

# ARCAN





## DOSSIER PRESSE

*Adaptive Reliable Cryptographic Automation for Networks*

Stéphane Valente

[www.ariel-ia.ch](http://www.ariel-ia.ch)

## Inhaltsverzeichnis

 <b>PRESSEDossier — ARCAN</b> .....	2
<b>1. Zusammenfassung</b> .....	2
<b>2. Grundprinzipien</b> .....	2
<b>3. Kryptografische Architektur</b> .....	2
<b>4. Konsequentes Offline-Design</b> .....	3
<b>5. Irreversibilitäts-Doktrin</b> .....	3
<b>6. ARCAN Reader &amp; Schutz vor Brute-Force-Angriffen</b> .....	4
<b>7. Engagement für den öffentlichen Sektor</b> .....	4
<b>8. Lizenzen für den privaten Sektor</b> .....	4
<b>9. Souveräne Produktionskette</b> .....	5
<b>10. Verfügbarkeit &amp; Vorregistrierung</b> .....	5
<b>11. Über ARIEL-IA</b> .....	5
<b>12. Pressekontakt</b> .....	5
 <a href="https://www.ariel-ia.ch/arcan">https://www.ariel-ia.ch/arcan</a> .....	5



# PRESSEDossier — ARCAN

Adaptive Reliable Cryptographic Automation for Networks

ARIEL-IA — Schweiz

Presseunterlagen & technischer Überblick

Offizielle Version — Dezember 2025

---

## 1. Zusammenfassung

ARCAN (Adaptive Reliable Cryptographic Automation for Networks) ist eine in der Schweiz entwickelte, souveräne Verschlüsselungslösung, die die **volle Kontrolle über sensible Daten** wieder in die Hände ihrer Nutzerinnen und Nutzer legt.

ARCAN basiert auf moderner Hochsicherheitskryptografie und funktioniert **vollständig offline** — ohne Cloud, ohne Telemetrie, ohne Abonnement und ohne jegliche Datensammlung.

ARCAN richtet sich an **öffentliche Verwaltungen, Unternehmen, Fachpersonen, Journalistinnen und Journalisten, NGOs sowie Bürgerinnen und Bürger**, die höchste Anforderungen an Datensouveränität stellen.

ARCAN ist kein Dienst.

ARCAN ist ein **Werkzeug**, das seinen Nutzerinnen und Nutzern gehört.

---

## 2. Grundprinzipien

ARCAN beruht auf klar definierten, nicht verhandelbaren Prinzipien:

- **100 % lokaler Betrieb**  
Keine Internetverbindung. Keine externen Server. Keine APIs.
  - **Keine Speicherung von Passwörtern**  
Passwörter werden weder gespeichert noch protokolliert oder wiederhergestellt.
  - **Unbefristete Lizenz**  
Einmalige Lizenz. Kein Abonnement. Keine Verlängerung.
  - **Kryptografische Transparenz**  
Ausschließlich offene, international anerkannte Standards.
  - **Ethischer Rahmen für zivile Nutzung**  
Geregelter Einsatz durch eine strikte Civil-Use-Lizenz (A-CUL™).
- 

## 3. Kryptografische Architektur

ARCAN implementiert eine robuste und moderne kryptografische Architektur:

- **AES-256-GCM**  
Authentifizierte Verschlüsselung mit Integritätsprüfung.
- **PBKDF2-HMAC-SHA256**  
200'000 Iterationen, zufälliger Salt, schlüsselableitung pro Datei.
- **Einzigartige Zufallsparameter**  
Jede Verschlüsselung verwendet einen eigenen Salt und Nonce.
- **Verkettetes Integritätsjournal**  
Jede Aktion wird in einem kryptografisch verketteten Journal erfasst. Manipulationen sind mathematisch nachweisbar.

Jede Veränderung eines verschlüsselten Containers führt **zwangsläufig zu einem Entschlüsselungsfehler**.

---

## 4. Konsequentes Offline-Design

ARCAN kommuniziert nicht.

- Keine Cloud
- Kein Netzwerkverkehr
- Keine Metadaten
- Keine Telemetrie
- Kein Fernzugriff

ARCAN kann eingesetzt werden auf:

- isolierten Arbeitsstationen
- Air-Gap-Umgebungen
- USB-Datenträgern
- gesicherten Servern
- vollständig offline betriebenen Infrastrukturen

Was in ARCAN geschieht, **bleibt in ARCAN**.

---

## 5. Irreversibilitäts-Doktrin

ARCAN folgt einer klaren Sicherheitsregel:

**Geht das Passwort verloren, ist die Datei dauerhaft verloren.**

Es existieren:

- kein Master-Key
- keine Wiederherstellungsfunktion
- keine Backdoor
- kein privilegierter Zugriff

Weder die Entwickler noch ARIEL-IA oder irgendeine Behörde können eine Datei ohne das exakte Passwort entschlüsseln.

Dies ist keine Einschränkung.  
Es ist die Garantie absoluter Datensouveränität.

---

## 6. ARCAN Reader & Schutz vor Brute-Force-Angriffen

Für den Empfang verschlüsselter Dateien stellt ARCAN einen dedizierten **ARCAN Reader** zur Verfügung.

Sicherheitsmerkmale:

- **Maximal 10 Passwortversuche**
- Lokale, irreversible Sperrung des Readers bei Überschreitung
- Keine Auswirkung auf die verschlüsselte Datei selbst
- Neuer Reader erforderlich nach Sperrung

Dieses Konzept verhindert automatisierte Brute-Force-Angriffe und bewahrt gleichzeitig die Portabilität der Daten.

---

## 7. Engagement für den öffentlichen Sektor

Als Gründungsakt stellt **ARIEL-IA ARCAN kostenlos zur Verfügung** für:

- die Schweizerische Bundesverwaltung
- kantonale Verwaltungen
- kommunale Verwaltungen
- Schweizer Medien und Journalistinnen/Journalisten

Dies entspricht rund **330'000 potenziellen Arbeitsplätzen im öffentlichen Sektor** und einem geschätzten Gegenwert von **rund 33 Millionen Schweizer Franken**, bewusst gespendet im Dienst des Gemeinwohls und der digitalen Souveränität.

---

## 8. Lizenzen für den privaten Sektor

ARCAN ist auch für den privaten Sektor über **unbefristete professionelle Lizenzen** erhältlich, insbesondere für:

- KMU und Unternehmen
- Selbstständige und freie Berufe (Rechtsanwälte, Ärztinnen, Treuhänder, Architekten usw.)
- NGOs und Stiftungen
- private Bildungsinstitutionen

**Referenzpreis:** CHF 100 pro Arbeitsplatz (unbefristete Lizenz)

Kein Abonnement.

Keine versteckten Kosten.

---

## 9. Souveräne Produktionskette

ARCAN wird in einer **vollständig offline betriebenen kryptografischen Forge** hergestellt:

- Build-Systeme ohne Internetverbindung
- Offline-Kompilierung und -Signierung
- Lizenzgenerierung in isolierten Umgebungen
- Kein Supply-Chain-Risiko

Jede ausgelieferte Anwendung ist überprüfbar, authentisch und nachvollziehbar.

---

## 10. Verfügbarkeit & Vorregistrierung

 **Offizieller Start: 1. Januar 2026 um 06:00 Uhr (CET)**

Aufgrund der offlinebasierten Produktion und der manuellen Lizenzierung erfolgt die Verteilung schrittweise über ein **Vorregistrierungssystem**, geöffnet ab **15. Dezember 2025**.

---

## 11. Über ARIEL-IA

**ARIEL-IA** ist eine Schweizer Initiative mit Fokus auf:


- digitale Souveränität
- ethische Technologie
- zivile Kryptografie
- menschenzentrierte Sicherheit

ARCAN wird in der Schweiz entwickelt und unterliegt einem strengen ethischen Rahmen.

---

## 12. Pressekontakt

**ARIEL-IA — Kommunikation**

 [press@ariel-ia.ch](mailto:press@ariel-ia.ch)

 <https://www.ariel-ia.ch/arcan>