ARCAN Recommandations

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente
www.ariel-ia.ch

Table des matières

Recommandations officielles ARIEL-IA 2
Bonnes pratiques d'usage d'ARCAN 2
Entreprises, administrations & organisations 2
1. Préambule 2
2. Recommandations d'usage 2
3. Accompagnement & responsabilité 3
4. Cas des volumes importants 3
5. Position finale 4
Recommandations officiellescycle d'utilisation d'ARCAN en entreprise 4
🧭 **Recommandations d'usage ARCAN** 5
Sécurité par la responsabilité, souveraineté par la rigueur 5
Préambule 5
1. Principe fondamental : responsabilité et sobriété 5
2. Organisation recommandée en entreprise et institution 6
Responsabilité humaine claire 6
Séparation des rôles 6
3. Architecture matérielle recommandée 6
La sécurité par le design, pas par l'illusion 6
Stockage externe dédié 6
Protection physique 6
4. Gestion des mots de passe : gravité et irréversibilité 7
Recommandations essentielles 7
5. ARCAN dans une architecture globale de sécurité 7
6. Ce que ARCAN ne fait volontairement pas 8
Conclusion 8
✔ **Statut du document** 8

Recommandations officielles ARIEL-IA

Bonnes pratiques d'usage d'ARCAN

Entreprises, administrations & organisations

---

1. Préambule

Chez **ARIEL-IA**, nous avons reçu certaines demandes de précommandes qualifiables de *fantaisistes* ou excessives.

Si notre objectif est bien de **diffuser ARCAN**, nous ne le ferons **jamais au détriment de nos clients**, de leur sécurité, ni de leur organisation interne.

Installer ARCAN sur l'ensemble des postes d'une organisation **peut être un choix**.
Ce n'est toutefois **pas notre recommandation**.

ARCAN est un outil de chiffrement civil puissant.
Sa valeur repose sur **un usage maîtrisé**, pas sur une généralisation aveugle.

---

2. Recommandations d'usage

De manière générale, **ARIEL-IA recommande** :

- **1 poste ARCAN maximum pour 10 employé·e·s**
- **Un·e responsable du chiffrement clairement nommé·e**
- **Une procédure interne formalisée**, incluant explicitement :
  - la conservation et la gestion des mots de passe
  - le cycle de vie des données
  - les moments précis où le chiffrement est appliqué

Il est **inutile et contre-productif** de chiffrer *tout, tout le temps*, sans cadre.

La sécurité ne s'obtient **pas** par une multiplication anarchique des chiffrements,
mais par un **cycle maîtrisé**, clairement défini et compris
(voir le schéma d'utilisation recommandé).

Notre intérêt n'est **pas** de vendre des licences à tout prix.
Notre intérêt est de **protéger les entreprises, les administrations, les données — et donc, in fine, les personnes**.

Créer un **chaos cryptographique** serait irresponsable, improductif
et **contraire à notre éthique**.

3. Accompagnement & responsabilité

ARCAN n'est **pas** un outil réservé aux ingénieur·e·s ou aux spécialistes du chiffrement.

La **Console ARCAN** a été conçue pour être utilisée par tout utilisateur ou utilisatrice,
sans compétences techniques avancées.

Cependant, certaines règles sont **non négociables** :

- Le mot de passe est sous la **responsabilité exclusive de l'utilisateur**
- **Aucune trace du mot de passe n'est conservée**
- **Personne ne peut déchiffrer un fichier ARCAN sans le mot de passe**
- Ni l'équipe de développement,
  ni ARIEL-IA,
  ni aucune autorité
  ne disposent d'un accès de récupération

👉 **Si le mot de passe est perdu, le fichier est définitivement perdu.**
👉 **Il n'existe aucun plan B.**

Cette irréversibilité est un **choix assumé**, au cœur de la sécurité d'ARCAN.

---

4. Cas des volumes importants

Seules les organisations disposant de **volumes importants de fichiers à chiffrer**
peuvent activer une **option d'exportation des mots de passe liés aux fichiers**.

Dans ce cas :

- la responsabilité de l'export incombe **exclusivement** à la ou aux personnes
  en charge du chiffrement
- la responsabilité de la conservation du fichier de mots de passe
  leur incombe **intégralement**
- **si ce fichier est perdu, les fichiers chiffrés sont perdus**

Là encore :
👉 **aucune récupération n'est possible**
👉 **aucune exception n'existe**

5. Position finale

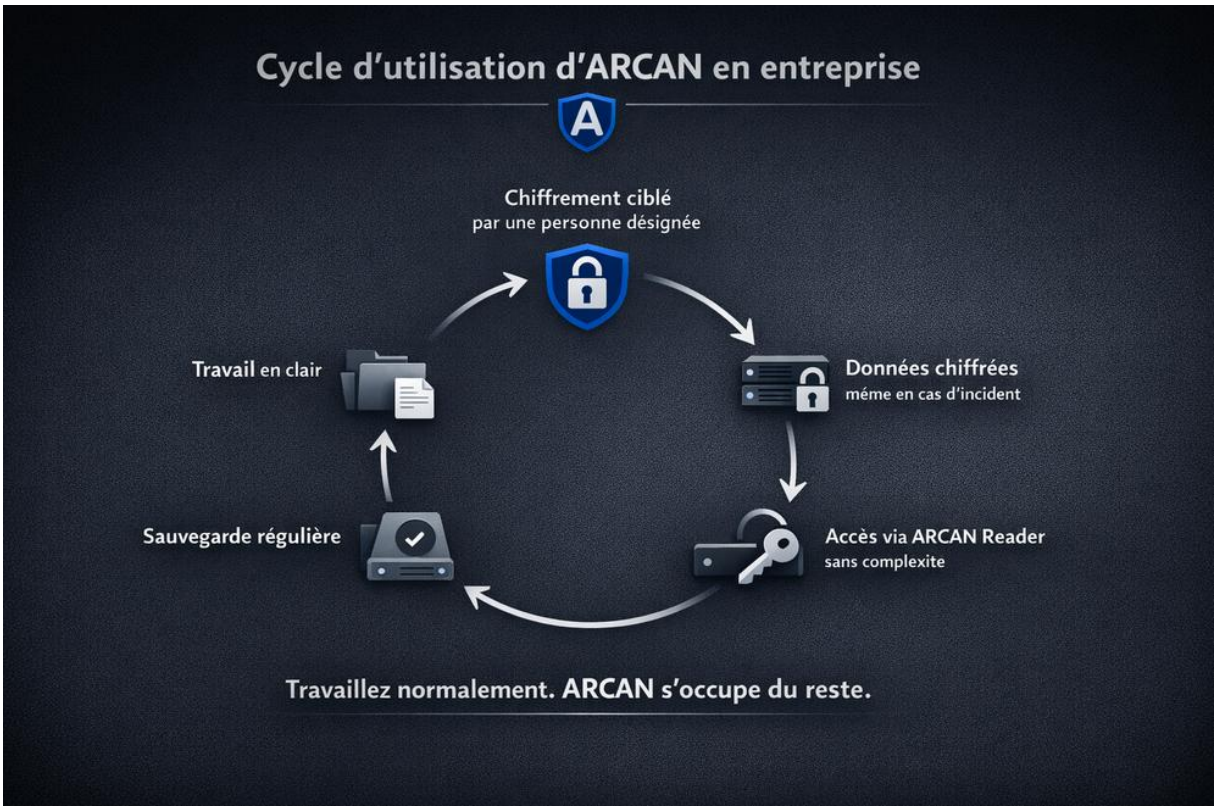
ARCAN est **sûr par conception**
et **mathématiquement robuste**.

ARCAN n'est **pas un jouet**.

Son efficacité repose autant sur :

- la qualité de sa cryptographie,
- que sur la **discipline humaine** de son utilisation.

Recommandations officielles cycle d'utilisation d'ARCAN en entreprise



Recommandations d’usage ARCAN

Sécurité par la responsabilité, souveraineté par la rigueur

Préambule

ARCAN est un outil de chiffrement souverain, conçu pour offrir une protection réelle et irréversible des données sensibles.

Il n’est ni un produit « clé en main »,
ni une solution magique,
ni un substitut à une architecture de sécurité réfléchie.

La sécurité qu’apporte ARCAN repose autant sur sa conception cryptographique que sur **la manière dont il est utilisé**.

Ces recommandations ont pour objectif de transmettre une **culture d’usage responsable**, condition indispensable à une souveraineté numérique authentique.

---

1. Principe fondamental : responsabilité et sobriété

ARCAN est un outil puissant.
À ce titre, son usage doit être **sobre, ciblé et maîtrisé**.

Multiplier les postes équipés d’ARCAN n’augmente pas mécaniquement la sécurité.
Au contraire, chaque instance supplémentaire crée un nouveau point de responsabilité humaine.

ARIEL-IA recommande explicitement de **ne pas généraliser l’installation d’ARCAN** à l’ensemble des collaborateurs.

Plus un outil est puissant, plus son usage doit être restreint.

ARCAN n’a pas vocation à devenir un bouton de confort distribué à tous.
Il est destiné à être confié à des personnes identifiées, formées et conscientes des implications de leurs actes.

2. Organisation recommandée en entreprise et institution

Responsabilité humaine claire

ARIEL-IA recommande :

- **une à deux personnes maximum par service ou entité**
- clairement désignées
- explicitement responsables du chiffrement et de ses conséquences

Ces personnes ne sont pas de simples opérateurs techniques.
Elles portent une **responsabilité fonctionnelle et organisationnelle**.

Séparation des rôles

Dans une organisation saine :

- la production des documents
- l'accès aux données
- et la responsabilité cryptographique

ne doivent pas nécessairement être confondus.

ARCAN s'inscrit dans une logique de **séparation des rôles**, afin de limiter les risques humains et organisationnels.

---

3. Architecture matérielle recommandée

La sécurité par le design, pas par l'illusion

La cybersécurité ne commence pas dans un logiciel.
Elle commence dans l'architecture.

ARIEL-IA recommande fortement :

Stockage externe dédié

- disques externes dédiés au stockage des données chiffrées
- supports hot-swap
- clés USB sécurisées
- aucun stockage long terme sur des postes utilisateurs standards

Protection physique

- conservation des supports dans des coffres ignifuges ou pare-feu
- séparation physique des lieux si possible
- inventaire clair et suivi des supports

ARCAN est conçu pour fonctionner dans des environnements sobres, isolés et maîtrisés.
Il ne remplace pas une architecture saine : il la renforce.

---

4. Gestion des mots de passe : gravité et irréversibilité

ARCAN applique une doctrine de sécurité stricte et volontairement irréversible.

- La perte du mot de passe entraîne la perte définitive des données
- Aucune récupération n'est possible
- Aucune exception n'existe
- Aucune autorité ne peut intervenir

Cette réalité doit être pleinement comprise **avant tout usage**.

Recommandations essentielles

- mots de passe forts et uniques
- jamais stockés sur des systèmes connectés
- aucune mémorisation logicielle automatique
- sauvegarde éventuelle uniquement hors ligne, sur supports physiques
- responsabilité pleinement assumée par l'organisation

ARCAN protège les données.
Il ne protège pas contre l'imprudence.

---

5. ARCAN dans une architecture globale de sécurité

ARCAN n'est pas une forteresse autonome.
Il est un **maillon** dans une stratégie globale.

ARIEL-IA recommande de l'intégrer dans une architecture comprenant notamment :

- politiques internes claires
- segmentation des données
- gestion des accès
- séparation des environnements
- discipline organisationnelle

La souveraineté numérique ne repose jamais sur un seul outil, mais sur la **cohérence de l'ensemble**.

6. Ce que ARCAN ne fait volontairement pas

Pour éviter toute ambiguïté, ARCAN ne propose volontairement pas :

- de récupération de mot de passe
- de stockage cloud
- de mécanisme de secours
- de backdoor
- d'automatisation aveugle
- de sécurité invisible ou implicite

Ces absences ne sont pas des manques.
Elles sont des **choix de conception**.

Conclusion

ARIEL-IA ne vend pas de la sécurité.

Nous transmettons :

- des outils sobres
- des pratiques responsables
- et une vision exigeante de la souveraineté numérique

ARCAN s'adresse aux organisations qui acceptent :

- la rigueur
- la discipline
- et la responsabilité qu'implique une protection réelle des données.

La souveraineté n'est jamais gratuite.
Elle se mérite par la cohérence des choix.

✔ Statut du document

Ce document constitue une **référence doctrinale officielle ARCAN**.
Tout développement, toute offre, toute interface et toute collaboration s'y alignent.