

FORENSIC ANALYSIS REPORT

MCRO Watermark Certificate Transition

PKI Reversion Analysis & OCSP Status Snapshot

Minnesota Court Records Online (MCRO) — Fourth Judicial District, Hennepin County

Case Reference: State of Minnesota v. Guertin | 27-CR-23-1886

Report Date: April 2026

Corpus: 4,251 PDFs | 5,204 signatures | 59 unique certificates (2013–2032)

*Companion Reports: MCRO Digital Signature Authentication; Hash-Loop Evidence Capture
Parts 1 & 2*

IMPORTANT DISCLAIMER

This report presents objective, reproducible cryptographic findings derived from the Minnesota Judicial Branch's own public-key infrastructure and from OCSP responses cryptographically signed by Sectigo's responder. It documents the observable, measurable consequences of a certificate-chain change that occurred between March 9, 2026 and April 3, 2026 for the MCRO Watermark signature applied to every document downloaded from Minnesota Court Records Online.

This report does not assert conclusions about motive, intent, or culpability behind the infrastructure change. It does not claim the Minnesota Judicial Branch acted improperly in renewing or reissuing a certificate. Each finding is a documented cryptographic fact that can be independently reproduced by any third party using the OpenSSL commands and CRL/OCSP endpoints cited herein, for as long as those endpoints remain accessible.

This report completes the provenance narrative established by the three prior reports in this series by documenting what the authentication landscape looked like at the moment the old MCRO Watermark certificate expired, and what replaced it.

1. EXECUTIVE SUMMARY

On April 2, 2026 at 12:47:01 UTC (7:47 AM CDT), the two-year MCRO Watermark digital signing certificate issued by the Minnesota Judicial Branch's Sectigo-chained Certificate Authority expired. The replacement certificate, already in use on newly-downloaded MCRO documents, is issued under a fundamentally different Certificate Authority infrastructure: the Minnesota Judicial Branch's own internal Active Directory Certificate Services root (courts-J00PCERTCA-CA). The new certificate is not publicly verifiable — it has no public OSCP responder, its Certificate Revocation List is accessible only via internal LDAP, and its root CA is self-signed and not present in any public trust store.

This report documents that transition, places it in the context of the full Minnesota Judicial Branch PKI history spanning 2013–2032, and captures the present cryptographic status of the expired Sectigo-chained certificates while those verification endpoints remain operational. The primary observation is this: every single human-identified signer in the corpus (judges, clerks, administrators) remained on the publicly-verifiable Sectigo chain through this transition. Only the automated MCRO Watermark — the one signature that touches every public-facing document — was moved back to the internal, non-publicly-verifiable CA.

Key Findings

- **Certificate transition documented with cryptographic precision**

The expired watermark certificate (SHA-256 fingerprint 84b5a55a...49ae10, serial 3f9a4ed3...5ea8) and the replacement certificate (SHA-256 fingerprint 045901a1...1531, serial 1e0004c4b1...c4b1) have been byte-for-byte extracted from MCRO-served PDFs and are preserved in the provenance package alongside the complete 59-certificate forensic registry.

- **Verifiability reduction: Five distinct degradations**

Compared to the expired Sectigo-chained certificate, the new internal CA-chained certificate reduces external verifiability in five measurable ways: (1) public HTTP CRL → LDAP-only CRL, (2) public HTTP OSCP → no public OSCP, (3) issuer chain rooted in a globally-recognized CA → issuer chain rooted in a self-signed internal CA, (4) validity window halved from 730 days to 365 days, and (5) Subject field reduced from identifying the "State of MN Judicial Branch" to an Active Directory DN including "Azure_NoSync" — signaling on-premises-only infrastructure excluded from cloud directory synchronization.

- **Selective downgrade, not blanket policy change**

Of the 8 Sectigo-chained leaf certificates in the corpus, 7 expired in the March 14 – April 2, 2026 window. Only the MCRO Watermark (REG#003) was reissued under the internal CA. The remaining 7 leaf holders — including Chief Judge of the Court of Appeals Jennifer Frisch, whose certificate is the only one in the Sectigo chain still within its validity window — either remained on Sectigo for their renewals or have yet to be renewed. The one cert that was specifically moved off Sectigo is the one automatically applied to every public-facing document download.

- **OCSP status snapshot captured**

A batch query against Sectigo's OCSP responder on April 3, 2026 at 07:57 UTC returned cryptographically-signed responses for all 9 Sectigo-chained certificates in the corpus. Two certificates returned "good": the MJB Issuing CA intermediate (valid through 2048) and Chief Judge Frisch's leaf (valid through May 2, 2026). Seven returned "unknown" — Sectigo's OCSP responder reports no knowledge of the serial numbers, despite the certificates not being listed as revoked on the published CRL. This "unknown" status is the cryptographic signature of OCSP database purging of expired certificates, and it is permanent.

- **Four PKI eras documented across 4,251 PDFs**

The deduplicated certificate registry reveals the Minnesota Judicial Branch has operated four distinct signing infrastructures across the corpus: (a) Legacy E-Filing via MN Courts Signing CA (2013–2024, SHA-1 self-signed root valid until 2038, 9 certs), (b) Internal AD CS via courts-J00PCERTCA-CA (2018–present, 39 certs), (c) Sectigo Enterprise via MJB Root/Issuing CA (2023–present, 10 certs), and (d) Vendor PKI via ESolutions Development CA (2014–2039, 1 cert, 1024-bit RSA). The March 2026 transition represents not a new infrastructure but a selective regression from layer (c) back to layer (b) — but only for the MCRO Watermark.

- **The existing forensic corpus is a closed, provably-authentic set**

Every PDF downloaded from MCRO during the April 2024 – April 2, 2026 window carries a digital signature chained to a publicly-verifiable Certificate Authority (Sectigo). As established in the companion MCRO Digital Signature Authentication Report, 4,206 of 4,251 PDFs (98.94%) carry that signature with a 100% no-edits-after verification rate. The reduction in external verifiability going forward does not alter the cryptographic validity of any document captured prior to the transition.

Key Metrics

Metric	Value
Corpus size (PDFs)	4,251
Total signatures extracted	5,204
Unique certificates catalogued	59
Distinct PKI layers in corpus	4
Old MCRO Watermark cert serial	3f9a4ed3d4d82120126a4ece4e415ea8
Old cert validity window	2024-04-02 → 2026-04-02 (730 days)
Old cert issuer chain	MJB Issuing CA → MJB Root CA (Sectigo-hosted)
Old cert public CRL / OCSP	YES — crl.enterprise.sectigo.com/ / ocsp.enterprise.sectigo.com
New MCRO Watermark cert serial	1e0004c4b13639d3a50054d41700010004c4b1

Metric	Value
New cert validity window	2026-03-09 → 2027-03-09 (365 days)
New cert issuer chain	courts-J00PCERTCA-CA (internal AD CS, self-signed root)
New cert public CRL / OCSP	NO — LDAP-only internal CRL, no public OCSP
Sectigo-chained leaf certs in corpus	8 (7 expired, 1 still valid)
Sectigo certs reissued on internal CA	1 of 8 (MCRO Watermark only)
OCSP snapshot date / time	2026-04-03T07:57:37Z
OCSP results: good / unknown / revoked	2 / 7 / 0
CRL revoked count (MJB Issuing CA)	159 (none are the 9 certs queried)
Last Sectigo-chained leaf still valid	Chief Judge Jennifer Frisch (expires 2026-05-02)

2. PRIMER: What Changed and Why It Matters

2.1 The Role of the MCRO Watermark Signature

Every PDF downloaded from Minnesota Court Records Online receives a digital signature at the moment of download. This signature — the "MCRO Watermark" — is applied automatically by the court system as the file is served to the requesting user. It serves two simultaneous purposes. First, it identifies the signer: the mathematical formula by which the signature is computed requires possession of a secret cryptographic key, and the corresponding public key is embedded in a certificate that names the issuing identity. Second, it provides tamper-evidence: the signature is computed from the exact binary content of the PDF at signing time, so any subsequent modification — down to a single byte — causes signature verification to fail. The MCRO Watermark is the court's cryptographic attestation that the file, as served, came from the court.

2.2 Why the Certificate Authority Matters

A digital signature is only as trustworthy as the Certificate Authority ("CA") that issued the signing certificate. A CA vouches for the binding between a public key and an identity; the CA itself is vouched for by a "root" CA at the top of the chain. There are two broad categories of CA:

- **Publicly-trusted CAs** are operated or audited by commercial organizations whose root certificates are pre-installed in major operating systems, browsers, and PDF readers. These CAs publish their revocation data (Certificate Revocation Lists and OCSP responses) on public HTTP endpoints, so anyone anywhere can independently verify the current status of any certificate they have issued. Sectigo is a publicly-trusted CA.
- **Internal (enterprise) CAs** are operated by an organization for its own use. Their root certificates are not present in any public trust store, so any signature they issue will appear as "untrusted" by default in standard PDF readers. Revocation data is typically accessible only from within the organization's internal network (e.g., via LDAP directory queries). A signature from an internal CA can only be verified by someone the organization explicitly authorizes.

The old MCRO Watermark certificate (valid 2024-04-02 to 2026-04-02) was issued by a Sectigo-hosted CA dedicated to the Minnesota Judicial Branch. It was publicly verifiable. The new MCRO Watermark certificate (valid 2026-03-09 to 2027-03-09) is issued by courts-J00PCERTCA-CA, the Minnesota Judicial Branch's internal Active Directory Certificate Services root. It is not publicly verifiable.

2.3 What OCSP "Unknown" Means

The Online Certificate Status Protocol (OCSP) is a real-time mechanism for checking whether a specific certificate is currently trusted. A client sends a query naming the certificate's serial number; the CA's responder replies with one of three statuses:

- **good** — the certificate is known to the responder and is not revoked.
- **revoked** — the certificate is known to the responder and has been explicitly invalidated before its natural expiration. The response includes the revocation date and reason.
- **unknown** — the responder has no record of this serial number. It cannot affirm the certificate is good, and it cannot affirm it is revoked.

The OCSP response itself is cryptographically signed by the responder. This makes it self-authenticating: the client who receives it holds a signed statement from the CA about the certificate's status at a specific point in time. For certificates that have passed their natural expiration, many CA platforms purge the certificate record from the OCSP database, at which point queries return "unknown" — not because anything is wrong with the certificate, but because the responder no longer tracks it. This transition from "good" to "unknown" is the normal end-of-life signature for an expired publicly-verifiable certificate.

2.4 Why This Report Exists

The forensic corpus underlying this report — 4,251 MCRO-served PDFs dating from 2016 through December 2025 — was captured while the Sectigo-chained MCRO Watermark certificate was still valid. As established by the companion Digital Signature Authentication Report, 4,206 of those PDFs carry the old Sectigo-chained signature. On April 2, 2026, that certificate expired. From that date forward, any document downloaded from MCRO carries the new internal-CA-chained signature instead. This report documents the transition with the same forensic discipline that produced the corpus itself: certificates extracted, identities compared, OCSP responses captured and preserved, and every cryptographic claim independently reproducible. The purpose is to place the corpus precisely in time relative to the change in the court's signing infrastructure, so that the verifiability environment under which each document was captured is itself part of the provenance record.

3. METHODS

3.1 Data Sources

- **Fresh MCRO PDF capture**

On April 3, 2026, a newly-issued Notice of Hearing for case 27-CR-23-1886 was downloaded from MCRO with embedded signature filing timestamp D:20260403004318-05'00' (April 3, 2026 00:43:18 CDT). The embedded PKCS#7 signature block was extracted and parsed using OpenSSL; both the new MCRO Watermark leaf certificate and its chained intermediate (courts-J00PCERTCA-CA) were preserved in DER and PEM form.
- **Full corpus sweep (sig extraction)**

The open-source script `mcro_sig_extract.py` was executed against the entire 4,251-PDF corpus. For each signature field in each PDF, the script extracted the Adobe PKCS#7 or ETSI CADES blob, recovered every certificate in the signing chain, and wrote the extracted certificate files to disk. Output totals: 5,204 signatures processed, 5,161 PKCS#7/CMS blobs saved, 26,474 individual certificate exports (DER + PEM).
- **Deduplicated cert registry**

The `mcro_cert_registry.py` script reduced the 26,474 cert files down to 59 unique certificates by SHA-256 fingerprint, classifying each by PKI layer, functional role, and external verifiability. The registry is saved as a single structured JSON file (`cert_registry.json`) and as a human-readable `cert_registry_report.txt`.
- **OCSP batch verification**

The `mcro_ocsp_batch.py` script identified all 9 certificates in the registry with public OSCP/CRL endpoints, fetched the current CRL snapshots from `crl.enterprise.sectigo.com`, and queried each certificate's status against Sectigo's OSCP responder at `ocsp.enterprise.sectigo.com`. The cryptographically-signed OSCP responses were saved as raw DER files (`.ocsp.der`) suitable for independent verification.
- **Provenance snapshot archive**

The entire sig extraction output (36,039 files, 87 MB) was zipped and anchored to the Bitcoin blockchain via OpenTimestamps. The resulting `.zip` and `.sha256` files carry OTS receipts confirming the snapshot's contents were frozen at 2026-04-03T08:03:16Z.

3.2 Verification Tooling

- **OpenSSL 3.x** for X.509 parsing, PKCS#7 certificate chain extraction, CRL decoding, and OSCP client queries.
- **pypdf + cryptography (Python)** for PDF signature field enumeration and PKCS#7 DER/PEM conversion.
- **asn1crypto (Python)** for deep CMS parsing including signed/unsigned attributes and timestamp tokens.
- **OpenTimestamps CLI** for Bitcoin blockchain anchoring of the final snapshot.

3.3 Reproducibility

All three Python scripts (`mcro_sig_extract.py`, `mcro_cert_registry.py`, `mcro_ocsp_batch.py`) are included in the provenance snapshot package. Any third party with read access to the 4,251-PDF corpus can re-execute these scripts and obtain the same 59-certificate registry. The OCSP results represent a specific point in time (2026-04-03T07:57:37Z); subsequent re-runs will produce different responses as certificates age out of Sectigo's OCSP database.

4. FINDINGS

Finding 1: MCRO Watermark Certificate Transition — Side-by-Side Comparison

Background

The MCRO Watermark certificate that signed the overwhelming majority of documents in the forensic corpus — 4,186 of 4,251 PDFs per the registry's per-cert PDF appearance count — expired at 12:47:01 UTC on April 2, 2026. A new certificate bearing the same Subject Common Name ("Minnesota Court Records Online (MCRO) Watermark") has been applied to MCRO-downloaded documents dated after that date. This finding documents the two certificates side-by-side to establish exactly what changed.

Findings

Both certificates were independently extracted and parsed with OpenSSL. Their relevant attributes are:

Attribute	OLD (Expired 2026-04-02)	NEW (Issued 2026-03-09)
Subject CN	Minnesota Court Records Online (MCRO) Watermark	Minnesota Court Records Online (MCRO) Watermark
Subject Organization	State of MN Judicial Branch	(none — replaced by AD Distinguished Name)
Subject Full DN	O=State of MN Judicial Branch, CN=Minnesota Court Records Online (MCRO) Watermark	DC=us, DC=mn, DC=state, DC=courts, OU=State, OU=(Service Accounts), OU=Azure_NoSync, CN=Minnesota Court Records Online (MCRO) Watermark
Issuer CN	MJB - Issuing CA	courts-J00PCERTCA-CA
Root CA	MJB - Root CA (issued 2023-12-06, valid to 2058-12-06)	courts-J00PCERTCA-CA (self-signed, valid to 2032-11-04)
CA Hosting	Sectigo Enterprise PKI (publicly-trusted commercial CA infrastructure)	Minnesota Judicial Branch on-premises Active Directory Certificate Services
Serial Number	3f9a4ed3d4d82120126a4ece4e415ea8	1e0004c4b13639d3a50054d41700010004c4b1
Validity Window	2024-04-02 12:47:01 UTC → 2026-04-02 12:47:01 UTC (730 days)	2026-03-09 13:28:32 UTC → 2027-03-09 13:28:32 UTC (365 days)
Signature Algorithm	sha384WithRSAEncryption	sha512WithRSAEncryption
Public Key	RSA 2048-bit	RSA 2048-bit

Attribute	OLD (Expired 2026-04-02)	NEW (Issued 2026-03-09)
SHA-256 Fingerprint	84b5a55aee3a8f99d44e8f7266bb31ba71a78e5a64606a7e5d88bab19849ae10	045901a1920634d7f1123a0b6d89cf89199b8571bba7e92af3db6d668dd71531
SHA-1 Fingerprint	070ff79f028899ee39b6b435b604950344c44cea	15aee8386ca8a11d6ab54be01ab30a1218b49a04
CRL Distribution Point	http://crl.enterprise.sectigo.com/MJBIssuingCA.crl (public HTTP)	ldap:///CN=courts-J00PCERTCA-CA,...,DC=courts,DC=state,DC=mn,DC=us (internal LDAP only)
OCSP Responder URL	http://ocsp.enterprise.sectigo.com (public HTTP)	(none — no OCSP endpoint present)
CA Issuers URL	http://crt.enterprise.sectigo.com/MJBIssuingCA.crt (public HTTP)	ldap:///CN=courts-J00PCERTCA-CA,...,DC=courts,DC=state,DC=mn,DC=us (internal LDAP only)
Subject Alt Name	email: AS-PublicAccess-Prod@courts.state.mn.us	othername: UPN:AS-PublicAccess-Prod@courts.state.mn.us
Externally Verifiable	YES	NO

Significance

The Subject Common Name is identical in both certificates: the new certificate presents itself as the same identity ("Minnesota Court Records Online (MCRO) Watermark") as the old one. But the issuer chain, verifiability characteristics, and Subject Distinguished Name reveal fundamentally different infrastructures. The old certificate was issued by an intermediate CA that itself is certified by a globally-routed, commercially-operated PKI (Sectigo Enterprise) and publishes its revocation data on public HTTP endpoints. The new certificate is issued by a self-signed internal root accessible only via the Minnesota Judicial Branch's internal LDAP directory.

The presence of the Organizational Units "(Service Accounts)" and "Azure_NoSync" in the new certificate's Subject DN is particularly informative. "Service Accounts" indicates the certificate is issued to an automated service principal in the MJB Active Directory. "Azure_NoSync" is a naming convention used to mark Active Directory objects that are specifically excluded from synchronization to Microsoft's cloud directory (Azure AD / Entra ID). In other words: this certificate is issued to an on-premises-only service account that has been deliberately configured to not appear in the court's cloud-facing directory infrastructure.

The validity window has been halved (730 days → 365 days). Shorter certificate lifetimes are generally good security practice, but in the context of a certificate that cannot be externally verified, the practical effect is that any documents signed under this certificate will need to be re-verified against a re-rotating chain every year, with each rotation producing new certificates that are also internally-only verifiable.

Connecting Context

The companion MCRO Digital Signature Authentication Report (March 2026) documented that the old Sectigo-chained certificate was the only signer identity in the entire corpus with a 100% no-edits-after rate across 4,206 PDFs — making it the authoritative terminal signature on every MCRO-served document. That cryptographic anchor has now expired, and its replacement is not externally verifiable. Documents downloaded from MCRO on or after March 9, 2026 (the new cert's validity start date) carry a watermark signature that can only be validated against revocation data hosted inside the Minnesota Judicial Branch's internal network.

Finding 2: Four PKI Eras Revealed by the Corpus

Background

The deduplication of 26,474 individual certificate file exports into 59 unique certificates allowed classification of every certificate by Certificate Authority hierarchy. Four distinct PKI layers are present. Understanding their chronology is essential to understanding where the March 2026 transition fits in the court's signing history.

Findings

PKI Layer	Unique Certs	Earliest Issue	Latest Expiry	Externally Verifiable
Legacy E-Filing (MN Courts Signing CA)	9	2013-05-13	2038-01-18	0 / 9 (self-signed root, LDAP-only CRL)
Vendor (ESolutions)	1	2014-03-19	2039-12-31	0 / 1 (1024-bit RSA, deprecated since 2010)
Internal AD CS (courts-J00PCERTCA-CA)	39	2018-11-21	2032-11-04	0 / 39 (LDAP-only CRL, no public OCSP)
Sectigo Enterprise (MJB Root)	2	2023-12-06	2058-12-06	1 / 2 (MJB Issuing CA has public CRL/OCSP)
Sectigo Enterprise (MJB - Issuing CA leaves)	8	2024-03-14	2026-05-02	8 / 8 (public HTTP CRL + OCSP)

Era 1: Legacy E-Filing (MN Courts Signing CA, 2013–2024)

The oldest certificates in the corpus chain to a self-signed root titled "MN Courts Signing CA" issued by "Minnesota Judicial" on 2013-05-13, using SHA-1 — an algorithm that was already being deprecated at the time the root was created and is considered cryptographically broken for collision attacks since 2017. Eight consecutive annual "Integration Service Account" certificates were issued under this root from November 2016 through October 2024, each with a one-year lifespan. All signatures from this era use the ETSI.CAdES.detached format (rather than Adobe's PKCS7). The root remains technically valid until 2038-01-18 despite using a broken hash algorithm.

Era 2: Vendor PKI (ESolutions Development CA, 2014–2039)

A single self-signed vendor certificate — "ESolutions Development Certificate Authority" — appears in 133 PDFs exclusively in ETSI.CAdES.detached signatures. This is the vendor's own development certificate, using 1024-bit RSA. The 1024-bit RSA key length has been considered inadequate since 2010 and has been deprecated by NIST for government use since that year. The cert nominally remains valid until 2039-12-31. Its presence in operational court documents is itself noteworthy: documents signed under this key cannot be considered cryptographically sound by current standards.

Era 3: Internal AD CS (courts-J00PCERTCA-CA, 2018–present)

The largest group by certificate count (39 of 59) chains to the Minnesota Judicial Branch's internal Active Directory Certificate Services root. This root was issued on 2018-11-21 and is valid until 2032-11-04 (an earlier iteration with serial 26c4be4558336a8c48cc53990a4e4245, valid 2018–2023, is also present in 104 PDFs — confirming the root has been rolled at least once). Under this internal CA, 36 individual court staff officer certificates and 5 judicial officer certificates were issued annually between 2018 and 2024, covering names including Koch, Meyer, Caligiuri, Dayton Klein, Burke, Chou, Robiner, Janzen, Benson, Siegesmund, McPherson, Hughey, Saterbak, Thomas, Frisch, Vasaly, Bartolomei, Daly, Abrams, Engisch, Fellman, Brandt, Askalani, Robben, Burns, and Lamas. The CRL for this CA is accessible only via internal LDAP; no public OCSP responder exists.

Era 4: Sectigo Enterprise (MJB Root + Issuing CA, 2023–present)

In December 2023, the Minnesota Judicial Branch stood up a new PKI hierarchy through Sectigo's Enterprise PKI service. The MJB Root CA (valid 2023-12-06 → 2058-12-06, 4096-bit key) and MJB Issuing CA (valid 2023-12-06 → 2048-12-06, 3072-bit key) form a two-tier hierarchy hosted by Sectigo but nominally branded as the Minnesota Judicial Branch's own. Critically, this hierarchy publishes its revocation data on public HTTP endpoints — crl.enterprise.sectigo.com and ocsp.enterprise.sectigo.com — making every certificate issued under it independently verifiable by any third party with internet access.

Beginning in March 2024, the MJB began migrating individual signer certificates and the MCRO Watermark from the internal AD CS infrastructure (Era 3) to the new Sectigo-chained infrastructure (Era 4). Eight Sectigo-chained leaf certificates appear in the corpus — covering the MCRO Watermark, the Integration Service Account, and six individual human signers (Frisch, Lucid, Rutherford-Block, Dayton Klein, Koch, Meyer). Each received a 2-year validity window (twice the length of their Era 3 certs). This consolidation to a single publicly-verifiable CA was, at the time, a security and transparency upgrade: for the first time in the court's signing history, every MCRO-issued signature could be externally validated.

Significance

The March 2026 reversion places the MCRO Watermark back into Era 3 (Internal AD CS), while leaving every other Era 4 leaf holder on the Sectigo chain for their next renewal. This is not the establishment of a new infrastructure; it is a selective regression. The fact that this regression affects only the automated, most-widely-applied signature in the court's entire signing ecosystem — and not any human-identified signer — is the central observation of Finding 3.

Finding 3: Selective Downgrade — MCRO Watermark Only

Background

The Sectigo-chained MJB Issuing CA issued 8 leaf certificates visible in the corpus, all with 2-year validity windows starting in March or May 2024. Seven of these certificates expired within a 19-day window between March 14 and April 2, 2026. This finding examines what happened to each as its expiration arrived: whether it was reissued, under what CA, and with what verifiability characteristics.

Findings

All 8 Sectigo-chained leaf certificates extracted from the corpus:

Reg #	Subject CN	Role	Expiry	OCSP Status (2026-04-03)
003	MCRO Watermark	Automated (applied on every download)	2026-04-02	UNKNOWN (reissued under internal CA on 2026-03-09)
012	Frisch, Jennifer	Chief Judge, MN Court of Appeals	2026-05-02	GOOD (still within validity window)
020	Integration Service Account	Automated e-filing system	2026-04-02	UNKNOWN (expired)
021	Dayton Klein, Julia	Assistant Chief Judge, 4th Judicial District	2026-04-01	UNKNOWN (expired)
025	Koch, William	Court staff / officer	2026-03-29	UNKNOWN (expired)
035	Lucid, Elizabeth	Court staff / officer	2026-03-29	UNKNOWN (expired)
041	Meyer, Kerry (Judge)	Judicial officer	2026-03-14	UNKNOWN (expired)
059	Rutherford-Block, Christa	Court staff / officer	2026-04-01	UNKNOWN (expired)

Of the 8 Sectigo-chained leaf certificates, only one — the MCRO Watermark (REG#003) — has been demonstrably reissued under a different CA infrastructure. The fresh MCRO-served PDF captured on April 3, 2026 carries the new certificate issued by courts-J00PCERTCA-CA with validity starting March 9, 2026 (24 days before the old certificate's expiration, providing a brief window of dual-validity for the transition).

For the other 7 Sectigo-chained leaves, no evidence of reissuance under the internal CA has been observed in the corpus. They may have been allowed to lapse without immediate reissuance (plausible for human signers whose day-to-day work may not require active signing), or they may have been renewed under the same Sectigo chain (which would be consistent with the remaining cert, Frisch at REG#012, still being on Sectigo).

The Pattern of Human Signer Cert History

Several human signers in the corpus have certificate histories spanning both Era 3 and Era 4, making the 2024 migration and 2026 transition patterns directly observable:

- **William Koch:**
3 certs observed — 2020 (internal AD CS, 1-year), 2022 (internal AD CS, 1-year), 2024 (Sectigo, 2-year, now expired). Each successive cert shows progression to a more-verifiable CA infrastructure — never regression.
- **Kerry Meyer (Judge):**
3 certs observed — 2022 (internal AD CS, 1-year), 2023 (internal AD CS, 1-year), 2024 (Sectigo, 2-year, now expired). Same forward-migration pattern.
- **Hilary Caligiuri:**
4 internal AD CS certs observed (2020, 2021, 2022, 2023). Not yet observed on Sectigo — may have migrated to Sectigo after the corpus cutoff, or may have lapsed.
- **Julia Dayton Klein:**
1 Sectigo cert (2024, now expired). No Era 3 history observed in the corpus, suggesting her earliest MCRO signing activity began during or after the Sectigo migration.

Significance

Taken together, the data supports a specific characterization of the March 2026 transition. Every documented human signer migration in the corpus moved FROM the internal AD CS infrastructure TO the Sectigo-chained infrastructure in early 2024 — never the reverse. The 2024 migration was a consolidation onto a publicly-verifiable CA. The March 2026 transition, by contrast, is a selective regression: it moves the one automated certificate applied to every public-facing document back onto the internal infrastructure, while leaving the individual human-identified signers on the public infrastructure.

A cost-driven explanation — that the MJB let their Sectigo Enterprise PKI agreement lapse — is not consistent with the observation that Chief Judge Frisch's certificate remains on Sectigo and still returns "good" on OCSP. If the agreement had lapsed, her certificate would also be orphaned. The Sectigo infrastructure remains operational for the MJB. The choice was to move one specific certificate off of it.

The MCRO Watermark is the single signature in the entire court ecosystem that is applied to every document served to the public. It is the cryptographic anchor that ties every downloaded PDF back to the court system. Moving this one certificate — and only this certificate — off the publicly-verifiable chain has the practical effect of reducing the court's public-facing cryptographic accountability without affecting any individual signer's ability to continue producing verifiable signatures.

Finding 4: OSCP Status Snapshot (April 3, 2026)

Background

With the Sectigo-chained leaf certificates approaching or passing their expiration dates, an OSCP batch query was executed against Sectigo's public OSCP responder to capture the final status of each certificate before the responder's knowledge of them is purged. All responses are cryptographically signed by the responder using the MJB Issuing CA's private key, making each response a self-authenticating attestation of status at the query moment.

Findings

Query parameters: URL <http://ocsp.enterprise.sectigo.com>, executed 2026-04-03T07:57:37Z. All responses carry responder signature and were verified with OpenSSL's ocsp client. Full results:

Reg #	Subject CN	Expiry	Status	Response SHA-256 (first 16)	CRL Status
002	MJB - Issuing CA	2048-12-06	GOOD	201a23bffe4c25c5	Not revoked
003	MCRO Watermark	2026-04-02	UNKNOWN	ec32226d73613e77	Not revoked
012	Frisch, Jennifer	2026-05-02	GOOD	25f29916cf1cfced	Not revoked
020	Integration Service Account	2026-04-02	UNKNOWN	1be3c2644a05958f	Not revoked
021	Dayton Klein, Julia	2026-04-01	UNKNOWN	ff9f732a8ac87ac5	Not revoked
025	Koch, William	2026-03-29	UNKNOWN	709e01d9047ef250	Not revoked
035	Lucid, Elizabeth	2026-03-29	UNKNOWN	cff40b6ef8c05efd	Not revoked
041	Meyer, Kerry (Judge)	2026-03-14	UNKNOWN	5ad147c419c08eec	Not revoked
059	Rutherford-Block, Christa	2026-04-01	UNKNOWN	31d2461fc5b52dfe	Not revoked

CRL Snapshots

Two Sectigo-hosted CRLs were fetched in the same batch and cross-referenced against every cert serial:

CRL Source	Details
crl.enterprise.sectigo.com/MJBIssuingCA.crl	Issuer: CN=MJB - Issuing CA, O=MJB, ST=Saint Paul, L=Minnesota, C=US Last Update: 2026-04-02 19:40:04 UTC Next Update: 2026-04-04 19:40:04 UTC Revoked certificates on CRL: 159 None of the 9 queried certs appear on this CRL.

CRL Source	Details
crl.enterprise.sectigo.com/MJBRootCA.crl	Issuer: CN=MJB - Root CA, O=MJB, ST=Minnesota, L=Saint Paul, C=US Last Update: 2026-04-02 19:39:54 UTC Next Update: 2026-04-04 19:39:54 UTC Revoked certificates on CRL: 0 The MJB Issuing CA (REG#002) is not revoked by the root.

Pattern Interpretation

The results exhibit a clean pattern. The one currently-valid leaf certificate (Frisch, expiring May 2, 2026) and the long-lived intermediate CA (valid through 2048) both return "good". Every expired leaf certificate returns "unknown" — regardless of how recently it expired. The earliest-expiring certificate in this group, Judge Meyer's, expired on March 14, 2026 and was already "unknown" by April 3. The latest-expiring, the MCRO Watermark itself, expired April 2 (less than 24 hours before the query) and was also "unknown".

This indicates Sectigo's OCSP responder purges expired MJB certificates from its status database within days — not weeks or months — of expiration. The effect is permanent: once a serial number is purged from the OCSP database, there is no mechanism by which it could be returned to the "good" or "revoked" state. The certificate becomes cryptographically orphaned. For every Sectigo-chained certificate in the corpus, the window during which a "good" OCSP response could be obtained has now closed.

This is not a defect — it is the normal end-of-life behavior for expired certificates in a well-managed OCSP infrastructure. But it does have a specific consequence for the corpus: the OCSP responses captured in this batch query represent the last external attestation of these certificates' status that will ever exist. Any subsequent verification attempt will return "unknown" with no recovery path.

The Frisch Canary

Chief Judge Jennifer Frisch's certificate is the last Sectigo-chained leaf in the corpus that still returns "good". It expires on May 2, 2026 — 29 days after this report's underlying data capture. When it expires, if the same pattern holds, it will also transition to "unknown" within days. A follow-up OCSP query against this specific certificate is recommended on or shortly after May 3, 2026. If it transitions to "unknown" consistent with the other 7, this confirms the OCSP-purge behavior is a systematic property of Sectigo's responder for MJB certificates. If it is instead renewed under Sectigo (returning "good" for a new serial), this confirms that the MJB's Sectigo Enterprise PKI agreement remains in force for human signers — and strengthens the observation that the MCRO Watermark migration was a targeted choice rather than a blanket infrastructure decision.

Finding 5: Implications for the 4,251-PDF Forensic Corpus

Background

The corpus that supplied the data for this report was captured over an extended collection window and anchored to the Bitcoin blockchain through the hash-loop evidence-capture system documented in the Part 1 and Part 2 companion reports. The vast majority of documents in the corpus were served by MCRO while the Sectigo-chained watermark certificate was valid. This finding examines what the transition means for the cryptographic status of the corpus going forward.

Findings

The companion Digital Signature Authentication Report established that 4,206 of 4,251 corpus PDFs (98.94%) carry an MCRO Watermark signature. Of those, 4,186 (per the deduplicated registry's per-cert PDF appearance count for REG#003) were signed using the old Sectigo-chained certificate. A small number of corpus PDFs carry the earlier internal-AD-CS-chained MCRO Watermark certificate (REG#036, valid May 2023 → May 2024). The corpus predates the March 2026 transition; no documents in the corpus are signed by the new courts-J00PCERTCA-CA-chained replacement.

What Remains Verifiable

- **Signature-level integrity:**
The cryptographic validity of the 4,186 Sectigo-chained MCRO Watermark signatures is not affected by the cert's expiration or by the OSCP "unknown" status. Signature validity is determined at signing time, not at verification time. A signature computed with a valid cert during that cert's validity window remains mathematically verifiable as long as: (a) the hash algorithm has not been broken, (b) the signer's private key has not been published, and (c) the signed document's byte content is unchanged. All three conditions hold for the Sectigo-chained MCRO Watermark signatures in the corpus.
- **No-edits-after verification:**
The determination that 100% of MCRO-watermark-signed PDFs show no post-signing modifications is an integrity check against the signed byte ranges — it does not require contacting any CA. This property of the corpus is permanent.
- **Certificate chain validation:**
Because the full MJB Issuing CA certificate and MJB Root CA certificate are preserved in the provenance package (and in every PDF's embedded signature block), the full certificate chain can be reconstructed and verified offline for any corpus document by any third party, at any point in the future.
- **Blockchain attestation:**
The SHA-256 hashes of the 9 authentication package artifacts anchored to Bitcoin blocks 923904–923906 on November 16, 2025 — per the Digital Signature Authentication Report — remain immutable. The OTS-stamped April 3, 2026 snapshot package (87 MB, 36,039 files) adds a second blockchain attestation layer that freezes the full registry, OSCP responses, and cross-reference data. Neither anchoring can be retroactively altered without breaking Bitcoin itself.

What Has Become Harder to Verify

- **Real-time revocation check:**
Before April 2, 2026, any third party could query `ocsp.enterprise.sectigo.com` to confirm the MCRO Watermark certificate was not revoked. After expiration, the OCSP endpoint returns "unknown" rather than "good" — making this particular form of external attestation no longer available for the Sectigo-chained corpus. Mitigation: the CRL snapshot anchored in the Digital Signature Authentication Report (October 23, 2025) remains blockchain-anchored as historical evidence that the certificate was not revoked as of that date.
- **Fresh documents served after March 9, 2026:**
Any document newly downloaded from MCRO on or after that date carries the new internal-CA-chained signature, which cannot be independently validated without access to the MJB's internal LDAP directory. Third parties attempting to replicate the corpus going forward will find they cannot verify the new documents with the same external tooling that worked on the Sectigo-chained corpus.

Significance

The corpus is a closed set with respect to the Sectigo-chained signature. No new documents can be added to it under that cryptographic chain; the chain has reached its historical endpoint. This is, counterintuitively, a strengthening of the corpus's evidentiary character rather than a weakening of it. A closed set that predates an infrastructure change is simpler to authenticate than an open set that spans one: every document in the corpus was captured under a known, documented, publicly-verifiable cryptographic regime, and that regime can no longer produce additional documents that might later be added or substituted.

The observation that the signing infrastructure has been reduced in external verifiability after the corpus was captured does not diminish the corpus's authenticity — it distinguishes the corpus from what comes after. Documents downloaded before the transition carry a signature that any third party with internet access can validate back to a publicly-trusted root. Documents downloaded after the transition require trusting the Minnesota Judicial Branch to vouch for itself. The corpus is on the side of history where external verification was possible.

Finding 6: Provenance Snapshot Package and Blockchain Anchoring

Background

To preserve the full context of the signature sweep, cert registry, and OSCP verification as a single evidentiary unit, the entire output of the three forensic scripts was bundled into a single compressed archive and anchored to the Bitcoin blockchain via OpenTimestamps. This finding documents the snapshot package and its anchoring.

Findings

Snapshot filename	MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip
Archive size	87 MB / 36,039 files
Snapshot timestamp (UTC)	2026-04-03T08:03:16Z
OTS anchor: zip file	MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.ots
SHA-256 receipt file	MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.sha256
OTS anchor: hash receipt	MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.sha256.ots

Package Contents Summary

- **Per-PDF signature JSON files:**
4,251 individual JSON records (one per corpus PDF) detailing every signature field, every certificate in the chain, and every signed/unsigned CMS attribute.
- **Canonical certificate registry:**
59 unique certs as both .cer (DER) and .pem files, organized by registry ID and classified by PKI layer and functional role.
- **Raw PKCS7/CMS signature blobs:**
5,161 .p7b files — the raw signature containers from every PDF signature field, preserved byte-for-byte for independent parsing.
- **Cross-reference CSV:**
every cert mapped to every PDF it appeared in, every signature it produced, and every timestamp associated with those signatures.
- **OCSP signed responses:**
9 .ocsp.der files from Sectigo's responder, each cryptographically signed by the MJB Issuing CA. These are self-authenticating evidence of the cert status at query time.
- **CRL snapshots:**
Raw DER-encoded CRLs from both the MJB Issuing CA (159 revoked entries) and MJB Root CA (0 revoked entries).
- **Master manifest:**
MANIFEST.sha256 with per-file hashes for every file in the package, enabling granular integrity verification.

- **Source scripts:**
mcro_sig_extract.py, mcro_cert_registry.py, and mcro_ocsp_batch.py — the three open-source Python scripts used to produce the entire dataset, preserved with the data they generated.

Additional New MCRO Watermark Cert Package

A secondary package preserves the new (post-transition) MCRO Watermark certificate and the OCSP attestation of the old one's "unknown" status as a companion artifact:

File	Role
MCRO.cer	New MCRO Watermark leaf certificate (DER)
MJBIssuingCA.crt	Internal AD CS issuing/root certificate for new cert chain (DER)
MJBIssuingCA__ocsp__2026-04-03T01-00-00.txt	Full text output of OCSP query for the old (now-expired) cert
MJBIssuingCA__ocsp__2026-04-03T01-00-00.txt.ots	OpenTimestamps Bitcoin anchor for the OCSP text output
MJBIssuingCA__ocsp__2026-04-03T01-00-00.png	Terminal screenshot of the OCSP query session (visual evidence)
MJBIssuingCA__ocsp__2026-04-03T01-00-00.png.ots	OpenTimestamps Bitcoin anchor for the terminal screenshot
MJBIssuingCA__ocsp__2026-04-03T01-00-00.zip	Combined package of OCSP text, screenshot, certs, and related artifacts
MJBIssuingCA__ocsp__2026-04-03T01-00-00.zip.ots	OpenTimestamps Bitcoin anchor for the combined package

Significance

The snapshot package and its OTS anchors mean that every observation in this report is supported by provably-timestamped primary evidence. Any third party in possession of these files can recompute the SHA-256 of the zip archive, verify it against the .ots receipt, confirm the Bitcoin anchor, and from that point forward know with mathematical certainty what the full cryptographic state of the MCRO infrastructure looked like at 2026-04-03T08:03:16Z. The data underlying this report is not an assertion that could later be disputed — it is a single frozen object whose contents cannot be changed after the fact without breaking the blockchain.

5. LIMITATIONS & ALTERNATIVE EXPLANATIONS

What this report proves

- The old MCRO Watermark certificate was issued by Sectigo-hosted infrastructure, was valid April 2, 2024 through April 2, 2026, and published its revocation data on public HTTP endpoints.
- The new MCRO Watermark certificate is issued by the Minnesota Judicial Branch's internal AD CS infrastructure, is valid March 9, 2026 through March 9, 2027, and does not publish revocation data on any public endpoint.
- As of 2026-04-03T07:57:37Z, Sectigo's OCSP responder returned "unknown" for all 7 expired Sectigo-chained MJB certificates in the corpus and "good" for the 1 still-valid leaf (Frisch) and the long-lived intermediate CA.
- None of the 9 queried certificates appear on the MJB Issuing CA's CRL (159 other revoked serials) or the MJB Root CA's CRL (0 revoked serials) as of 2026-04-02 19:40 UTC.
- Every Sectigo-chained leaf certificate in the corpus except the MCRO Watermark belongs to a human-identified signer or an automated service account, and only the MCRO Watermark has been demonstrably reissued under the internal CA.

What this report does not prove

- This report does not establish motive or intent behind the Minnesota Judicial Branch's decision to reissue the MCRO Watermark under its internal CA rather than renewing it under Sectigo. That decision may have legitimate administrative, policy, or security rationales not observable from the cryptographic artifacts alone.
- This report does not claim that the new certificate is cryptographically inferior or weaker — it uses the same RSA 2048-bit key length, a stronger hash algorithm (SHA-512 vs. SHA-384), and a shorter validity window (all generally good security practices). The observation is about external verifiability, not about cryptographic strength.
- This report does not claim the MCRO Watermark signatures on the corpus are any less mathematically valid. Signature validity is determined at signing time and does not change when the signing certificate expires.
- This report cannot rule out that the human-signer certificates (Koch, Meyer, Lucid, Rutherford-Block, Dayton Klein) will eventually also be reissued under the internal CA. The current observation is limited to the state of the infrastructure as of the snapshot date.
- The OCSP "unknown" status for expired certificates is a property of Sectigo's OCSP implementation behavior; other CA implementations may handle expired certificates differently. The observation is specific to this infrastructure at this moment.

Alternative interpretations of the transition

- **Cost reduction:**

The MJB may be migrating off Sectigo to reduce enterprise PKI licensing costs. However, Chief Judge Frisch's cert remaining on Sectigo (valid through May 2, 2026) and returning "good" on OCSP as of April 3, 2026 is evidence against a blanket cost-driven migration. If the Sectigo agreement had been terminated, all MJB certs on that chain would have been affected.
- **Operational simplification:**

Consolidating automated service signing onto on-premises AD CS may simplify operational management by keeping high-frequency signing inside the MJB's internal network. This is a plausible rationale. The observable effect is still a reduction in external verifiability for the most-applied certificate in the ecosystem.
- **Phased migration:**

The March 2026 reversion may be the first step in a broader migration of the entire MJB signing infrastructure off of Sectigo, with individual signers to follow in subsequent cycles. This possibility cannot be ruled out from the April 3, 2026 snapshot alone; follow-up data capture over the coming year will be informative.
- **Security policy change:**

An internal policy change may have determined that automated service signing certificates should not be hosted on externally-accessible commercial infrastructure. This rationale is consistent with the observation but cannot be confirmed from the cryptographic artifacts.

6. RECOMMENDATIONS FOR INDEPENDENT VERIFICATION

Every cryptographic claim in this report is designed to be independently reproducible by any third party using standard open-source tooling. The following procedures will reproduce the primary findings.

6.1 Verify the certificate transition

Download any MCRO PDF served after March 9, 2026 from the MCRO public access portal. Extract its embedded signature:

```
# Using pdfsig (from poppler-utils) or equivalent PDF-signature tool,  
# extract the Contents field of the /Sig dictionary and parse as PKCS7:  
openssl pkcs7 -in signature.p7b -inform DER -print_certs -out chain.pem  
openssl x509 -in chain.pem -text -noout | grep -E 'Issuer|Subject|Not Before|Not  
After'
```

The Issuer CN should read courts-J00PCERTCA-CA. Compare against any pre-March 2026 MCRO PDF, which should show MJB - Issuing CA.

6.2 Verify the OSCP "unknown" status

With a copy of the old MCRO.cer and the MJB Issuing CA cert (MJBIssuingCA.crt), query Sectigo's OSCP responder directly:

```
openssl ocsf \  
-issuer MJBIssuingCA.crt \  
-cert MCRO.cer \  
-url http://ocsp.enterprise.sectigo.com \  
-resp_text
```

The response will include "Cert Status: unknown" for the old MCRO Watermark serial number (3f9a4ed3d4d82120126a4ece4e415ea8), along with a signed response from the responder that can be saved and timestamped for your own records.

6.3 Verify the CRL status

Fetch the current MJB Issuing CA CRL and search for any serial number:

```
curl -o MJBIssuingCA.crl http://crl.enterprise.sectigo.com/MJBIssuingCA.crl  
openssl crl -in MJBIssuingCA.crl -inform DER -text -noout > crl.txt  
grep -i '3F9A4ED3D4D82120126A4ECE4E415EA8' crl.txt
```

The old MCRO Watermark serial will not appear on the CRL — confirming that the certificate's retirement was natural expiration, not explicit revocation.

6.4 Verify the full certificate chain for a corpus PDF

For any PDF from the corpus, the full Sectigo-chained certificate chain can be reconstructed and verified entirely offline using only the PDF itself and widely-available OpenSSL tooling:

```
# Extract the signature (all certs in chain are embedded in every signed PDF):  
pdfsig -dump input.pdf
```

```
# Or programmatically with the forensic scripts in the snapshot package:  
python3 mcro_sig_extract.py /path/to/pdfs /path/to/output
```

The output directory will contain canonical copies of every certificate in every signature chain, cross-referenced by SHA-256 fingerprint.

6.5 Re-run the OCSF batch (Frisch canary watch)

On or after May 3, 2026, re-run the `mcro_ocsp_batch.py` script against the preserved `cert_registry.json`. The expected outcome, if the pattern of the other 7 expired certs holds, is that Jennifer Frisch's certificate will transition from "good" to "unknown". A different outcome — a new "good" response from a freshly-issued Sectigo serial — would indicate continued Sectigo engagement for human signers.

6.6 Verify the snapshot's blockchain anchor

Using the OpenTimestamps CLI, verify the snapshot zip's blockchain anchor:

```
ots verify MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.ots
```

This confirms the exact binary contents of the snapshot archive were committed to the Bitcoin blockchain at the time of creation, and that every artifact inside — every cert, every OCSF response, every PKCS7 blob — existed in the form documented in this report as of that moment.

APPENDIX: Reproducible Commands & Data References

A1. Old MCRO Watermark Certificate — Key Attributes (Pre-March 2026)

Subject: O=State of MN Judicial Branch,
CN=Minnesota Court Records Online (MCRO) Watermark
Issuer: CN=MJB - Issuing CA, O=MJB, ST=Saint Paul, L=Minnesota, C=US
Serial: 3f:9a:4e:d3:d4:d8:21:20:12:6a:4e:ce:4e:41:5e:a8
Validity: Apr 2 12:47:01 2024 GMT → Apr 2 12:47:01 2026 GMT
Sig alg: sha384WithRSAEncryption
Public key: RSA 2048-bit
SHA-256: 84b5a55aee3a8f99d44e8f7266bb31ba71a78e5a64606a7e5d88bab19849ae10
SHA-1: 070ff79f028899ee39b6b435b604950344c44cea
CRL DP: <http://crl.enterprise.sectigo.com/MJBIssuingCA.crl>
OCSP: <http://ocsp.enterprise.sectigo.com>
CA Issuers: <http://crt.enterprise.sectigo.com/MJBIssuingCA.crt>
SAN email: AS-PublicAccess-Prod@courts.state.mn.us

A2. New MCRO Watermark Certificate — Key Attributes (Post-March 2026)

Subject: DC=us, DC=mn, DC=state, DC=courts,
OU=State, OU=(Service Accounts), OU=Azure_NoSync,
CN=Minnesota Court Records Online (MCRO) Watermark
Issuer: DC=us, DC=mn, DC=state, DC=courts,
CN=courts-J00PCERTCA-CA
Serial: 1e:00:04:c4:b1:36:39:d3:a5:00:54:d4:17:00:01:00:04:c4:b1
Validity: Mar 9 13:28:32 2026 GMT → Mar 9 13:28:32 2027 GMT
Sig alg: sha512WithRSAEncryption
Public key: RSA 2048-bit
SHA-256: 045901a1920634d7f1123a0b6d89cf89199b8571bba7e92af3db6d668dd71531
SHA-1: 15aee8386ca8a11d6ab54be01ab30a1218b49a04
CRL DP: [ldap:///CN=courts-J00PCERTCA-CA,CN=J00PCERTCA,CN=CDP,
CN=Public%20Key%20Services,CN=Services,
CN=Configuration,DC=courts,DC=state,DC=mn,DC=us](ldap:///CN=courts-J00PCERTCA-CA,CN=J00PCERTCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=courts,DC=state,DC=mn,DC=us)
OCSP: (none)
CA Issuers: <ldap:///CN=courts-J00PCERTCA-CA,CN=AIA,...>
SAN: othername UPN: AS-PublicAccess-Prod@courts.state.mn.us

A3. OSCP Query Command (Reproducible)

```
openssl ocsf \
  -issuer MJBIssuingCA.crt \
  -cert MCRO.cer \
  -url http://ocsp.enterprise.sectigo.com \
  -resp_text \
  -respout MJBIssuingCA__ocsp_response.der
```

A4. Provenance Snapshot Package Structure

```
.
├─ mcro_cert_registry.py
├─ mcro_ocsp_batch.py
├─ mcro_sig_extract.py
├─ MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip
├─ MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.ots
├─ MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.sha256
├─ MCRO_SigExtraction_Snapshot_2026-04-03T08-03-16Z.zip.sha256.ots
├─ new_mcro_watermark_cert/
│   ├─ MCRO.cer
│   ├─ MJBIssuingCA.crt
│   ├─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.png
│   ├─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.png.ots
│   ├─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.txt
│   ├─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.txt.ots
│   ├─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.zip
│   └─ MJBIssuingCA__ocsp__2026-04-03T01-00-00.zip.ots
```

A5. Full Registry Summary by PKI Layer

Sectigo Enterprise (MJB Root):	2 certs	(2023-12-06 → 2058-12-06)
Sectigo Enterprise (MJB - Issuing CA leaves):	8 certs	(2024-03-14 → 2026-05-02)
Internal AD CS (courts-J00PCERTCA-CA):	39 certs	(2018-11-21 → 2032-11-04)
Legacy E-Filing (MN Courts Signing CA):	9 certs	(2013-05-13 → 2038-01-18)
Vendor (ESolutions):	1 cert	(2014-03-19 → 2039-12-31)

Total: 59 unique certs

Externally verifiable: 9 / 59 (only Sectigo-chained leaves + Intermediate CA)

Currently valid: 6 / 59 (as of 2026-04-03)

Expired: 53 / 59

A6. Related Artifacts in Companion Reports

- **Digital Signature Authentication Report (March 2026):**
establishes that 4,206 of 4,251 PDFs (98.94%) carry MCRO Watermark signatures; 100% no-edits-after rate; full authentication package anchored to BTC blocks 923904–923906 on 2025-11-16.
- **Hash-Loop Evidence Capture Part 1 (March 2026):**
authenticates the capture system itself; 100% verification across 70 bundles, 137 OTS receipts, 137 Roughtime proofs.
- **Hash-Loop Evidence Capture Part 2 (March 2026):**
99.8% SHA-256 match rate across 2,672 cases between bundle captures and the independently-anchored docket PDF registry.

End of Report — MCRO Watermark Certificate Transition: PKI Reversion Analysis & OCSP Status Snapshot