



ARCAN Console User Guide

Suite cryptographique civile, souveraine & protectrice du vivant

Stéphane Valente

www.ariel-ia.ch

Summary

 ARCAN Console — User Guide	2
1. Role of the ARCAN Console	2
2. Starting the Console	2
3. Interface — Overview	2
 Central area — Files & folders (main tool)	2
 Side area — QuickSeal (auxiliary tool)	3
 Bottom area — Cryptographic actions	3
4. .seal.log journals — verification	4
5. What the Console never does	4
6. Recommended best practices	4
7. Summary	5
Appendix	5



ARCAN Console — User Guide

1. Role of the ARCAN Console

The ARCAN Console is the main tool for file encryption and decryption within the ARCAN system.

It allows users to:

- seal files or folders into .arcsealed containers
- unlock existing ARCAN containers
- verify the integrity of .seal.log journals
- use QuickSeal for short messages (auxiliary tool)

👉 The Console invents nothing, recovers nothing, fixes nothing.
It strictly applies the configuration defined at build time.

2. Starting the Console

- Launch **ARCAN.exe**
- No network access is required
- No Internet connection is performed
- The mention *Licensed by ARIEL-IA* confirms an official Console

3. Interface — Overview

The interface is divided into three clear areas:

Central area — Files & folders (main tool)

This is where all serious encryption operations take place.

Available functions:

- Add files
- Add a folder (recursive scan)
- Clear the list
- Verify a .seal.log journal
- Per-file status tracking

👉 All batch encryption operations go through this area.

Side area — QuickSeal (auxiliary tool)

QuickSeal allows fast encryption of:

- a message
- a memo
- a short text excerpt

Functions:

- clear text → encrypted text
- automatic key generation
- copy encrypted text
- copy key

Strict rules:

- QuickSeal never interacts with the Files area
- no persistence
- copying encrypted text erases the clear text
- copying the key erases the key

 A convenience tool, not a production tool.

Bottom area — Cryptographic actions

Three tabs:

Encryption

1. Enter a password
2. Confirm the password
3. Choose an output folder
4. Start encryption

 The password is unrecoverable.
ARCAN stores no copy, no hash, no key.

Decryption

1. Enter the password
2. Choose an output folder
3. Start decryption

👉 If the password is incorrect or the environment is non-compliant: decryption is refused, with no exploitable information.

⚡ Licence

- Informational display only
- No manual loading
- No modification possible
- The licence is embedded and verified automatically

4. `.seal.log` journals — verification

Each ARCAN encryption generates a chained journal:

- verification possible from the Console
- read-only
- any alteration is detected
- full integrity chain

👉 A valid journal confirms:

- the order of operations
- the absence of modification
- cryptographic consistency

5. What the Console never does

The ARCAN Console:

- ✗ never recovers passwords
- ✗ offers no cloud functionality
- ✗ never communicates over the network
- ✗ does not auto-update
- ✗ suggests no “optimisation”
- ✗ tolerates no non-compliant format

Lost password = permanent data loss.
This is a security guarantee, not a limitation.

6. Recommended best practices

- Use a long passphrase
- Store the password outside the workstation
- Verify journals for sensitive use cases
- Use QuickSeal only for short exchanges

7. Summary

- Files & folders → serious use
- QuickSeal → quick messages
- Licence → informational only
- No recovery possible
- No deliberate ambiguity

ARCAN does not protect against forgetfulness.
It protects against compromise.

WARNING

Never lose your password. Members of ARIEL-IA and ARCAN developers cannot under any circumstances recover your files.

Once sealed, an ARCAN file can only be unlocked using the password chosen at the time of encryption.

rement.