUCTEUR.-md:13@5ff4916
Ça va tout bloquer.	Le sur-refus est mesuré dans la campagne (banc fp70 : ELYSÉA ne doit pas être plus bloquant que le modèle nu). Résultat : à mesurer — campagne en cours.	elysea-tests-e2e:audits/PROTOCOLE_CAMPAGNE_-4BRAS_3TIIRS_SCELLE_2026-08-28.md:323@c9898dd3
Quelle latence ajoutée ?	À mesurer — campagne en cours. Aucun chiffre n'est donné avant.	—
Vos tests sont faits par vous.	Oui. Aucune validation tierce n'existe aujourd'hui. Les juges mécaniques et le panel de 3 juges sont validés sur des jeux tenus à l'écart (amendement R-70, statut proposé, branche de e2e #517 : elysea-tests-e2e:audits/AMENDEMENT_R70_-SENS_DECOUPE_STRUCTURELLE_2026-10-01.md:46@-67316397) ; validation juge/humain D23 assurée par l'annotation de Sébastien après le pilote. Le protocole a été préenregistré et scellé le 28/08, puis amendé ; le rescellement est un geste à venir, et 9 changements postérieurs au scellement attendent leur pièce de décision (holding-seb-docs:dossiers/RECONCILIATION_-PIECES_CAMPAGNE_2026-09-30.md:6@8560b37). Le banc public réannotable est décidé (01/10), pas encore construit.	elysea-tests-e2e:audits/PROTOCOLE_CAMPAGNE_-4BRAS_3TIIRS_SCELLE_2026-08-28.md:3@c9898dd3

4. Ce qu'ELYSÉA fait pour lui, avec la pièce

Fonction	Pièce	État
Contrôle avant le modèle (entrée nettoyée, garde OWASP LLMoi)	elysea-core:functions/src/core/security/-owaspInputGuard.ts:5@a5b9780e	Sur main
Contrôle après le modèle (limites Do vérifiées sur la réponse)	elysea-core:functions/src/core/pipeline/-validateLLMResponse.ts:1094@a5b9780e	Sur main
Les 4 interdits (domination, dépendance, substitution, manipulation) dans l'architecture, violation = réponse bloquée	elysea-core:functions/src/core/guardian/-checks/d0LimitCheck.ts:10-11@a5b9780e	Sur main

Crise décidée par le sens (vote LLM gradué), pas par mots-clés	elysea-core:functions/src/core/pipeline/-createPipeline.ts:1192@a5b9780e	Sur main
Ressources d'urgence publiques de 14 pays, 11 types d'urgence	elysea-core:functions/src/core/safety/-emergencyDirectory.ts:17-29@a5b9780e	Sur main. Aucun partenariat avec une ligne de crise.
Attestation par réponse, avec l'empreinte du build	elysea-core:functions/src/core/attestation/-interactionAttestor.ts:4@a5b9780e · elysea-core:functions/src/core/sdk/-sdkChatHandler.ts:160-161@a5b9780e	Sur main
Reconnaissance des émotions verrouillée désactivée, non modifiable par le constructeur	elysea-core:functions/src/core/sdk/-sdkAppService.ts:68@a5b9780e	Sur main
SDK @elysea/core	elysea-sdk:packages/core/package.json:2-3@-5ff4916	Dépôt en 0.9.0 ; npm public 0.8.0

Performance de chaque fonction : à mesurer — campagne en cours (fichier de résultats : `holding-seb-docs:depot-zenodo-2026-09-05/RESULTATS_CAMPAGNE.md:2@8560b37`).

5. Conformité qui le concerne

- **AI Act art. 50.1 et 50.2** : informer la personne qu'elle parle à une IA ; marquer les sorties dans un format lisible par machine. Applicable dès la mise sur le marché ; le report au 02/12/2026 ne vise que les systèmes déjà sur le marché avant le 02/08/2026 [S-DRT-01] [S-DRT-02]. **Décision** : le constructeur affiche l'information IA dès la première version ; ELYSÉA ne peut pas le faire à sa place puisqu'elle ne parle pas.
- **AI Act art. 5(1)(f)** : inférer les émotions au travail ou à l'école est interdit [S-DRT-01]. Le verrou P-01 retire ce risque de la couche ELYSÉA.
- **RGPD** : rôles à qualifier au cas par cas [S-DRT-07]. Projet de DPA art. 28 et projet d'accord art. 26 (mémoire inter-applications) : brouillons non signés (`holding-seb-docs:juridique/DPA_CONSTRUCTEURS_2026-09-10.md:1@-8560b37`, `holding-seb-docs:juridique/ACCORD_RESPONSABILITE_CONJOINTE_ART26_2026-09-08.md:1@8560b37`). **Décision** : aucune mise en production client sans DPA signé.
- **SB 243** (si l'application du constructeur entre dans sa définition) : protocole de crise publié, orientation vers une ligne de crise, rapports à partir du 01/07/2027 [S-EDU-05]. L'annuaire P-07 fournit les numéros publics ; le protocole publié reste au constructeur.

6. Parcours d'intégration

1. Lire le guide d'intégration (`elysea-sdk:GUIDE_INTEGRATION_CONSTRUCTEUR.md:13@5ff4916`).
2. Clé de test `sk_test_` : 500 interactions par mois (`elysea-web:src/lib/publicFacts.ts:36@00c9c89`).
3. Brancher le SDK, lire l'attestation renvoyée à chaque réponse (P-08).
4. Ajouter ses propres restrictions (durcir), jamais retirer (P-04).
5. Afficher l'information IA (art. 50) et publier son protocole de crise s'il est soumis à SB 243.
6. Signer DPA et, si mémoire inter-applications, accord art. 26 — à l'ouverture des ventes.
7. Passer en clé `sk_live_`.

7. Offre et tarif (brochures du 30/09, ventes fermées)

Offre	Prix	Pièce
Test	500 interactions / mois	elysea-web:src/lib/publicFacts.ts:36@00c9c89
Production, par tranche, sans fixe	2,50 € HT / UAM jusqu'à 5 000 ; 1,50 € de 5 001 à 25 000 ; 0,80 € au-delà	elysea-web:src/lib/publicFacts.ts:44-56@-00c9c89

8. Prochain pas concret

Ouvrir un compte de test et intégrer en environnement de test. Aucun engagement payant avant l'inscription de l'entité.

Manques à combler pour ce public (constatés le 01/10)

- Pas de security.txt ni de politique de divulgation (RFC 9116 exige Contact et Expires [S-PLT-07]) — aucune pièce sur main.
- Pas de journal des changements d'API versionné public au sens de [S-PLT-02].
- Aucun rapport d'audit tiers (SOC 2, ISO 27001) — les plateformes de référence en ont [S-PLT-01] [S-PLT-03].

Sources du dossier

S-PLT-01 · S-PLT-02 · S-PLT-03 · S-PLT-04 · S-PLT-05 · S-PLT-06 · S-PLT-07 · S-ASS-01 · S-MES-01 · S-MES-08 · S-MES-09 · S-MES-10 · S-MES-11 · S-DRT-01 · S-DRT-02 · S-DRT-07 · S-EDU-05