CertGrep Suite

The Swiss Army Toolkit for PKI & X.509 Certificate Inspection

Free Open Source · Commercial Edition · CLI & Web · Multi-language

2026
04-04

Current Release

7 Languages
Supported

Self-Hosted
Privacy First

Mountain Informatik GmbH · John Buehrer

https://gitlab.com/umi-ch/cert-grep

The Problem: PKI is Critical — But Nearly Invisible

Why certificate inspection matters

Hard to See

X.509 certificates are binary or base64-encoded blobs. Raw OpenSSL commands produce dense walls of text that require expert interpretation.

Silent Failures

Expired certs, weak algorithms, broken chains, and misconfigured keys cause outages and security breaches — often discovered too late.

Quantum Deadline

Post-quantum cryptography migration has a 2030 planning horizon. Organizations need to inventory and assess their certificate estate today.

Most IT teams rely on ad-hoc OpenSSL one-liners, browser pop-ups, or online tools that track your data. There is a better way.

What is a Digital Certificate?

A familiar analogy for a technical concept

Like a Passport…

- Issued by a trusted authority (Certificate Authority = Passport Office)
- Contains verified identity information
- Has an expiry date — and must be renewed
- Some issuers are more trusted than others
- Can be revoked if compromised
- Machines verify them automatically — but humans need help reading them

Certificate Types CertGrep Handles

X.509 Certificates
The standard — websites, email, code signing

PKCS#12 / .p12 / .pfx
Bundled cert + key containers

Java KeyStores (.jks)
Enterprise Java & middleware

Certificate Signing Requests (CSR)
Before issuance

Certificate Revocation Lists (CRL)
Who's been revoked

Private & Public Keys
RSA, EC, Ed25519, Ed448, DSA

PKCS#7 Chains
Multi-cert bundles

A Certificate, As Your System Stores It

Readable by machines. Not so much by humans.

$ cat server.crt

```
-----BEGIN CERTIFICATE-----
MIIByzCCAXCgAwIBAgIUA0FPi1+H3weXcNdF38bi
YH2kMdswCgYIKoZIzj0EAwIwRDEdMBsGA1UEAwwU
VGVzdCBJbnRlcm1lZGlhdGUgQ0ExFjAUBgNVBAoM
DUNlcnRHcmVwIFRlc3QxCzAJBgNVBAYTAkNIMB4X
DTI2MDIyNTEyMDAwMFoXDTI3MDIyNTEyMDAwMFow
QjEbMBkGA1UEAwwSc2VydmVyLmV4YW1wbGUuY29t
MRYwFAYDVQQKDA1DZXJ0R3JlcCBUZXN0MQswCQYD
VQQGEwJDSDBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABJ2FsNx+wBA4L8jsx49OAcHCI/zK0wOT63DK
xCxVuv5eqFp7SdwZbpGyVEKIQ52L9jCxl1RLUZvz
5DXtvlAoBWCjQjBAMB0GA1UdDgQWBBQuDc2X5hND
ql5ZXcMdAOoiZtaRb+ARxDAKBggqhkjOPQQDAgNJ
ADBGAiEA46AWGxe9F95zyfl5t6ntCEsexey4pwSr
YfXF3dj1Pf+0Ds+g4Q==
-----END CERTIFICATE-----
```

or

$ openssl x509 -text -noout -in server.crt

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial: 03:41:4f:8b:5f:87:df:07:...
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: CN=Test Intermediate CA,
      O=CertGrep Test, C=CH
    Validity
      Not Before: Feb 25 12:00:00 2026 GMT
      Not After : Feb 25 12:00:00 2027 GMT
    Subject: CN=server.example.com,
      O=CertGrep Test, C=CH
    Subject Public Key Info:
      Algorithm: id-ecPublicKey (256 bit)
      pub: 04:9d:85:b0:dc:7e:c0:10:...
      ASN1 OID: prime256v1 (P-256)
    X509v3 extensions:
      Subject Key ID: 2E:0D:CD:97:...
      Auth Key ID:    96:9A:25:FA:...
  Signature: 30:46:02:21:00:e3:a0:...
  ⋮  (truncated — full output is much longer)
```

Same certificate — two problems: raw PEM is machine-readable. OpenSSL text is technically complete but dense and hard to read. CertGrep fixes both.

CertGrep: The Same Certificate, Clearly

One command. Human-readable. Actionable.

Quick Summary (summary_0)

```
$ cert-grep  server.crt  summary_0


0: Certificate:
  Issuer:     CN = Test Intermediate CA
  Subject:    CN = server.example.com
  Serial:       03:41:4f:8b:5f:87:df:07
  Not Before:   Feb 25 12:00:00 2026 GMT
  Not After:    Feb 25 12:00:00 2027 GMT

1: Certificate:
  Issuer:     CN = Test Root CA
  Subject:    CN = Test Intermediate CA
  Serial:       4c:a9:5d:dd:72:b2:88:00
  Not Before:   Feb 25 12:00:00 2026 GMT
  Not After:    Feb 24 12:00:00 2031 GMT
```

Default View (no flags needed)

```
$ cert-grep  server.crt


0: Certificate:
  Issuer:    CN = Test Intermediate CA
             O = CertGrep Test, C = CH

  Subject:   CN = server.example.com
             O = CertGrep Test, C = CH

  Signature: ecdsa-with-SHA256

  Key:       EC 256-bit  (P-256)
  Not Before: Feb 25 12:00:00 2026 GMT
  Not After:  Feb 25 12:00:00 2027 GMT
              [328 days remaining]

  Key Usage:  Digital Signature
  Ext Usage:  TLS Web Server Auth
  Subj KID:   2E:0D:CD:97:E6:13:43:64:...
  Auth KID:   96:9A:25:FA:AA:5E:59:5D:...
```

Auto-detects format · No flags needed · 5 detail levels · Supports PEM, DER, PKCS#12, JKS, CSR, CRL, private/public keys, and more

CertGrep Web — Enterprise-Scale in a Browser

Self-hosted · No tracking · Handles hundreds of certificates in one session

Four input modes

Paste PEM · Upload a file · Enter any URL (live SSL Grep) · Browse built-in demo corpus: many PKI examples.

Bulk & batch — no limits

Load a file of certs or a list of URLs in one go. Output is scrollable and structured — handles hundreds, no overload.

Compliance recipe pattern

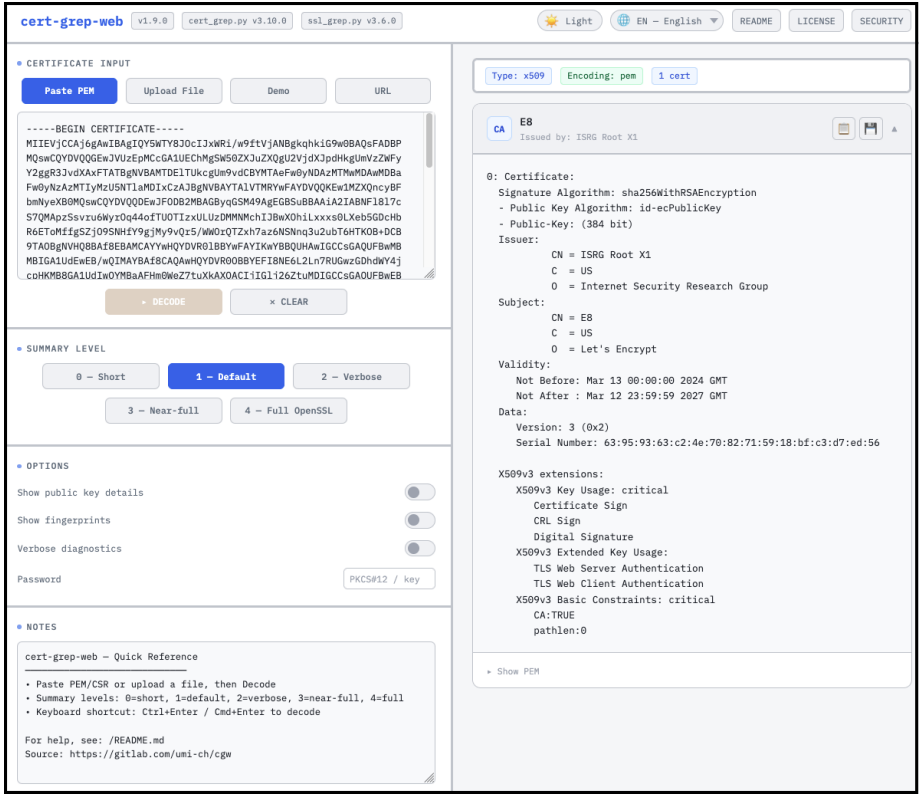
Define a URL list or cert file once, reload it regularly. Fresh batch inspection every time — recurring compliance checks

Self-hosted · Zero data retention

Nothing leaves your server. No telemetry, no third-party calls. Works in air-gapped environments. GDPR-compliant.

Multilingual support · No end-user install

EN DE FR IT ES NL SV. Users open a browser tab — nothing to install. IT deploys once via Docker or Kubernetes.



Handles hundreds of certs per session

The CertGrep Suite — Three Tools, One Workflow

CLI · Network · Web — for every environment

CertGrep CLI

cert-grep.py

- Inspect any certificate format — PEM, DER, PKCS#12, JKS, CSR, CRL
- Auto-detects format — no flags needed
- Bash & PowerShell compatible
- Library mode — import into your own Python scripts
- 5 verbosity levels from quick summary to full output
- Offline — no network, no tracking

SSL Grep

ssl-grep.py

- Fetch live TLS certificate chains from any host
- Inspect what a server actually presents in production
- Proxy support for enterprise environments
- Timeout & error handling built in
- Verify chains and scan for weaknesses in one command
- Complements CertGrep CLI seamlessly

CertGrep Web

Flask · Kubernetes · Self-Hosted

- Browser UI — no installation for end users
- Paste PEM, upload files, or probe live TLS endpoints
- Docker / Kubernetes deployment with TLS & mTLS support
- 7 languages: EN, DE, FR, IT, ES, NL, SV
- No external dependencies · No data retention · No tracking
- Built-in sample corpus for training & demos

Key Features — CertGrep Stands Out

Depth and simplicity in one tool

Format Auto-Detection

Never specify the format manually. CertGrep identifies PEM, DER, PKCS#12, JKS, CSR, CRL, and more automatically.

Post-Quantum Ready

Detects and displays ML-DSA, ML-KEM, and SLH-DSA (NIST PQC) certificates as support matures.

Weakness Scanner

Policy-driven scan for broken algorithms: RSA≤1024, SHA-1, MD5. Quantum migration config included.

Chain Verification

Offline cryptographic chain validation: linkage, signatures, validity, CA constraints, key usage, path length.

Safe Key Inspection

Private key metadata displayed safely — type, size, curve, fingerprint. No private material ever shown.

Library Mode

Import cert-grep as a Python library. Embed inspection in your own tools, pipelines, or automation scripts.

The Quantum Cryptography Threat — A 2030 Deadline

2030

Planning horizon
for PQC migration

What is the risk?

Quantum computers can break RSA and Elliptic Curve cryptography. Encrypted data captured today can be decrypted retroactively when quantum hardware matures — the "harvest now, decrypt later" threat.

What must organizations do?

Identify every certificate using vulnerable algorithms (RSA, ECC). Inventory thousands of certs across servers, smart cards, IoT, code-signing, VPNs. Prioritize replacement.

How CertGrep helps?

The built-in quantum migration policy flags RSA ≤3072 and EC ≤384 as advisories — giving security teams a head start on identifying what must change before the deadline.

NIST standardised post-quantum algorithms (ML-DSA, ML-KEM, SLH-DSA) in 2024. CertGrep already recognises them.

Who Wants CertGrep?

A tool that scales from hobbyist to enterprise

PKI Professionals

Daily-use inspection of certificates, chains, CRLs, keystores across enterprise environments.

Enterprise Security

Certificate inventory audits, weakness scanning, quantum migration planning across thousands of certs.

DevOps & Platform Eng.

CI/CD pipeline integration, Kubernetes TLS debugging, cert-manager verification, mTLS setup.

PKI Vendors & Resellers

Showcase & validate issued certificates. White-label or integrate CertGrep as a support tool.

Entry-Level IT

Clear, readable output with built-in examples — the fastest way to learn what a certificate contains, and other PKI structures too. Eg: CSR, CRL, JKS.

IT Hobbyists

Inspect your own Let's Encrypt cert, browser TLS chains, or self-signed PKI with one command.

CertGrep vs. The Alternatives

Why existing tools fall short

Capability	OpenSSL CLI	Browser Tool	Online Decoder	ssl-checker sites	CertGrep
Auto-detects format	✗	✗	~	✗	✓
Human-readable output	✗	~	~	~	✓
Works offline / no tracking	✓	✓	✗	✗	✓
Handles PKCS#12 & JKS	✓	✗	~	✗	✓
Chain verification	✓	✗	✗	✗	✓
Weakness / quantum scan	✗	✗	✗	✗	✓
Scripting / library mode	✓	✗	✗	✗	✓
Web UI — self-hosted	✗	n/a	✗	✗	✓
7 language UI	✗	✗	✗	✗	✓
No expertise needed	✗	~	~	~	✓

✓ = Full support ~ = Partial ✗ = Not supported

Free & Commercial Editions

Open source that seeds a commercial business

Free / Open Source

AGPL-3.0 licence with dual-licence option

- Full CertGrep CLI (cert-grep.py)
- Full SSL Grep (ssl-grep.py)
- CertGrep Web — self-hosted deployment
- All certificate formats & algorithms
- Chain verification & weakness scan
- 7-language web UI
- Docker & Kubernetes deployment
- Community support via GitLab Issues
- Source code — auditable, forkable

Commercial Edition

Annual licence · Enterprise & site licences available

- Everything in the Free edition
- Commercial licence — no AGPL obligations
- Priority support & SLA
- Feature roadmap influence
- Branded / white-label option
- On-premise deployment assistance
- Integration consulting (EJBCA, cert-manager, K8s PKI)
- Bulk / site licensing for large teams
- Invoice-based purchasing for enterprise procurement

The Business Case — Save Money by Purchasing

Real value beyond the free edition

Certificate Inventory at Scale

Large enterprises manage thousands of certs across smart cards, servers, code signing, IoT, and VPNs. CertGrep provides the inspection layer to build and maintain that inventory — without buying expensive commercial PKI platforms.

Reduce Security Risk Before It Becomes an Incident

Expired certs cause outages. Weak algorithms create vulnerabilities. CertGrep's weakness scanner identifies problems proactively — before auditors, attackers, or angry customers do.

Quantum Migration — Act Now, Not Under Pressure

Organizations that start their PQC inventory in 2025–2026 will hit the 2030 deadline comfortably. Those that wait will face expensive emergency migrations. CertGrep provides the starting point.

Developer Productivity

A PKI engineer spending 30 minutes per day on manual OpenSSL parsing saves hours per week with CertGrep. For a team of 10, that's meaningful. Tool ROI is achieved in days.

Privacy by Design — Self-Hosted, No Tracking

A genuine differentiator in the market

⚠ Online Certificate Decoders

- Upload your certificate — it is recorded on their servers
- Certificate contents reveal subject names, SANs, key types — sensitive metadata
- Many sites are unmaintained and rarely updated
- Some aggregate data for advertising or threat intelligence products
- None match CertGrep's format breadth or feature depth
- You have no control over retention or downstream use

✓ CertGrep — Your Infrastructure

- CLI tool runs 100% locally — nothing leaves your machine
- CertGrep Web is self-hosted — your server, your data
- No telemetry, no analytics, no third-party calls
- Docker image is fully auditable — open source
- Works in air-gapped and high-security environments
- GDPR-compliant by architecture — no data to protect

The AI Pair-Programming Advantage

PKI Domain Expertise

20+ years professional PKI experience

\+

AI Pair Programming

Claude — supervised agentic coding

=

Professional Commercial Tool

At startup speed and cost

Rapid Response to Market Needs

Feature requests and PKI standard updates can be implemented and released in days rather than months. CertGrep already tracks NIST PQC as the standard matures.

Domain-Correct from Day One

AI generates the code, but a senior PKI architect validates every output. The result: fewer bugs, better edge-case coverage, and output that PKI professionals trust.

Published Methodology — Transparency as a Feature

The AI development process is openly documented at gitlab.com/umi-ch/cert-grep/insights — demonstrating responsible AI-assisted development.

Product Roadmap

Where CertGrep is heading

Subject to customer feedback, market research, and available funding.

Delivered | In Progress / Planned | Commercial Milestone

Now — v3.x

- Full format support (PEM/DER/P12/JKS/CSR/CRL/Keys)
- Chain verification & weakness scan
- 7-language web UI
- Docker / Kubernetes deployment
- Post-quantum cert detection

Near Term

- Let's Encrypt customer quick-review mode
- Certificate expiry alerting (web & CLI)
- API endpoint for integration
- Extended quantum migration reporting
- Market research & customer feedback integration

Commercial Focus

- Enterprise site licensing
- White-label / OEM packaging
- EJBCA & cert-manager deep integration
- Certificate inventory database mode
- On-premise support contracts

Business Model — Freemium Done Right

Open source as market seeding, commercial as revenue

Free OSS — Broad Awareness

GitLab, communities, IT hobbyists, students

Self-Hosted Web — Teams Adopt

DevOps teams, PKI engineers, security teams

Commercial Licence — Enterprises

Site licences, support SLAs, integrations

Strategic Partnerships

PKI vendors, MSSP, PKI-as-a-Service providers

→ Free product creates brand recognition and grows the user base that commercial prospects come from.

→ AGPL-3.0 dual-licence: open source users get full functionality; commercial buyers avoid AGPL obligations.

→ Agile development with AI pair-programming means fast response to customer feedback — competitive advantage.

→ Established freemium models (HashiCorp, Elastic, GitLab) validate this path for infrastructure tools.

Get Started with CertGrep

Try the Free Edition

Clone or download from GitLab.
No registration, no tracking.
gitlab.com/umi-ch/cert-grep

Evaluate CertGrep Web

Deploy with Docker in minutes.
Self-hosted, multi-user,
multi-language.

Discuss Commercial Needs

Site licensing, support SLAs,
integration consulting.
Contact Mountain Informatik GmbH.

John Buehrer · Mountain Informatik GmbH · Switzerland

gitlab.com/umi-ch/cert-grep · Open source · Dual-licensed · Self-hosted

The Market Opportunity — By the Numbers

PKI is large, growing fast, and structurally underserved in tooling

$6–7B

PKI market size, 2024

Growing at ~20% CAGR → $20–24B by 2032 (Fortune Business Insights / Grand View Research)

4B+

Active Let's Encrypt certs, 2025

Free/automated segment alone — total active certs on the public internet: 110M+ websites

10,000+

Certs per complex enterprise estate

Yet most IT teams have no fast inspection tool — they rely on OpenSSL one-liners

47 days

New max TLS cert lifetime from 2029

CA/Browser Forum, April 2025. Manual management becomes impossible. See next slide.

$6.9B

DigiCert acquired, 2024

Clearlake Capital + TA Associates — strong investor signal in PKI / digital trust at scale

89%

Fortune 500 use EV/OV certificates

As do 97 of 100 largest banks — every one has a certificate estate that needs inspection

Why Now — Three Structural Market Drivers

Tailwinds that make PKI inspection tooling essential, not optional

1

The 47-Day Cert Lifetime Rule (2029 Deadline)

The CA/Browser Forum voted in April 2025 to reduce maximum TLS certificate validity from 398 days to just 47 days, effective March 2029. When certificates expire every 47 days, manual renewal and inspection workflows collapse. Every organisation will need automation and fast inspection tooling — CertGrep's weakness scanner and SSL Grep address this directly.

2

The Post-Quantum Migration Deadline (2030)

NIST standardised ML-DSA, ML-KEM, and SLH-DSA in 2024. RSA and Elliptic Curve certs must be migrated before quantum computers can crack them — a process that starts with inventory. Organisations that begin their PQC certificate inventory in 2025–2026 will hit the 2030 horizon comfortably. CertGrep's quantum migration policy (configs/quantum.conf) flags at-risk certs on day one.

3

The CLM Tooling Gap — No Good Middle Ground

Enterprise CLM: Venafi (acquired by CyberArk ~$1B, 2024), Keyfactor, AppViewX — powerful but complex and expensive, designed for large teams. Hobbyist/DevOps: Raw OpenSSL CLI — functional but hard to use, no summary view, no weakness scan. CertGrep occupies the uncrowded middle: professional inspection at zero (OSS) or low (commercial) cost, for the individual engineer and the mid-market alike.

Positioning note: CertGrep doesn't need to capture 1% of the $6B PKI market to build a profitable business. It needs a fraction of the millions of IT engineers who handle certificates daily and currently rely on ad-hoc OpenSSL commands or online decoders that track their data. The 47-day rule alone will force every organisation to get serious about certificate visibility by 2029.