Stéphane Valente

ARCAN

ARCAN Reader User Guide

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente

www.ariel-ia.ch

Summary

📘 ARCAN Reader — User Guide (EN)

1. Role of ARCAN Reader

ARCAN Reader is the public tool used to read / decrypt files protected by ARCAN (.arcsealed).
Its role is deliberately unique and strict:

- open an ARCAN container
- attempt decryption using the provided password
- restore the file **only if all conditions are met**

👉 ARCAN Reader does not protect anything by itself.
Security relies exclusively on ARCAN encryption and the password.

---

2. Starting ARCAN Reader

- Launch **ARCAN_Reader.exe** (or the portable version)
- No installation required
- No network access
- No Internet connection
- No account, no licence to enter

ARCAN Reader operates entirely offline.

---

3. Interface — step-by-step operation

The ARCAN Reader interface is intentionally minimal.

Step 1 — File selection

- Click **Browse**
- Select a `.arcsealed` file

Step 2 — Output folder

- Choose the folder where the decrypted file will be written
- ARCAN Reader can write **only** inside this folder

👉 Any attempt to write outside this perimeter is refused.

Step 3 — Password

- Enter the exact password used during encryption
- The password is:
    o not stored
    o not memorised
    o not transmitted
    o not retained

Step 4 — Decryption

- Click **Decrypt**
- Two possible outcomes:

✅ **Success**
The file is restored in the selected folder.

❌ **Refusal**
Decryption is impossible in this environment
(incorrect password, altered file, or non-compliant format).

No exploitable information is provided.

---

4. Security and deliberately strict behaviour

ARCAN Reader applies a **hostile-by-default** posture:

- every file is considered untrusted
- any inconsistency results in refusal
- zero tolerance
- no bypass
- no "try anyway" mode

👉 ARCAN Reader either works — or it stops.

5. Password attempts

- The number of attempts is deliberately limited
- After several failures, ARCAN Reader locks permanently

👉 In case of lockout:

- download ARCAN Reader again
- retry with the correct password

This mechanism is a **UX deterrent**, not a cryptographic security promise.

6. What ARCAN Reader will never do

ARCAN Reader:

- ❌ does not recover passwords
- ❌ does not offer "lenient" compatibility
- ❌ never connects to the Internet
- ❌ sends no telemetry
- ❌ does not auto-update
- ❌ embeds no secret key
- ❌ does not repair damaged files

Lost password = permanent loss of the file.
This is a **security guarantee**, not a limitation.

---

7. Recommended best practices

- Store the password separately from the `.arcsealed` file
- Use a long passphrase
- Verify the origin of the ARCAN file
- Download ARCAN Reader only from an official source

---

8. Summary

- ARCAN Reader is a **read-only** tool
- It is public, intentionally simple and strict
- It makes no illusory promises
- Security relies exclusively on the password

ARCAN Reader is designed as a **compromise**.
Its compromise never compromises your data.