Cryptographic Weaknesses in the SAT FIEL PKI Infrastructure:
A Static and Structural Analysis of Mexico's Tax Identity Framework

Certificate Lifecycle, Key Protection Schemes, and Password-Based Encryption Vulnerabilities

Eduardo Dorantes
Independent Security Researcher
github.com/doranteseduardo · March 2026

ABSTRACT

This paper presents a structural and cryptographic analysis of the FIEL (Firma Electrónica Avanzada) digital identity infrastructure operated by Mexico's Servicio de Administración Tributaria (SAT). Through static analysis of the three artefacts issued to taxpayers — an X.509 v3 certificate (.cer), an encrypted PKCS#8 private key (.key), and a PKCS#10 certificate signing request (.req) — the author documents a series of cryptographic design decisions that, in combination, represent a material security concern for the approximately 27 million active FIEL holders in Mexico. Key findings include: a PBKDF2 key derivation scheme with 2,048 iterations (nearly three orders of magnitude below current NIST guidance), a deprecated 3DES-CBC cipher for private key protection, SHA-1 in certificate requests, and an 8-byte PBKDF2 salt. A proof-of-concept attack pipeline is documented — including exact tooling, parameters extracted from the .key structure, and throughput measurements derived from public GPU benchmarks — to quantify the practical attack surface. No private key material, cryptographic secrets, or personal data belonging to third parties are disclosed herein. All analysis was performed on artefacts obtained through the author's own FIEL enrolment.

Keywords: PKI, FIEL, e.firma, SAT, PBKDF2, 3DES, key derivation, password cracking, X.509, PKCS#8, Mexico, e-government, cryptographic analysis, responsible disclosure

1. INTRODUCTION

The FIEL (Firma Electrónica Avanzada) — rebranded as e.firma in 2017 — is Mexico's national qualified electronic signature scheme, administered by the Servicio de Administración Tributaria (SAT). It serves as the primary digital identity credential for tax filings, government procurement, corporate registration, and a growing range of legal and financial transactions. Possession of a valid FIEL is effectively mandatory for any registered taxpayer or legal entity in Mexico.

The credential consists of three files issued at enrolment: an X.509 certificate (.cer) signed by the SAT Certification Authority, an RSA-2048 private key (.key) encrypted under a user-chosen password, and a certificate signing request (.req) generated by the SAT's CertiSAT Web client. The security of the entire system ultimately depends on the strength of the password-based encryption protecting the private key —

since compromise of that key enables an adversary to sign arbitrary tax documents, corporate filings, or government contracts with full legal validity.

This research was motivated by an observation during routine handling of the author's own FIEL artefacts: the PKCS#8 structure of the .key file uses parameters inconsistent with current cryptographic best practice. This paper documents those parameters, quantifies their security implications against applicable standards, presents a documented proof-of-concept attack pipeline, and proposes concrete remediations.

2. ARTEFACT STRUCTURE

The FIEL credential set comprises three DER-encoded binary files. Their structure was verified through OpenSSL 3.0 and ASN.1 parsing tools.

2.1 Certificate (.cer) — X.509 v3

The certificate is a standard X.509 v3 DER-encoded file signed by the SAT Certification Authority. Key parameters:

Field	Value
Version	X.509 v3
Signature Algorithm	sha256WithRSAEncryption
Public Key	RSA-2048
Key Usage	Digital Signature, Non Repudiation, Data Encipherment, Key Agreement
Extended Key Usage	E-mail Protection, TLS Web Client Authentication
Basic Constraints	CA:FALSE (critical)
Validity	4 years — Aug 2022 to Aug 2026
Issuer OID	SAT970701NN3 — SERVICIO DE ADMINISTRACION TRIBUTARIA
Serial Encoding	ASCII decimal digits in DER INTEGER — non-standard (see §4.2)

Table 1. X.509 certificate parameters extracted from .cer artefact.

A notable non-standard behaviour is the encoding of the certificate serial number: the SAT stores it as the ASCII bytes of its decimal representation rather than a true DER INTEGER. This is a conformance deviation from RFC 5280 §4.1.2.2 but does not constitute an exploitable security vulnerability.

2.2 Private Key (.key) — PKCS#8 Encrypted

The private key file is a DER-encoded EncryptedPrivateKeyInfo structure (RFC 5958). ASN.1 parsing exposes the complete encryption parameter set:

```
SEQUENCE {
  SEQUENCE {
    OID  : PBES2            (1.2.840.113549.1.5.13)
    SEQUENCE {
      SEQUENCE {
        OID  : PBKDF2       (1.2.840.113549.1.5.12)
        SEQUENCE {
          OCTET STRING : <8-byte salt>   -- 64 bits
          INTEGER      : 2048            -- iteration count
        }
      }
      SEQUENCE {
```

```
    OID  : des-ede3-cbc  (1.2.840.113549.3.7)
    OCTET STRING : <8-byte IV>
   }
  }
 }
 OCTET STRING : <1,224-byte encrypted key material>
}
```

Parameter	SAT Value	NIST / Standard Requirement	Status
KDF	PBKDF2	Acceptable (RFC 8018)	OK
PRF	HMAC-SHA1	SHA-256 preferred (SP 800-132)	WARN
Iterations	2,048	≥ 600,000 SHA-1 (SP 800-132, 2023)	FAIL ✗
Salt length	8 bytes (64 bit)	≥ 128 bits / 16 bytes (SP 800-132)	FAIL ✗
Cipher	3DES-CBC	AES required; 3DES disallowed ≥2023 (SP 800-131A r2)	FAIL ✗
RSA key size	2,048 bits	Acceptable to 2030 (SP 800-57)	OK

Table 2. PKCS#8 encryption parameters. Critical rows highlighted. Iteration count row shaded as the primary vulnerability.

2.3 Certificate Signing Request (.req) — PKCS#10

The .req file is a PKCS#10 CertificationRequest (RFC 2986) in DER encoding, generated by the SAT's CertiSAT Web application. Two noteworthy elements were identified.

First, the CSR is signed with sha1WithRSAEncryption, while the resulting certificate is issued with sha256WithRSAEncryption. This asymmetry indicates that CertiSAT Web has not been updated despite SHA-1 being deprecated for digital signatures since NIST SP 800-131A (2011) and retired by major CAs in 2015–2017.

Second, the CSR contains a challengePassword attribute (OID 1.2.840.113549.1.9.7) with a base64-encoded 20-byte value — the exact size of a SHA-1 digest. Its derivation is not publicly documented by the SAT, suggesting some derivative of the enrolment password or session nonce is embedded in the CSR, warranting further protocol analysis.

3. CRYPTOGRAPHIC ANALYSIS

3.1 PBKDF2 Iteration Count — Primary Vulnerability

PBKDF2 (RFC 8018) derives a symmetric key from a password by iterating HMAC-SHA1 a configurable number of times. The iteration count is the primary mechanism for imposing computational cost on offline brute-force: an attacker who obtains the .key file must execute PBKDF2 for every candidate password tested.

The SAT uses 2,048 iterations. NIST SP 800-132 (2023) requires a minimum of 600,000 iterations for PBKDF2-HMAC-SHA1. OWASP's Password Storage Cheat Sheet (2024) recommends 1,300,000. The SAT's value is 293× to 635× below these thresholds, with a proportional reduction in attack cost.

3.2 3DES-CBC — Deprecated Cipher

Triple DES (des-ede3-cbc) was formally disallowed by NIST for all new applications from 2023 onwards (SP 800-131A Rev.2). The SAT is issuing credentials in 2025–2026 using this disallowed cipher. AES-256-GCM is the appropriate replacement, providing authenticated encryption and eliminating the 64-bit block size constraint that underlies the Sweet32 attack (CVE-2016-2183).

3.3 Salt Length

The observed PBKDF2 salt is 8 bytes (64 bits). NIST SP 800-132 recommends a minimum of 128 bits (16 bytes), generated from a CSPRNG. While 8 bytes prevents universal rainbow tables, it permits targeted precomputation against known password patterns (e.g., RFC-derived passwords, common Mexican password sets) at marginal additional cost.

3.4 Key Pair Integrity

Verification of the RSA modulus across the .cer and decrypted .key confirmed that both share an identical modulus — the credential pair is intact and untampered. This confirms the analysis targets a validly issued SAT credential.

4. PROOF-OF-CONCEPT ATTACK PIPELINE

This section documents the complete attack methodology that a well-resourced adversary would employ against a stolen FIEL .key file. The pipeline is presented for scientific reproducibility. No attack was executed against third-party credentials; parameters shown are derived from the author's own artefact. All tooling referenced is publicly available and widely used in security research.

4.1 Extracting Attack Parameters from the .key File

The PKCS#8 structure yields all parameters required to configure a targeted offline attack via standard ASN.1 parsing:

```
# Step 1 — Parse the PKCS#8 header to extract PBKDF2 parameters
$ openssl asn1parse -inform DER -in Claveprivada_FIEL.key

Output (relevant fields):
    6:d=2  OID : PBES2
   21:d=4  OID : PBKDF2
   34:d=5  OCTET STRING [8 bytes] : <salt>
   44:d=5  INTEGER                : 0800  (= 2048 iterations)
   50:d=4  OID : des-ede3-cbc
   60:d=4  OCTET STRING [8 bytes] : <IV>

# Step 2 — Confirm the private key decrypts successfully (verify password)
$ openssl pkcs8 -inform DER -in Claveprivada_FIEL.key \
         -passin pass:<password> -out /tmp/key_dec.pem
=> Success: key decrypted (confirms PBES2+PBKDF2+3DES pipeline)
```

4.2 hashcat Attack Configuration

hashcat mode 12300 targets PBKDF2-SHA1. For PKCS#8 with 3DES-CBC, a custom extraction script converts the .key to a hashcat-compatible hash line embedding the salt, iteration count, IV, and ciphertext. The command structure for the attack is:

```
# hashcat mode 12300: PBKDF2-SHA1 (used by SAT FIEL .key)
# Alternatively: mode 15500 (PKCS#12 PBKDF) depending on exact framing

$ hashcat -m 12300 \
          -a 0 \
          fiel_hash.txt \
          wordlist.txt \
          --rules best64.rule \
          -O

# For pure brute-force over 6-char alphanumeric space:
```

```
$ hashcat -m 12300 \
          -a 3 \
          fiel_hash.txt \
          '?1?1?1?1?1?1' \
          -1 '?l?u?d' \
          --increment \
          -O

# Hash line format (extracted from PKCS#8 DER structure):
# $pbkdf2-sha1$2048$<base64_salt>$<base64_ciphertext_first_block>
```

4.3 Time-to-Crack Estimates: Python vs. C vs. GPU

Three implementation tiers were evaluated for the brute-force attack: Python (hashlib.pbkdf2_hmac), C with OpenSSL (PKCS5_PBKDF2_HMAC, -O3 -march=native), and GPU via hashcat. Python was benchmarked empirically at ~684/s on development hardware. C single-threaded reaches approximately 8,000/s on modern hardware (-O3, AVX2) — an 11× improvement over Python, but still CPU-bound. The meaningful leap comes from GPU parallelism: hashcat on an RTX 4090 delivers ~1,660,000/s effective throughput at 2,048 iterations — approximately 2,200× faster than Python and 207× faster than C single-thread. PBKDF2 is intentionally resistant to GPU acceleration (sequential hash iterations), but the SAT's low iteration count of 2,048 still makes GPU attacks highly practical.

Charset / Len	Keyspace	Python ~684/s	C 1-core ~8,000/s	C 16-core ~128,000/s	RTX 4090 ~1.66M/s
alnum len=4	14,776,336	6.0 hrs	30.7 min	1.9 min	8.9 sec
alnum len=5	916,132,832	15.5 days	31.8 hrs	2.0 hrs	9.2 min
alnum len=6	56,800,235,584	2.6 years	82.2 days	5.1 days	9.5 hrs
alnum len=7	3,521,614,606,208	163 years	14.0 yrs	318 days	24.6 days
alnum len=8	218,340,105,584,896	>10K yrs	865 yrs	54.1 yrs	4.2 yrs
alnum len=9	13,537,086,546,263,552	>600K yrs	>53K yrs	>3,300 yrs	258 yrs
[A-Z0-9] len=4	1,679,616	40.9 min	3.5 min	13.1 sec	1.0 sec
[A-Z0-9] len=5	60,466,176	1.0 day	2.1 hrs	7.9 min	36.4 sec
[A-Z0-9] len=6	2,176,782,336	36.8 days	3.1 days	4.7 hrs	21.9 min
[A-Z0-9] len=7	78,364,164,096	3.6 yrs	113 days	7.1 days	13.1 hrs
[A-Z0-9] len=8	2,821,109,907,456	130 yrs	11.2 yrs	255 days	19.7 days
[A-Z0-9] len=9	101,559,956,668,416	>4,700 yrs	403 yrs	25.2 yrs	1.9 yrs

Table 3. Exhaustive brute-force ETA across implementation tiers. C rate estimated at 8,000/s per core on modern hardware (-O3, AVX2); GPU from hashcat public benchmarks (hashcat.net, 2024). Green = under 1 min. Yellow = under 1 hr. Orange = under 1 day.

The C implementation offers a meaningful speedup over Python for CPU-only scenarios — reducing a 4-character [A-Z0-9] exhaustion from 41 minutes to 3.5 minutes single-thread, and to 13 seconds with 16 threads. However, the GPU remains the dominant attack vector: the RTX 4090 is 207× faster than C single-thread and makes any password up to 6 characters in [A-Z0-9] crackable in under 22 minutes without any pattern knowledge.

Beyond generic brute-force, two additional attack strategies yield dramatically faster results by exploiting information embedded in the certificate itself. The SAT certificate exposes the holder's full name, RFC, and

CURP — all of which encode birth date and initials. A mask attack exploiting this structure reduces the effective keyspace by orders of magnitude:

Attack type	Mask / Pattern	Keyspace	GPU ETA (RTX 4090)
Generic brute-force	?1?1?1?1?1?1?1?1?1 (-1 ?u?d)	101,559,956,668,416	1.9 years
Mask: 3 uppercase + 6 digits	?u?u?u?d?d?d?d?d?d	17,576,000,000	~2.9 hours
Mask: 2 uppercase + 6 digits	?u?u?d?d?d?d?d?d	676,000,000	~6.8 minutes
Targeted: initials + birth date variants	INITIALS + DDMMYY / MMDDYY / YYYYMMDD	~100,000	< 0.1 seconds
Dictionary (rockyou.txt)	—	14,344,391	~9 seconds
Dictionary + best64 rules	rockyou + mutation rules	~900,000,000	~9 minutes

Table 4. Targeted attack strategies using certificate metadata. Red rows: attacks exploiting name/date patterns exposed in the .cer file. The targeted initials+date attack requires only the public certificate — no prior knowledge of the password.

The most significant finding is that the SAT certificate publicly discloses all information needed to construct a targeted attack: full name (initials), RFC (encodes birth date as DDMMYY), and CURP (HDFRND09 encodes sex, state, and birth date). A credential following the extremely common pattern of initials + birth date variants — as observed in the specimen artefact — is recoverable in under 0.1 seconds with no GPU required, purely from the public certificate and a targeted candidate generator.

Config	Eff. H/s (RTX 4090)	9-char [A-Z0-9] ETA	Targeted ETA
SAT FIEL — 2,048 iter	~1,660,000	1.9 years	< 0.1 seconds
NIST min — 600,000 iter	~5,667	~570 years	~18 seconds
OWASP — 1,300,000 iter	~2,615	>1,000 years	~38 seconds

Table 5. Comparative attack cost: SAT vs. NIST/OWASP targets. Note: increasing iterations does not protect against targeted attacks when the password pattern is derivable from public certificate metadata.

4.4 Local Execution Script and Artefact Policy

The attack pipeline was implemented as a self-contained Python script (fiel_attack_pipeline.py) with three operational modes: (1) single-password verification via OpenSSL subprocess or PyCryptodome; (2) dictionary attack with live progress reporting (attempts/sec, candidate count); and (3) incremental brute-force over the full alphanumeric charset with per-length progress. All operations run entirely in memory with no disk writes. The script was executed locally against the author's own FIEL artefact and confirmed the parameter values documented in §2.2 and §4.1–4.3. Benchmarked rate: 684 attempts/second on development hardware.

Artefact distribution policy: the attack script, any derived hash lines, intermediate memory dumps, cracked password material, or any execution artefact will NOT be distributed under any medium, channel, or circumstance — including private communication, version control repositories, or academic supplementary materials. The pipeline is documented here at the command and algorithm level exclusively, sufficient for independent reproduction by any researcher against their own FIEL credential.

5. STANDARDS COMPLIANCE MATRIX

Standard	Parameter	Requirement	SAT Implementation	Status
NIST SP 800-132	PBKDF2 iterations	≥ 600,000 (SHA-1)	2,048	FAIL
NIST SP 800-132	Salt length	≥ 128 bits	64 bits	FAIL
NIST SP 800-131A r2	Cipher	AES; 3DES disallowed 2023	3DES-CBC	FAIL
NIST SP 800-131A r2	Hash (CSR)	SHA-2 family	SHA-1	FAIL
NIST SP 800-57 pt1	RSA key size	≥ 2048 bits (to 2030)	2,048 bits	PASS
RFC 5280 §4.1.2.2	Serial number	DER INTEGER	ASCII decimal	PARTIAL
RFC 5280 §4.2.1.3	Key Usage	Fit-for-purpose	Overly broad	REVIEW
OWASP PCSCS 2024	PBKDF2 iter.	1,300,000 (SHA-1)	2,048	FAIL
NOM-151-SCFI-2016	Cert validity	≤ 4 years	4 years	PASS

Table 4. Compliance matrix. NIST SP 800-131A Rev.2 disallows 3DES for all new applications as of 2023.

5b. DISTRIBUTED CLOUD ATTACK ANALYSIS

Cloud GPU marketplaces such as Vast.ai, Lambda Cloud, and AWS make high-throughput GPU clusters accessible to any attacker with a credit card and no specialised hardware. This section quantifies the cost and time of a distributed PBKDF2 attack against FIEL credentials using commercially available cloud infrastructure as of March 2026.

Key insight: cost is invariant to parallelism

The total monetary cost of exhausting a given password space is constant regardless of how many GPUs are deployed. Doubling the GPU count halves the wall-clock time but doubles the hourly rate, leaving total spend unchanged. The only variable parallelism controls is time-to-completion — and with spot instances on Vast.ai at approximately $0.35/GPU-hour, that time can be reduced to minutes for the most common attack scenarios.

Attack scenario	Total cost (any config)	1x GPU	8x GPU	64x GPU	256x GPU
Targeted (initials+date, 100K)	< $0.001	60 ms	8 ms	< 1 ms	< 1 ms
rockyou dict (14M)	< $0.001	8.6 sec	1.1 sec	135 ms	34 ms
rockyou + best64 (~900M)	$0.053	9.0 min	1.1 min	8.5 sec	2.1 sec
[A-Z0-9] len=6 (2.2B)	$0.127	21.9 min	2.7 min	20.5 sec	5.1 sec
[A-Z0-9] len=7 (78B)	$4.59	13.1 hrs	1.6 hrs	12.3 min	3.1 min
[A-Z0-9] len=8 (2.8T)	$165	19.7 days	2.5 days	7.4 hrs	1.8 hrs
[A-Z0-9] len=9 (101T)	$5,948	1.9 years	88.5 days	11.1 days	2.8 days

Table 6. Cloud GPU attack cost and time (Vast.ai RTX 4090 spot, ~$0.35/GPU-hr). Cost column is constant: parallelism trades time for speed, not money. Red rows are achievable for under $1 USD total.

Mass attack: the iZED breach at scale

The December 2024 iZED leak of 111,000+ FIEL .key files enables a mass parallel attack in which each credential is attacked independently and simultaneously. Assuming an average password falls within the rockyou + best64 rules space (~900M candidates) — a conservative assumption — the total cost to attempt all 111,000 credentials is fixed at approximately $5,851 USD, regardless of the time frame chosen:

Target completion time	GPUs required	Total cost	Cost at NIST 600K iter
1 hour	~16,717	$5,851	$1,713,971 (293× more)
1 day	~697	$5,851	$1,713,971 (293× more)
1 week	~100	$5,851	$1,713,971 (293× more)
1 month	~23	$5,851	$1,713,971 (293× more)

Table 7. Mass cracking of 111,000 iZED-leaked .key files at scale. Total cost is invariant to time frame — only GPU count changes. Green column shows cost multiplier if SAT used NIST-minimum iterations.

The implication is direct: a criminal organisation with a $5,851 cloud budget — equivalent to approximately two months of a junior developer's salary — can systematically attempt to recover the passwords of every credential in the iZED dataset. With 100 GPUs over one week, the operation is undetectable, fully offline, and leaves no forensic trace on SAT infrastructure. Had the SAT implemented the NIST-minimum of 600,000 iterations, the same attack would cost $1.7 million USD — a 293× increase that renders mass cracking economically unviable for all but state-level adversaries.

6. REAL-WORLD CONTEXT: THE CHRONUS BREACH AND PRIOR SAT CREDENTIAL LEAKS

The vulnerabilities described in this paper are not theoretical. Two documented incidents in 2024–2026 confirm that the attack surface analysed here is actively exploited, and that FIEL credentials are already circulating in criminal markets.

6.1 December 2024 — Direct e.firma Credential Leak

In December 2024, a threat actor identified as 'iZED' published a dataset containing over 111,000 SAT access credentials, explicitly including e.firma passwords and private key files. This represents the first publicly documented instance of FIEL .key files circulating outside of legitimate custody. Given the 2,048-iteration PBKDF2 scheme documented in this paper, any password in that dataset — recoverable in seconds to minutes per credential on a single GPU — grants an adversary a fully operational FIEL capable of signing legally binding documents without any further access to SAT systems.

6.2 January 2026 — Chronus: 2.3 TB, 25 Institutions, 36.5 Million Records

On 30 January 2026, the criminal group Chronus — operating in coordination with groups Lizard, Blackout, and adrxx — released 2.3 terabytes of data exfiltrated from 25 Mexican public institutions, including the SAT, IMSS-Bienestar, SEP, and the Secretaría de Salud. The dataset exposed personal records of between 36 and 36.5 million Mexicans, equivalent to 29% of the national population and approximately 59% of the economically active population.

The compromised data included: full names, addresses, CURP, RFC, social security numbers, institutional email addresses, medical records, social programme registries, and complete fiscal administrative databases. This data circulated freely on Telegram and deep web marketplaces. Investigators confirmed the breach exploited compromised valid credentials and infrastructure described as over two decades old — consistent with the legacy cryptographic parameters documented in this paper.

Critically, the SAT data exposed in the Chronus breach provides exactly the metadata required to execute the targeted attack described in §4.3: full name (initials), RFC (encodes birth date), and CURP (encodes sex, state, birth date). Any FIEL holder whose RFC and name appear in the leaked dataset — potentially tens of millions — is now exposed to a targeted attack requiring under 0.1 seconds of GPU time, without access to their .key file, purely to construct the candidate list. If their .key file was also exfiltrated, the credential is fully compromised.

6.3 Documented Breach Timeline

Date	Incident	FIEL Relevance	Source
Dec 2024	Threat actor 'iZED' leaks 111,000+ SAT credentials including e.firma keys and passwords	**DIRECT — .key files and passwords published**	Revista Morelia, 2026
30 Jan 2026	Chronus releases 2.3 TB from 25 institutions; 36.5M Mexicans exposed including SAT fiscal databases	HIGH — RFC, CURP, name data enables targeted credential attacks	El Universal, Infobae, 2026
Jan 2026	ATDT confirms breached systems ran on infrastructure 20+ years old with unrevoked valid credentials	SYSTEMIC — confirms legacy crypto environment	ATDT official statement, 2026

Table 5. Documented breach incidents confirming active exploitation of the SAT credential surface.

7. IMPACT ASSESSMENT

The combination of the cryptographic weaknesses documented in §2–§5 and the confirmed breaches documented in §6 produces a concrete, active threat model. The following assessment reflects the post-breach environment as of March 2026, in which .key files and associated metadata are confirmed to be in criminal circulation.

Threat	Attack Vector	Severity	Likelihood — Post-Breach
Private key offline brute-force	iZED leak (Dec 2024) confirmed .key files in circulation; Chronus breach compounds exposure	**Critical**	**CONFIRMED ACTIVE**
Targeted attack via certificate metadata	Chronus leak exposed RFC/CURP/name for ~30M+ contributors; targeted candidate list buildable in seconds	**Critical**	**CONFIRMED ACTIVE**
CFDI invoice fraud	Compromised FIEL enables unlimited CFDI issuance; SAT itself documents billions in CFDI fraud annually	**Critical**	High
Tax identity impersonation	Filing declarations, modifying tax status, accessing SAT portal with stolen credential	**Critical**	High
Legal document fraud	FIEL carries legal presumption of authorship; no real-time revocation mechanism	**Critical**	Medium–High
Mass credential cracking	111K+ confirmed stolen .key files; 2,048-iteration PBKDF2 makes bulk cracking viable with modest GPU cluster	**Critical**	High

Table 6. Post-breach threat model as of March 2026. 'CONFIRMED ACTIVE' denotes threats with documented real-world evidence.

The legal asymmetry compounds the risk: a document signed with a compromised FIEL carries full legal presumption of authorship under the Ley de Firma Electrónica Avanzada (LFEA). The burden of proof falls on the victim to demonstrate the key was compromised — a process that requires judicial intervention and may take months or years, during which fraudulently signed documents remain legally binding.

8. RECOMMENDATIONS

#	Recommendation	Standard Basis	Priority
R1	Increase PBKDF2 iteration count to ≥ 600,000 (NIST minimum) or ≥ 1,300,000 (OWASP) for all new and renewed credentials.	NIST SP 800-132 OWASP PCSCS	**Critical**
R2	Replace 3DES-CBC with AES-256-GCM for private key encryption. GCM provides authenticated encryption; eliminates Sweet32 risk.	NIST SP 800-131A r2	**Critical**
R3	Increase PBKDF2 salt to ≥ 128 bits (16 bytes) from a CSPRNG.	NIST SP 800-132	**High**
R4	Update CertiSAT Web to generate CSRs with SHA-256 (sha256WithRSAEncryption).	NIST SP 800-131A	**High**
R5	Document and publish the enrolment protocol, including challengePassword derivation, for independent review.	Transparency best practice	Medium
R6	Enforce minimum password complexity for FIEL passwords and provide real-time strength feedback in CertiSAT Web.	NIST SP 800-63B	Medium
R7	Restrict Key Usage to Digital Signature + Non Repudiation for pure signing credentials.	RFC 5280, least privilege	Low
R8	Correct serial number encoding to comply with RFC 5280 §4.1.2.2.	RFC 5280	Low

Table 6. Prioritised remediation recommendations.

9. TOOLS AND ENVIRONMENT

Tool / Reference	Version	Purpose
OpenSSL	3.0+	Certificate parsing, key decryption, ASN.1 analysis, modulus verification
od (GNU coreutils)	8.32	Raw binary inspection of .req and .key DER structures
openssl asn1parse	3.0+	ASN.1 tree decomposition of PKCS#8 and PKCS#10 structures
hashcat	v6.2+	PBKDF2-SHA1 throughput reference; mode 12300 / 15500 for PKCS#8
Python 3	3.11+	Pipeline automation and parameter extraction scripts
RFC 8018 / RFC 5958	IETF	Normative reference for PBKDF2 and PKCS#8 structures
RFC 5280 / RFC 2986	IETF	X.509 certificate and PKCS#10 CSR profiles
NIST SP 800-132	2023	PBKDF2 iteration count and salt length guidance
NIST SP 800-131A r2	2019	Algorithm and key length transition; 3DES deprecation
OWASP PCSCS	2024	Password Storage Cheat Sheet — iteration count recommendation

Table 7. Tools and normative references.

10. CONCLUSION

The FIEL / e.firma infrastructure is a foundational component of Mexico's digital government and tax ecosystem, relied upon by approximately 27 million taxpayers for legally binding electronic signatures. The analysis presented in this paper reveals that the private key protection scheme employed by the SAT — PBKDF2 with 2,048 iterations, 3DES-CBC encryption, and an 8-byte salt — falls significantly short of current cryptographic standards on multiple dimensions simultaneously.

These are not theoretical vulnerabilities. In December 2024, over 111,000 SAT e.firma credentials including .key files and passwords were confirmed leaked. In January 2026, the Chronus group exfiltrated 2.3 TB from 25 government institutions including the SAT, exposing fiscal metadata for over 30 million contributors — precisely the data needed to construct targeted attacks against FIEL credentials in under 0.1 seconds per candidate on a GPU. The attack pipeline documented in §4 of this paper applies directly to the credentials confirmed in circulation.

The most critical finding is the PBKDF2 iteration count of 2,048 — 293× below the NIST minimum. A single RTX 4090 exhausts a 6-character [A-Z0-9] password space in under 22 minutes. For the most common Mexican credential pattern (initials + birth date), the effective attack time is under 0.1 seconds — derivable entirely from the public certificate and the Chronus breach data, without ever accessing the target's .key file. Once the key is obtained, the password is the only barrier, and that barrier is demonstrably weak.

The legal consequence is severe: a FIEL signature carries full legal presumption of authorship under the LFEA. A victim of FIEL compromise must prove — judicially, over months or years — that a signed document was not their act. Meanwhile, fraudulent CFDIs generate real tax obligations, fraudulent contracts are binding, and there is no real-time revocation mechanism.

The remediation requires no changes to certificate formats, legal frameworks, or user-facing workflows. Increasing PBKDF2 iterations to 600,000 and replacing 3DES with AES-256-GCM would raise the minimum attack cost by three orders of magnitude. The SAT has the technical capacity to implement this in a routine platform update. Given that confirmed stolen credentials are already in active circulation, there is no justification for further delay.

This research was conducted entirely on artefacts obtained through the author's own FIEL enrolment. No third-party credentials were accessed or examined. No private key material, cryptographic secrets, or personal data belonging to others are disclosed.

RESPONSIBLE DISCLOSURE NOTICE

This paper describes structural cryptographic weaknesses in a publicly deployed government PKI system, based solely on analysis of artefacts issued to the author through the standard SAT enrolment process. No authentication mechanisms were circumvented, no third-party credentials were accessed, and no private key material or personal data belonging to others are disclosed herein. The findings have been submitted to the SAT's official security contact and to CERT-MX (UNAM-CERT) prior to publication, consistent with responsible disclosure principles (ISO/IEC 29147). The author encourages the SAT to treat this report as an opportunity to modernise the FIEL key protection scheme in line with current international standards.

References.

[1] NIST SP 800-132 (2023). Recommendation for Password-Based Key Derivation. NIST.

[2] NIST SP 800-131A Rev.2 (2019). Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST.

[3] NIST SP 800-57 Part 1 Rev.5 (2020). Recommendation for Key Management. NIST.

[4] NIST SP 800-63B (2017). Digital Identity Guidelines: Authentication and Lifecycle Management. NIST.

[5] RFC 8018 (2017). PKCS #5: Password-Based Cryptography Specification Version 2.1. IETF.

[6] RFC 5958 (2010). Asymmetric Key Packages. IETF.

[7] RFC 5280 (2008). Internet X.509 PKI Certificate and CRL Profile. IETF.

[8] RFC 2986 (2000). PKCS #10: Certification Request Syntax Specification. IETF.

[9] OWASP Password Storage Cheat Sheet (2024). owasp.org/www-project-cheat-sheets.

[10] Stevens, M. et al. (2017). The First Collision for Full SHA-1. CRYPTO 2017. (SHAttered).

[11] Bhargavan, K. & Leurent, G. (2016). On the Practical (In-)Security of 64-bit Block Ciphers. CCS 2016. (Sweet32, CVE-2016-2183).

[12] NOM-151-SCFI-2016. Requisitos para la conservación de mensajes de datos y digitalización de documentos. SE, México.

[13] hashcat Performance Benchmarks (2024). hashcat.net/hashcat.

[14] SAT. e.firma (FIEL) — sat.gob.mx/tramites/16703.

[15] Salles Sainz Grant Thornton (2026). Ciberataque a SAT, IMSS y Morena expone datos de 36 millones. El Universal, 10 Feb 2026.

[16] Chronus Group (2026). Filtración de 2.3 TB — 25 instituciones públicas mexicanas. Deep web disclosure, 30 Jan 2026. Reported by: Infobae, La Silla Rota, Alto Nivel.

[17] Revista Morelia (2026). Hackeo masivo en México 2026: Chronus filtra datos del SAT e IMSS. Jan 2026.

[18] ATDT — Agencia de Transformación Digital y Telecomunicaciones (2026). Tarjeta informativa sobre el incidente Chronus. gob.mx, 31 Jan 2026.

[19] iZED (2024). Filtración de 111,000+ credenciales SAT incluyendo claves e.firma. Dec 2024. Reported by: Revista Morelia.

[20] Ley de Firma Electrónica Avanzada (LFEA). DOF, 11 Jan 2012. México.