ARCAN Empfehlungen

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente
www.ariel-ia.ch

Zusammenfassung

DE DEUTSCHE VERSION

Offizielle Empfehlungen ARIEL-IA

Bewährte Praktiken für die Nutzung von ARCAN

Unternehmen, öffentliche Verwaltungen & Organisationen

---

1. Präambel

Bei ARIEL-IA haben wir bestimmte Vorbestellanfragen erhalten, die als fantasievoll oder überzogen einzustufen sind.
Auch wenn es unser Ziel ist, ARCAN zu verbreiten, werden wir dies **niemals** auf Kosten unserer Kunden, ihrer Sicherheit oder ihrer internen Organisation tun.

Die Installation von ARCAN auf allen Arbeitsplätzen einer Organisation **kann** eine Entscheidung sein.
Sie ist jedoch **nicht unsere Empfehlung**.

ARCAN ist ein leistungsfähiges ziviles Verschlüsselungswerkzeug.
Sein Wert beruht auf einer **kontrollierten und beherrschten Nutzung**, nicht auf einer blinden Verallgemeinerung.

---

2. Nutzungsempfehlungen

Grundsätzlich empfiehlt ARIEL-IA:

- **Maximal 1 ARCAN-Arbeitsplatz pro 10 Mitarbeitende**
- **Eine klar benannte verantwortliche Person für die Verschlüsselung**
- **Ein formalisierter interner Prozess**, der ausdrücklich umfasst:
    - die Aufbewahrung und Verwaltung von Passwörtern
    - den Lebenszyklus der Daten
    - die genau definierten Zeitpunkte, zu denen Verschlüsselung angewendet wird

Alles jederzeit und ohne Rahmen zu verschlüsseln ist unnötig und kontraproduktiv.

Sicherheit entsteht nicht durch eine anarchische Vervielfachung von Verschlüsselungen, sondern durch einen **kontrollierten, klar definierten und verstandenen Zyklus**
(siehe empfohlenes Nutzungsschema).

Unser Interesse besteht nicht darin, um jeden Preis Lizenzen zu verkaufen.
Unser Interesse ist es, Unternehmen, Verwaltungen und Daten zu schützen —
und damit letztlich die Menschen.

Ein kryptographisches Chaos zu erzeugen wäre verantwortungslos, ineffektiv
und widerspräche unserer Ethik.

---

3. Begleitung & Verantwortung

ARCAN ist kein Werkzeug, das ausschließlich Ingenieur:innen oder
Verschlüsselungsspezialist:innen vorbehalten ist.
Die ARCAN-Konsole wurde so konzipiert, dass sie von jeder Nutzerin und jedem Nutzer
ohne fortgeschrittene technische Kenntnisse verwendet werden kann.

Bestimmte Regeln sind jedoch nicht verhandelbar:

- Das Passwort liegt in der **ausschließlichen Verantwortung der Nutzerin oder des Nutzers**
- Es wird **keine Spur des Passworts** gespeichert
- Niemand kann eine ARCAN-Datei ohne Passwort entschlüsseln
- Weder das Entwicklungsteam,
  noch ARIEL-IA,
  noch irgendeine Behörde
  verfügen über einen Wiederherstellungszugang

👉 Geht das Passwort verloren, ist die Datei endgültig verloren.
👉 Es gibt keinen Plan B.

Diese Irreversibilität ist eine bewusste Entscheidung
und steht im Zentrum der Sicherheit von ARCAN.

---

4. Umgang mit großen Datenmengen

Nur Organisationen mit großen Mengen zu verschlüsselnder Dateien
können eine Option zum Export der dateibezogenen Passwörter aktivieren.

In diesem Fall:

- liegt die Verantwortung für den Export **ausschließlich** bei den für die Verschlüsselung zuständigen Personen
- liegt die Verantwortung für die Aufbewahrung der Passwortdatei vollständig bei ihnen
- geht diese Datei verloren, sind auch die verschlüsselten Dateien verloren

Auch hier gilt:
👉 keine Wiederherstellung ist möglich
👉 es gibt keinerlei Ausnahme

5. Abschließende Position

ARCAN ist **sicher durch Design**
und mathematisch robust.

ARCAN ist **kein Spielzeug**.

Seine Wirksamkeit beruht ebenso auf:

- der Qualität seiner Kryptographie,
- wie auf der **menschlichen Disziplin** bei seiner Nutzung.

Offizielle Empfehlungen — ARCAN-Nutzungszyklus in Organisationen

🧭 ARCAN Nutzungsempfehlungen

Sicherheit durch Verantwortung, Souveränität durch Konsequenz

Präambel

ARCAN ist ein souveränes Verschlüsselungswerkzeug, das entwickelt wurde, um einen realen und irreversiblen Schutz sensibler Daten zu gewährleisten.
Es ist weder ein schlüsselfertiges Produkt,
noch eine magische Lösung,
noch ein Ersatz für eine durchdachte Sicherheitsarchitektur.

Die von ARCAN gebotene Sicherheit beruht ebenso auf seinem kryptographischen Design wie auf der Art und Weise seiner Nutzung.

Diese Empfehlungen sollen eine Kultur der verantwortungsvollen Nutzung vermitteln — eine unverzichtbare Voraussetzung für echte digitale Souveränität.

---

1. Grundprinzip: Verantwortung und Zurückhaltung

ARCAN ist ein leistungsstarkes Werkzeug.
Daher muss seine Nutzung zurückhaltend, gezielt und kontrolliert erfolgen.

Die Vervielfachung von mit ARCAN ausgestatteten Arbeitsplätzen erhöht die Sicherheit nicht automatisch.
Im Gegenteil: Jede zusätzliche Instanz schafft einen neuen Punkt menschlicher Verantwortung.

ARIEL-IA empfiehlt ausdrücklich, ARCAN **nicht** auf alle Mitarbeitenden auszurollen.
Je mächtiger ein Werkzeug ist, desto stärker sollte sein Einsatz begrenzt sein.

ARCAN ist nicht dazu bestimmt, ein Komfortknopf für alle zu werden.
Es soll identifizierten, geschulten Personen anvertraut werden,
die sich der Konsequenzen ihres Handelns bewusst sind.

---

2. Empfohlene Organisation in Unternehmen und Institutionen

Klare menschliche Verantwortung
ARIEL-IA empfiehlt:

- ein bis maximal zwei Personen pro Abteilung oder Einheit
- klar benannt
- ausdrücklich verantwortlich für die Verschlüsselung und deren Folgen

Diese Personen sind keine bloßen technischen Bediener.
Sie tragen eine **funktionale und organisatorische Verantwortung**.

Trennung der Rollen
In einer gesunden Organisation müssen:

- die Erstellung von Dokumenten
- der Zugriff auf Daten
- die kryptographische Verantwortung

nicht zwangsläufig zusammenfallen.

ARCAN folgt einer Logik der Rollentrennung,
um menschliche und organisatorische Risiken zu begrenzen.

---

3. Empfohlene Hardware-Architektur

Sicherheit durch Design, nicht durch Illusion

Cybersicherheit beginnt nicht in einer Software.
Sie beginnt in der Architektur.

ARIEL-IA empfiehlt dringend:

Dedizierte externe Speicher

- externe Datenträger ausschließlich für verschlüsselte Daten
- Hot-Swap-Medien
- gesicherte USB-Schlüssel
- keine Langzeitspeicherung auf Standard-Arbeitsplätzen

Physischer Schutz

- Aufbewahrung der Datenträger in feuerfesten oder brandsicheren Tresoren
- physische Trennung der Standorte, wenn möglich
- klare Inventarisierung und Nachverfolgung der Datenträger

ARCAN ist für den Einsatz in nüchternen, isolierten und kontrollierten Umgebungen konzipiert.
Es ersetzt keine gesunde Architektur — es verstärkt sie.

---

4. Passwortmanagement: Ernsthaftigkeit und Irreversibilität

ARCAN verfolgt eine strikte und bewusst irreversible Sicherheitsdoktrin:

- Der Verlust des Passworts führt zum endgültigen Verlust der Daten
- Keine Wiederherstellung ist möglich
- Es gibt keine Ausnahme

- Keine Autorität kann eingreifen

Diese Realität muss vor jeder Nutzung vollständig verstanden werden.

Zentrale Empfehlungen

- starke und einzigartige Passwörter
- niemals auf vernetzten Systemen gespeichert
- keine automatische softwareseitige Speicherung
- optionale Sicherung ausschließlich offline auf physischen Medien
- volle Verantwortung liegt bei der Organisation

ARCAN schützt Daten.
Es schützt nicht vor Unachtsamkeit.

---

5. ARCAN innerhalb einer globalen Sicherheitsarchitektur

ARCAN ist keine autonome Festung.
Es ist ein Baustein innerhalb einer Gesamtstrategie.

ARIEL-IA empfiehlt die Einbettung in eine Architektur, die insbesondere umfasst:

- klare interne Richtlinien
- Datensegmentierung
- Zugriffsmanagement
- Trennung der Umgebungen
- organisatorische Disziplin

Digitale Souveränität beruht niemals auf einem einzelnen Werkzeug,
sondern auf der Kohärenz des Ganzen.

---

6. Was ARCAN bewusst nicht tut

Zur Vermeidung jeglicher Mehrdeutigkeit bietet ARCAN bewusst keine:

- Passwortwiederherstellung
- Cloud-Speicherung
- Notfall- oder Rettungsmechanismen
- Backdoors
- blinde Automatisierung
- unsichtbare oder implizite Sicherheit

Diese Abwesenheiten sind keine Mängel.
Sie sind **bewusste Designentscheidungen**.

Schlussfolgerung

ARIEL-IA verkauft keine Sicherheit.
Wir vermitteln:

- nüchterne Werkzeuge
- verantwortungsvolle Praktiken
- und eine anspruchsvolle Vision digitaler Souveränität

ARCAN richtet sich an Organisationen, die bereit sind:

- Strenge
- Disziplin
- und die Verantwortung zu übernehmen, die echter Datenschutz erfordert

Souveränität ist niemals kostenlos.
Sie wird durch kohärente Entscheidungen verdient.

✔ **Dokumentenstatus**
Dieses Dokument stellt eine offizielle doktrinäre Referenz von ARCAN dar.
Alle Entwicklungen, Angebote, Schnittstellen und Kooperationen richten sich danach.