DOCTRINE ARCAN

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente
www.ariel-ia.ch

Table des matières

🟦 DOCTRINE ARCAN — Version 1.0

Suite cryptographique civile, souveraine & protectrice du vivant

---

1. Préambule

ARCAN n'est pas un logiciel de plus dans un monde saturé d'outils numériques.
Il a été pensé, conçu et construit pour répondre à un besoin fondamental :

Protéger les données des citoyens, des institutions et des organisations civiles, sans jamais les exposer à des tiers, des serveurs, des entreprises ou des États.

Nous vivons une époque où la donnée est devenue un actif stratégique, parfois manipulé sans transparence, parfois stocké sans consentement, parfois exigé sans nécessité.
Dans ce contexte, ARCAN apporte une réponse simple et sans ambiguïté :

La donnée privée doit le rester.
Point final.

ARCAN protège.
ARCAN ne surveille pas.
ARCAN ne trahit pas.

---

2. Principes fondamentaux

ARCAN repose sur quatre piliers indiscutables :

🟦 1) Confidentialité absolue

Ce qui est chiffré par l'utilisateur ne peut être lu
– ni par ARIEL-IA,
– ni par un fournisseur,
– ni par un tiers,
– ni par une autorité,
– ni par un attaquant.

🟦 2) Intégrité vérifiable

Toute altération, même minime, d'un scellé ARCAN est détectée.
L'outil refuse alors toute extraction.

🟦 3) Souveraineté totale

ARCAN fonctionne hors-ligne.
Sans cloud.
Sans compte.
Sans télémétrie.
Sans dépendance.

🟦 4) Usage exclusivement civil

ARCAN ne sera pas utilisé pour nuire, espionner, attaquer, opprimer ou surveiller.
Il est destiné à la protection, jamais à l'offensive.

---

3. Souveraineté numérique

ARCAN repose sur une conviction simple :

La sécurité ne peut pas dépendre d'une infrastructure que l'on ne contrôle pas.

C'est pourquoi :

- Aucun serveur n'est contacté.
- Aucune donnée ne transite.
- Aucune métadonnée n'est collectée.
- Aucun identifiant n'est généré.
- Aucun compte n'est nécessaire.

ARCAN appartient aux utilisateurs.
Pas à ARIEL-IA.
Pas à un fournisseur.
Pas à une plateforme.
Pas à une économie opaque.

C'est la définition même de la souveraineté numérique.

---

4. Cryptographie & Transparence

ARCAN s'appuie exclusivement sur des standards clairs, éprouvés et audités :

- **AES-256-GCM** pour la confidentialité et l'intégrité
- **PBKDF2-HMAC-SHA256** pour la dérivation de mot de passe
- **SHA-256** pour la chaîne d'intégrité

ARCAN ne contient :

- aucune porte dérobée,

- aucune clé maître,
- aucune possibilité de récupération,
- aucun canal caché.

Le fonctionnement est documenté et compréhensible.
La sécurité repose sur la *mathématique*, jamais sur l'opacité.

---

5. Intégrité & Confidentialité absolues

ARCAN respecte les règles suivantes :

✓ Le fichier original n'est jamais modifié

ARCAN crée un scellé, il ne touche pas au document d'origine.

✓ Toute tentative de modification entraîne un refus

Le moindre bit altéré invalide l'extraction.

✓ Trop de tentatives = verrouillage

Pour empêcher les attaques offline, ARCAN considère alors le scellé comme compromis.

✓ Mot de passe perdu = accès perdu

Ce n'est pas une limitation.
C'est une garantie.
Un scellé auquel on peut accéder sans mot de passe n'est pas un scellé :
c'est une illusion de sécurité.

---

6. Usage civil exclusif

ARCAN protège les organisations civiles :

- administrations publiques,
- cabinets juridiques,
- médecins,
- ingénieurs,
- journalistes,
- PME,
- fondations,
- institutions démocratiques.

ARCAN **ne sera jamais délivré** à :

- des armées,
- des organisations offensives,
- des acteurs cherchant à surveiller ou opprimer,
- des structures dont l'activité menace la démocratie ou le vivant.

L'éthique prime sur la technique.

---

7. Gouvernance ARIEL-IA

L'équipe d'ARIEL-IA applique une règle simple :

🟥 ARIEL-IA se réserve le droit de refuser toute demande de licence, sans fournir de justification.

Pourquoi ?

1. **Pour protéger la démocratie**
   Un outil cryptographique puissant doit rester aux mains d'acteurs responsables.
2. **Pour empêcher les dérives**
   Certains usages ne peuvent être soutenus ou cautionnés.
3. **Pour rester souverain**
   Aucun acteur externe ne peut exiger une licence.

La décision de délivrance ou de refus est **un acte souverain**, non négociable, non contestable.

---

8. Engagements vis-à-vis des utilisateurs

ARCAN garantit que :

- vos fichiers resteront **vôtres**,
- aucune donnée ne sera transmise,
- aucune porte dérobée ne sera créée,
- aucune pression ne fera évoluer la philosophie de l'outil,
- la confidentialité est un droit, pas un service.

ARCAN ne fera jamais :

- de suivi,
- de profilage,
- d'analyse de contenu,
- de stockage caché,
- d'exploitation des données,

- de récupération de mot de passe.

ARCAN n’est pas un jouet.
ARCAN est une responsabilité.

---

9. Responsabilités de l’utilisateur

Utiliser ARCAN implique :

- de choisir un mot de passe robuste,
- de protéger ce mot de passe,
- de gérer vos scellés avec sérieux,
- de comprendre que personne ne pourra les rouvrir à votre place.

ARCAN vous donne **la maîtrise totale**.
Cette maîtrise implique une part de responsabilité.

---

10. Conclusion

ARCAN a été conçu pour protéger ce qui doit l’être :
les données des citoyens, des familles, des institutions, des entreprises, des démocraties.

Dans un monde où trop de solutions demandent votre confiance sans jamais la mériter,
ARCAN propose l’inverse :

Il mérite la confiance, précisément parce qu’il ne vous en demande aucune.

Pas de collecte.
Pas de cloud.
Pas de surveillance.
Pas d’excuse.
Pas de compromis.

ARCAN n’est pas là pour plaire.
Il est là pour protéger.

Parce que la démocratie n’existe pas sans vie privée.
Parce que la liberté n’existe pas sans souveraineté.
Parce que les citoyens méritent un outil qui ne regarde pas ce qu’il protège.

ARCAN fait ce pourquoi il a été créé.
Uniquement cela.
Et cela suffit.