

ARCAN





PRESS DOSSIER — ARCAN

Adaptive Reliable Cryptographic Automation for Networks

Stéphane Valente

www.ariel-ia.ch

Summary

 PRESS DOSSIER — ARCAN	2
1. Executive Summary	2
2. Core Principles	2
3. Cryptographic Architecture	2
4. Offline-Only by Design	3
5. Irreversibility Doctrine	3
6. ARCAN Reader & Anti-Bruteforce Protection	4
7. Public Sector Commitment	4
8. Private Sector Licensing	4
9. Sovereign Production Chain	5
10. Availability & Pre-Reservations	5
11. About ARIEL-IA	5
12. Press Contact	5
 https://www.ariel-ia.ch/arcan	5



PRESS DOSSIER — ARCAN

Adaptive Reliable Cryptographic Automation for Networks

ARIEL-IA — Switzerland

Press Release & Technical Overview

(Version EN · Official · December 2025)

1. Executive Summary

ARCAN (Adaptive Reliable Cryptographic Automation for Networks) is a Swiss-developed cryptographic solution designed to restore full digital sovereignty over sensitive data.

ARCAN provides **state-of-the-art encryption**, operating **entirely offline**, without cloud services, without telemetry, without subscriptions, and without any form of hidden data collection.

It is built for **public administrations, enterprises, professionals, journalists, NGOs, and citizens** who require absolute control over their data.

ARCAN is not a service.

ARCAN is a tool — owned by its users.

2. Core Principles

ARCAN is built upon five non-negotiable principles:

- **100% local operation**
No internet connection. No external servers. No APIs.
 - **No password storage**
Passwords are never saved, cached, logged, or recoverable.
 - **Permanent license**
One-time license. No subscriptions. No renewals.
 - **Cryptographic transparency**
Based exclusively on open, internationally recognized standards.
 - **Ethical civil use**
Governed by a strict civil-use license (A-CUL™).
-

3. Cryptographic Architecture

ARCAN implements a robust and modern cryptographic stack:

- **AES-256-GCM**
Authenticated encryption with integrity verification.
- **PBKDF2-HMAC-SHA256**
200,000 iterations, random salt, per-file derivation.
- **Randomized parameters**
Unique salt and nonce for every encryption operation.
- **Chained integrity journal**
Each action is recorded in a cryptographically chained log, making tampering mathematically detectable.

Any modification of an encrypted container results in a mandatory decryption failure.

4. Offline-Only by Design

ARCAN does not communicate.

- No cloud
- No background traffic
- No metadata leakage
- No telemetry
- No analytics
- No remote access

ARCAN can operate on:

- isolated workstations
- air-gapped environments
- USB keys
- secure servers
- offline infrastructures

What happens inside ARCAN **stays inside ARCAN**.

5. Irreversibility Doctrine

ARCAN enforces a strict security doctrine:

If the password is lost, the file is lost. Permanently.

There is:

- no master key
- no recovery mechanism
- no backdoor
- no privileged access

Not even the developers of ARCAN can decrypt a file without the exact password.

This is not a limitation.

It is the guarantee of absolute sovereignty.

6. ARCAN Reader & Anti-Bruteforce Protection

To allow recipients to open encrypted files, ARCAN provides a dedicated **ARCAN Reader**.

Security features include:

- **Maximum of 10 password attempts**
- Local, irreversible lock after limit is reached
- No impact on the encrypted file itself
- New Reader required after lock

This prevents brute-force attacks while preserving file portability.

7. Public Sector Commitment

As a founding gesture, **ARIEL-IA offers ARCAN free of charge** to:

- Swiss Federal Administration
- Cantonal administrations
- Municipal administrations
- Swiss journalists and media organizations

This represents approximately **330,000 potential public sector workstations**, corresponding to an estimated value of **CHF 33 million**, voluntarily donated in service of the public good and digital sovereignty.

8. Private Sector Licensing

ARCAN is also available to private organizations through **permanent professional licenses**, including:

- SMEs and enterprises
- Independent professionals (lawyers, doctors, architects, accountants)
- NGOs and foundations
- Educational institutions

Reference price: CHF 100 per workstation (perpetual license)

No subscriptions.
No hidden costs.

9. Sovereign Production Chain

ARCAN is built using a **fully offline cryptographic forge**:

- Build machines never connected to the internet
- Offline compilation and signing
- License generation in isolated environments
- No supply-chain exposure

This guarantees the integrity and authenticity of every delivered executable.

10. Availability & Pre-Reservations

Official release:

 **January 1st, 2026 — 06:00 CET**

Due to the offline production and manual licensing process, ARCAN is distributed progressively through a **pre-reservation system** starting December 15th, 2025.

11. About ARIEL-IA

ARIEL-IA is a Swiss initiative dedicated to:

- digital sovereignty
- ethical technology
- civil cryptography
- human-centric security

ARCAN is developed in Switzerland and governed by a strict ethical framework.

12. Press Contact

ARIEL-IA — Communication

 press@ariel-ia.ch

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