DOSSIER PRESSE

Adaptive Reliable Cryptographic Automation for Networks

Stéphane Valente

www.ariel-ia.ch

Sommaire

📜 **DOSSIER DE PRESSE — ARCAN** 2

1. Résumé exécutif 2

2. Principes fondateurs 2

3. Architecture cryptographique 2

4. Conception hors-ligne intégrale 3

5. Doctrine d'irréversibilité 3

6. ARCAN Reader & protection anti-bruteforce 4

7. Engagement envers le secteur public 4

8. Licences pour le secteur privé 4

9. Chaîne de production souveraine 5

10. Disponibilité & pré-réservations 5

11. À propos d'ARIEL-IA 5

12. Contact presse 5

🌐 https://www.ariel-ia.ch/arcan 5

📜 DOSSIER DE PRESSE — ARCAN

Adaptive Reliable Cryptographic Automation for Networks

ARIEL-IA — Suisse
Dossier de presse & aperçu technique
Version officielle — Décembre 2025

---

1. Résumé exécutif

ARCAN (Adaptive Reliable Cryptographic Automation for Networks) est une solution suisse de chiffrement souverain, conçue pour redonner un **contrôle total** sur les données sensibles.

ARCAN repose sur une cryptographie moderne de haut niveau et fonctionne **entièrement hors-ligne**, sans cloud, sans télémétrie, sans abonnement et sans aucune collecte de données.

ARCAN s'adresse aux **administrations publiques, entreprises, professionnels, journalistes, ONG et citoyens** qui exigent une maîtrise absolue de leurs informations.

ARCAN n'est pas un service.
ARCAN est un **outil**, qui appartient à celles et ceux qui l'utilisent.

---

2. Principes fondateurs

ARCAN est construit autour de principes non négociables :

- **Fonctionnement 100 % local**
  Aucune connexion Internet. Aucun serveur externe. Aucune API.
- **Aucune mémorisation de mot de passe**
  Les mots de passe ne sont jamais stockés, ni enregistrés, ni récupérables.
- **Licence perpétuelle**
  Paiement unique. Aucun abonnement. Aucun renouvellement.
- **Transparence cryptographique**
  Standards ouverts, éprouvés et internationalement reconnus.
- **Cadre éthique d'usage civil**
  Encadré par une licence stricte d'usage civil (A-CUL™).

---

3. Architecture cryptographique

ARCAN implémente une pile cryptographique robuste et moderne :

- **AES-256-GCM**
  Chiffrement authentifié avec vérification d'intégrité.
- **PBKDF2-HMAC-SHA256**
  200 000 itérations, salt aléatoire, dérivation par fichier.
- **Paramètres aléatoires uniques**
  Chaque opération utilise un salt et un nonce distincts.
- **Journal d'intégrité chaîné**
  Chaque action est inscrite dans un journal cryptographique lié à la précédente, rendant toute altération mathématiquement détectable.

Toute modification d'un container chiffré entraîne **un échec obligatoire du déchiffrement**.

---

4. Conception hors-ligne intégrale

ARCAN ne communique pas.

- Aucun cloud
- Aucun trafic réseau
- Aucune métadonnée
- Aucune télémétrie
- Aucun accès distant

ARCAN peut être utilisé sur :

- postes isolés
- environnements air-gap
- clés USB
- serveurs sécurisés
- infrastructures hors-ligne

Ce qui se passe dans ARCAN **reste dans ARCAN**.

---

5. Doctrine d'irréversibilité

ARCAN applique une règle fondamentale :

Si le mot de passe est perdu, le fichier est définitivement perdu.

Il n'existe :

- aucune clé maître
- aucun mécanisme de récupération
- aucune backdoor
- aucun accès privilégié

Ni les développeurs, ni ARIEL-IA, ni aucune autorité ne peuvent déchiffrer un fichier sans le mot de passe exact.

Ce n'est pas une limite.
C'est la garantie d'une souveraineté absolue.

---

6. ARCAN Reader & protection anti-bruteforce

Pour permettre aux destinataires d'ouvrir des fichiers chiffrés, ARCAN fournit un **ARCAN Reader** dédié.

Caractéristiques de sécurité :

- **Maximum de 10 tentatives de mot de passe**
- Blocage local irréversible du Reader au-delà
- Aucun impact sur le fichier chiffré
- Nouveau Reader requis après blocage

Ce mécanisme empêche toute automatisation d'attaque par force brute tout en conservant la portabilité des fichiers.

---

7. Engagement envers le secteur public

Dans un geste fondateur, **ARIEL-IA met ARCAN gratuitement à disposition** :

- de la Confédération suisse
- des administrations cantonales
- des administrations communales
- des journalistes et médias suisses

Cela représente environ **330 000 postes publics potentiels**, soit une valeur estimée à **environ 33 millions de francs**, volontairement offerte au service du bien commun et de la souveraineté numérique.

---

8. Licences pour le secteur privé

ARCAN est également proposé au secteur privé via des **licences professionnelles perpétuelles**, destinées notamment aux :

- PME et entreprises
- indépendants et professions libérales (avocats, médecins, fiduciaires, architectes, etc.)
- ONG et fondations
- institutions éducatives privées

Prix de référence : 100 CHF par poste (licence à vie)

Aucun abonnement.
Aucun coût caché.

---

9. Chaîne de production souveraine

ARCAN est produit via une **forge cryptographique entièrement hors-ligne** :

- machines de build jamais connectées à Internet
- compilation et signature hors-ligne
- génération des licences en environnement isolé
- absence totale de risque supply-chain

Chaque exécutable livré est traçable, vérifiable et authentique.

---

10. Disponibilité & pré-réservations

⏲️ **Lancement officiel : 1er janvier 2026 à 06h00 (CET)**

En raison du processus de production hors-ligne et du licensing manuel, ARCAN est distribué progressivement via un **système de pré-réservations**, ouvert dès le **15 décembre 2025**.

---

11. À propos d'ARIEL-IA

ARIEL-IA est une initiative suisse dédiée à :

- la souveraineté numérique
- la technologie éthique
- la cryptographie civile
- la sécurité centrée sur l'humain

ARCAN est développé en Suisse et régi par un cadre éthique strict.

---

12. Contact presse

ARIEL-IA — Communication
📧 press@ariel-ia.ch

🌐 https://www.ariel-ia.ch/arcan