ARCAN — OFFICIAL DOCTRINE

Adaptive Reliable Cryptographic Automation for Networks

Stéphane Valente
www.ariel-ia.ch

Summary

🔵 ARCAN — OFFICIAL DOCTRINE

Version 1.0

Adaptive Reliable Cryptographic Automation for Networks
ARIEL-IA — Switzerland

---

1. ARCAN is not a disguise.

ARCAN does not obscure reality.
ARCAN does not simulate security.
ARCAN **is** security.

It is not a cosmetic layer.
It is not a promise.
It is not a marketing construct.

ARCAN is a **cryptographic vault**, absolute by design.

---

2. Lose the password → lose the file.

Without exception.
Without recovery.
Without support.
Without appeal.

ARCAN does not provide:

- password recovery
- reset mechanisms
- backup keys
- emergency access
- master credentials

The password **is the life of the file**.
If it disappears, the file disappears with it.

This rule is irreversible and intentional.

---

3. No one can access the data. Ever.

There is no privileged access.

Not for:

- the developer
- the organization
- the infrastructure operator
- the software publisher
- any authority
- any institution
- any third party

There is no exception.
There will never be one.

Data sovereignty means **exclusive ownership** by the holder of the password.

---

4. Even infinite computing power changes nothing.

ARCAN does not rely on tricks.
It does not rely on shortcuts.
It does not rely on secrecy.

It relies on:

- modern cryptographic standards
- mathematically proven constructions
- strong randomness
- non-optimizable key derivation

No amount of GPUs, clusters, or future hardware can extract a single character without the correct password.

This is not an estimate.
It is a mathematical reality.

---

5. No server. No dependency. No surveillance.

ARCAN does not communicate.

- No cloud
- No server
- No API
- No telemetry
- No metadata collection
- No network traffic

ARCAN does not listen.
ARCAN does not observe.
ARCAN does not report.

Files may be stored:

- on local disks
- on USB keys
- on private servers
- in offline archives
- in physically secured locations

The choice belongs **only** to the data owner.

---

6. Cryptography over convenience.

ARCAN deliberately rejects convenience features that weaken security.

There is:

- no synchronization
- no recovery service
- no central account
- no “forgot password”
- no hidden assistance

Usability must **never** compromise sovereignty.

ARCAN favors responsibility over comfort.

---

7. Offline by design, not by configuration.

ARCAN is not “offline-capable”.
ARCAN is **offline-native**.

No option needs to be enabled.
No setting can disable this behavior.

ARCAN cannot be turned into a connected system.

---

8. Integrity is mandatory, not optional.

Every encryption operation produces:

- a sealed container

- an authenticated payload
- a chained integrity journal

Any alteration — even a single bit — results in a **mandatory failure**.

There is no partial success.
There is no degraded mode.

Integrity is absolute.

---

9. Anti-bruteforce is enforced at the edge.

ARCAN provides a dedicated **ARCAN Reader** for recipients.

This Reader enforces:

- a strict limit of **10 password attempts**
- a local, irreversible lock after exhaustion
- no impact on the encrypted file itself

The Reader can be replaced.
The file cannot be weakened.

---

10. Civil use only.

ARCAN is governed by a strict **Civil-Use License (A-CUL™)**.

ARCAN must not be used for:

- military applications
- offensive cyber operations
- mass surveillance
- intrusive monitoring
- coercive control systems

Strong cryptography requires strong ethics.

---

11. A mandatory warning to users.

ARCAN must always display the following warning before encryption:

“ARCAN is not a toy.
If you lose the password, the file is permanently lost.
No recovery is possible.

No assistance can help you.
Confirm that you understand."

Encryption cannot proceed until this acknowledgment is confirmed.

This is not negotiable.

---

12. Sovereign production is part of security.

ARCAN is produced using:

- offline build machines
- isolated signing environments
- manual license generation
- no connected supply chain

Security does not stop at cryptography.
It includes the **entire production chain**.

---

13. ARCAN is a responsibility.

ARCAN empowers users — and holds them accountable.

With sovereignty comes responsibility.
With freedom comes discipline.

ARCAN does not protect users from themselves.
It protects data from everyone else.

---

14. Final statement

ARCAN does not ask for trust.
ARCAN removes the need for trust.

No authority is required.
No permission is needed.
No dependency exists.

ARCAN stands on mathematics, ethics, and sovereignty.

That is its doctrine.
That is its boundary.
That is its promise.