ARCAN — OFFIZIELLE DOKTRIN

Adaptive Reliable Cryptographic Automation for Networks

Stéphane Valente

www.ariel-ia.ch

Inhaltsverzeichnis

🔵 ARCAN — OFFIZIELLE DOKTRIN

Version 1.0

Adaptive Reliable Cryptographic Automation for Networks
ARIEL-IA — Schweiz

---

1. ARCAN ist keine Tarnung.

ARCAN verschleiert nichts.
ARCAN simuliert keine Sicherheit.
ARCAN **ist** Sicherheit.

Es ist keine kosmetische Schicht.
Es ist kein Versprechen.
Es ist kein Marketingkonstrukt.

ARCAN ist ein **kryptografischer Tresor**, absolut konzipiert.

---

2. Passwort verloren → Datei verloren.

Ohne Ausnahme.
Ohne Wiederherstellung.
Ohne Support.
Ohne Berufung.

ARCAN bietet:

- keine Passwortwiederherstellung
- keine Reset-Mechanismen
- keine Sicherungsschlüssel
- keinen Notfallzugang
- keine Master-Zugangsdaten

Das Passwort **ist das Leben der Datei**.
Verschwindet es, verschwindet die Datei mit ihm.

Diese Regel ist absichtlich und unumkehrbar.

---

3. Niemand kann auf die Daten zugreifen. Niemals.

Es gibt keinen privilegierten Zugriff.

Nicht für:

- den Entwickler
- die Organisation
- den Infrastrukturbetreiber
- den Softwarehersteller
- irgendeine Behörde
- irgendeine Institution
- irgendeine Drittpartei

Es gibt keine Ausnahme.
Und es wird niemals eine geben.

Datensouveränität bedeutet **ausschliessliches Eigentum** der Person mit dem Passwort.

---

4. Selbst unendliche Rechenleistung ändert nichts.

ARCAN basiert nicht auf Tricks.
Nicht auf Abkürzungen.
Nicht auf Geheimhaltung.

ARCAN beruht auf:

- modernen kryptografischen Standards
- mathematisch bewiesenen Konstruktionen
- starker Zufälligkeit
- nicht optimierbarer Schlüsselableitung

Keine Anzahl an GPUs, Clustern oder zukünftiger Hardware kann auch nur ein einziges Zeichen ohne das korrekte Passwort extrahieren.

Das ist keine Schätzung.
Das ist eine mathematische Realität.

---

5. Kein Server. Keine Abhängigkeit. Keine Überwachung.

ARCAN kommuniziert nicht.

- Keine Cloud
- Kein Server
- Keine API
- Keine Telemetrie
- Keine Sammlung von Metadaten
- Kein Netzwerkverkehr

ARCAN hört nicht zu.
ARCAN beobachtet nicht.
ARCAN meldet nichts.

Dateien können gespeichert werden:

- auf lokalen Datenträgern
- auf USB-Sticks
- auf privaten Servern
- in Offline-Archiven
- an physisch gesicherten Orten

Die Entscheidung liegt **ausschliesslich** beim Dateninhaber.

---

6. Kryptografie vor Bequemlichkeit.

ARCAN lehnt bewusst Komfortfunktionen ab, die Sicherheit schwächen.

Es gibt:

- keine Synchronisation
- keinen Wiederherstellungsdienst
- kein zentrales Konto
- kein „Passwort vergessen“
- keine versteckte Unterstützung

Benutzerfreundlichkeit darf **niemals** die Souveränität kompromittieren.

ARCAN bevorzugt Verantwortung gegenüber Bequemlichkeit.

---

7. Offline per Design, nicht per Einstellung.

ARCAN ist nicht „offline-fähig“.
ARCAN ist **offline-nativ**.

Es gibt keine Option, die aktiviert werden muss.
Es gibt keine Einstellung, die dieses Verhalten ändern kann.

ARCAN kann nicht in ein vernetztes System umgewandelt werden.

---

8. Integrität ist verpflichtend, nicht optional.

Jede Verschlüsselung erzeugt:

- einen versiegelten Container

- eine authentifizierte Nutzlast
- ein verkettetes Integritätsjournal

Jede Veränderung — selbst eines einzelnen Bits — führt zu einem **zwingenden Fehlschlag**.

Es gibt keinen Teilerfolg.
Es gibt keinen degradierenden Modus.

Integrität ist absolut.

---

9. Brute-Force-Schutz wird am Rand durchgesetzt.

ARCAN stellt einen dedizierten **ARCAN Reader** für Empfänger bereit.

Dieser Reader erzwingt:

- eine strikte Begrenzung auf **10 Passwortversuche**
- eine lokale, irreversible Sperrung nach Überschreitung
- keinen Einfluss auf die verschlüsselte Datei selbst

Der Reader kann ersetzt werden.
Die Datei darf nicht geschwächt werden.

---

10. Ausschliesslich zivile Nutzung.

ARCAN unterliegt einer strikten **Civil-Use-Lizenz (A-CUL™)**.

ARCAN darf nicht verwendet werden für:

- militärische Anwendungen
- offensive Cyberoperationen
- Massenüberwachung
- invasive Überwachungssysteme
- Zwangs- oder Kontrollmechanismen

Starke Kryptografie erfordert starke Ethik.

---

11. Verpflichtende Warnung für Benutzer.

ARCAN muss vor jeder Verschlüsselung zwingend folgende Warnung anzeigen:

**„ARCAN ist kein Spielzeug.
Wenn das Passwort verloren geht, ist die Datei dauerhaft verloren.
Eine Wiederherstellung ist nicht möglich.**

Keine Unterstützung kann helfen.
Bitte bestätigen Sie, dass Sie dies verstanden haben.“

Die Verschlüsselung darf erst nach dieser Bestätigung erfolgen.

Dies ist nicht verhandelbar.

---

12. Souveräne Produktion ist Teil der Sicherheit.

ARCAN wird produziert mit:

- offline betriebenen Build-Systemen
- isolierten Signaturumgebungen
- manueller Lizenzgenerierung
- keiner vernetzten Supply-Chain

Sicherheit endet nicht bei der Kryptografie.
Sie umfasst die **gesamte Produktionskette**.

---

13. ARCAN ist Verantwortung.

ARCAN stärkt die Nutzer — und macht sie verantwortlich.

Mit Souveränität kommt Verantwortung.
Mit Freiheit kommt Disziplin.

ARCAN schützt Benutzer nicht vor sich selbst.
ARCAN schützt Daten vor allen anderen.

---

14. Abschliessende Erklärung

ARCAN verlangt kein Vertrauen.
ARCAN macht Vertrauen überflüssig.

Keine Autorität ist erforderlich.
Keine Erlaubnis wird benötigt.
Keine Abhängigkeit existiert.

ARCAN steht auf Mathematik, Ethik und Souveränität.

Das ist seine Doktrin.
Das ist seine Grenze.
Das ist sein Versprechen.