



BULK VALIDATION – PKI VS. VERAFILE

A Comparative Analysis of Performance,
Architecture, and Security

Abstract v1.4

*At enterprise scale, PKI validation measures in hours, while
VeraFile validation measures in minutes. Together, they
deliver continuous, scalable, and complete file trust.*





About VeraSec Technologies LLC

VeraSec Technologies is a pioneer in digital artifact integrity, focused on moving the security context from the infrastructure directly to the file itself. While traditional security models rely on centralized systems to establish and maintain trust, VeraSec's patented technologies empower files to carry their own verifiable identity - preparing them for an actual Zero Trust world.

Operating at the forefront of Portable File Identity (PFI), VeraSec invented the Validation Integrity Key (VIK) process. This innovation patches a fundamental vulnerability in traditional PKI that has persisted for decades. By cryptographically binding a file's content and metadata into a compact, human-readable identifier embedded directly within the artifact, VeraSec helps organizations establish durable, portable trust in every digital asset, signed or un-signed - wherever it travels.

About The Publisher

Brian Hajost (bhajost@verasec.net) is a cybersecurity entrepreneur and technologist with more than 30 years of experience in information security, compliance automation, and trusted computing systems.

As the founder of SteelCloud, he pioneered the automation of DISA STIG and CIS benchmark compliance for the DoD, federal agencies, and enterprise customers. Brian holds 17 patents in information technology and mobile security. In 2022 he was named one of the "Top 10 Most Influential People in Cyber Security" by CIO Views.

His current work focuses on solving what he describes as the Artifact Identity Problem - the absence of durable identity for files as they move across distributed systems and untrusted networks.



Bulk Validation: VeraFile vs. PKI

A Comparative Analysis of Performance, Architecture, and Security

Executive Summary

As organizations scale digital operations, the need to validate the integrity and authenticity of large volumes of files has become a critical requirement. Public Key Infrastructure (PKI) has long been the standard for establishing signer identity and non-repudiation. However, PKI was not designed for high-volume, continuous validation of heterogeneous file populations.

This paper presents a comparative analysis between traditional PKI-based validation and VeraFile's Portable File Identity (PFI) model using Verification Integrity Keys (VIKs). Based on measured and modeled results, VeraFile demonstrates **order-of-magnitude improvements in validation throughput**, while also addressing critical integrity gaps left by PKI alone.

The key conclusion is that PKI and VeraFile are not competing technologies, but rather complementary layers. PKI provides **identity assurance**, while VeraFile provides **continuous integrity and artifact continuity assurance**. Together, they form a complete and scalable file trust architecture.

Introduction: The Scaling Problem in File Validation

Enterprise environments today manage millions of files across:

- Document repositories (PDF, Office)
- Log and telemetry systems
- DevSecOps pipelines
- Cross-domain and cloud storage systems

While PKI enables secure signing of high-value artifacts, the majority of files remain:

- unsigned
- inconsistently validated
- difficult to verify at scale

Even when files are signed, validating those signatures across large datasets introduces significant computational and architectural overhead.



The central challenge is: ***How can organizations continuously validate the integrity of all files, while preserving strong identity assurance for signed artifacts?***

PKI Validation Model

PKI validation operates as a **multi-stage, conditional workflow**.

Validation Process

For a signed PDF, PKI validation typically involves:

1. File type identification
2. Signature detection (e.g., /Sig, /ByteRange)
3. Reconstruction of signed byte ranges
4. Hash computation
5. Cryptographic signature verification (CMS/PKCS#7)
6. Certificate chain validation (X.509)
7. Revocation checking (OCSP / CRL)

This process must be repeated for each file individually.

Structural Characteristics

PKI validation is:

- **format-dependent** (PDF ≠ DOCX ≠ executable)
- **conditional** (only applies if a signature exists)
- **multi-layered** (parser + crypto + trust infrastructure)

Performance Characteristics -Based on modeled enterprise conditions:

3 MB Signed PDFs

Scenario	Single Threaded	
	Files/Hour	MB/sec
Best Case	16K – 24K	13 – 20
Typical Enterprise	9K – 16K	7 – 14
Heavy Validation	5K – 9K	3 – 7



20 MB Signed PDFs

Scenario	Single Threaded	
	Files/Hour	MB/sec
Best Case	10K – 16K	60 - 90
Typical Enterprise	6K - 11K	35 - 60
Heavy Validation	4K - 6K	20 - 35

These results highlight a fundamental constraint: **PKI validation throughput is limited primarily by trust infrastructure, not data throughput.**

VeraFile Validation Model

VeraFile introduces a different architectural approach: **Portable File Identity (PFI)**.

Each file carries a **Verification Integrity Key (VIK)** derived from:

- file content
- file name
- file size

This allows direct validation without format-specific parsing.

Validation Process

VeraFile validation consists of:

1. Read VIK (from filename or metadata)
2. Recompute identity basis
3. Compare result

This is a **single-pass, deterministic operation**.

Measured Performance

Empirical results:

3 MB Files

- **320,000 files/hour** (*single-threaded*)
- ~267 MB/sec



20 MB Files

- 67,000 files/hour (*single-threaded*)
- ~372 MB/sec

These results demonstrate:

- high efficiency
- near-streaming throughput
- minimal per-file overhead

Scaling Behavior

VeraFile behaves as a **data-local hashing pipeline**.

Projected scaling (*conservative*):

Threads	3 MB Files	20 MB Files
1	320K/hr.	67K/hr.
4	~0.9M – 1.1M/hr.	~193K – 228K/hr.
8	~1.5M – 2.0M/hr.	~311K – 418K/hr.
16	~2.1M – 3.5M/hr.	~450K – 729K/hr.

Scaling is sub-linear due to:

- storage bandwidth
- memory contention
- per-file overhead

However, throughput remains significantly higher than PKI.

Direct Performance Comparison

Single-Threaded Comparison - 3 MB “Office” Files

Method	Files/Hour
PKI (<i>typical</i>)	9K – 16K
VeraFile (<i>measured</i>)	320K

VeraFile: 20× – 35× faster



Single-Thread Comparison - 20 MB “Office” Files

Method	Files/Hour
PKI (<i>typical</i>)	6K – 11K
VeraFile (<i>measured</i>)	67K

VeraFile: 6× – 11× faster

Key Observation

The performance difference is not incremental, it is architectural:

- PKI: parsing + trust-bound
- VeraFile: hashing + data-bound

Architectural Differences

Dimension	PKI	VeraFile
Validation Model	Conditional	Deterministic
File Parsing	Required	None
Signature Detection	Required	VIK Detection
Certificate Validation	Required	None
Revocation Checks	Often Required	None
File Coverage	Partial	Universal
Scaling Bottleneck	Trust Infrastructure	Data Throughput

Security Gaps in PKI

While PKI provides strong identity guarantees, it does not inherently protect against:

Signature Removal

A signed file can be stripped of its signature:

- Result: unsigned file
- PKI cannot indicate prior signed state

Signature Replacement

A file can be replaced with another validly signed version:

- PKI still validates
- No continuity assurance

File Renaming

File names can be changed without invalidating signatures:

- breaks contextual integrity
- not detectable by PKI

VeraFile + PKI: A Combined Model

The strongest architecture is not replacement, but combination of signing and sealing.

Complementary Roles

Capability	PKI	VeraFile
Identity of signer	✓	✗
Non-repudiation	✓	✗
Detect tampering	⚠	✓
Detect signature removal	✗	✓
Detect renaming	✗	✓
Universal coverage	✗	✓

Operational Model

High-Frequency Validation

- VeraFile (daily / continuous)
- Detects tampering, renaming and signature removal

Low-Frequency Validation

- PKI (weekly / monthly)
- Confirms signer identity and certificate trust

Result: Continuous integrity + periodic identity assurance



Strategic Implications

Performance

VeraFile enables validation at:

- Millions of files per hour (*parallelized*)
- Operates without trust infrastructure bottlenecks

Security

VeraFile protects:

- The file itself
- The persistence of signatures
- The continuity of artifact identity

Operational Efficiency

Organizations can:

- Validate entire repositories daily
- Reduce reliance on expensive PKI operations
- Maintain strong compliance posture

Conclusion

PKI remains essential for establishing identity and non-repudiation. However, it is not designed for high-speed, continuous validation across large and diverse file populations. VeraFile introduces a complementary capability: **portable, deterministic file identity** that enables fast, universal validation. Together, they form a layered trust model:

- PKI proves who signed a file
- VeraFile proves it is still that same file.

This combination represents a new category: **Signature Continuity Assurance**. A model in which:

- Every file can be validated continuously
- Signed artifacts remain verifiably intact
- Trust scales with data, not infrastructure

At enterprise scale, PKI validation measures in hours, while VeraFile validation measures in minutes. Together, they deliver continuous, scalable, and complete file trust.