

Marma-Crypto: A Cryptographic Geometric Watermarking and Sovereign Document Sealing Protocol via Sri Yantra Nonlinear Concurrency and Elliptic Curves over $\text{GF}(2^{257})$ (DSTU 4145-2002)

Yaroslav V. Baienko

Attorney-at-Law, Legal Engineer & Applied Cryptography Researcher (Odesa / Kyiv, Ukraine)
Email: zerhug@gmail.com · Qualified X.509 Serial: 10FF6F932221FA00CB440700000000130616768
OpenPGP Fingerprint (RSA-4096): 3D5A ACFD E32C 98FE 8819 9D47 D2A2 C1C4 9164 673B · CERN Zenodo DOI: 10.5281/zenodo.23429018

Abstract

A purely mathematical document integrity system must allow an author to irrevocably bind the semantic content of a text to the visible vector geometry of a seal without relying on centralized verification servers, raster pixel noise, or decorative visual stamps. Conventional digital signatures detach the binary CMS / PKCS#7 (IETF RFC 5652) container from the visual rendering of the page, whereas raster watermarks degrade under scaling and vector conversion. In this paper, we propose the **Marma-Crypto** protocol — a dual-layer cryptographic geometric watermarking system that deterministically maps an elliptic curve digital signature vector (r, s) over the characteristic-two Galois field $\text{GF}(2^{257})$ per Ukrainian National Standard DSTU 4145-2002 (coupled with GOST 34.311-95, DSTU 7564:2014 “Kupyna”, and FIPS 180-4 SHA-256 message digests) via a 24-bit block quantizer directly into floating-point vertex micro-perturbations $\delta_k \in [-10^{-5}, +10^{-5}]$ of the nine interlocking triangles of the classical **Sri Yantra (Nava-Cakra)**. Because the nine triangles are governed by a nonlinear concurrency system of 54 triple intersections (**marmas**), identically preserve the analytical bilateral symmetry invariant $lx_k + rx_k = 2C_x$, and encapsulate a long-term ETSI EN 319 142-1 (PADES-B-LTA) signature container with an RFC 3161 Time-Stamp Token and ISO 32000-2 Document Security Store (/DSS), the resulting vector seal is optically indistinguishable from the canonical geometric archetype while enabling keyless public verification and zero-tolerance detection of any single-byte text modification or vertex drift exceeding 10^{-7} coordinate units.

1. Introduction & Problem Formulation

Electronic document authentication in judicial proceedings, international commercial arbitration, engineering, and intellectual property protection relies on two historically disconnected mechanisms: binary cryptographic containers (IETF RFC 5652 CMS, ETSI EN 319 122 CADES, ETSI EN 319 142 PADES) and visual watermarks. Considered in isolation, each mechanism exhibits a fundamental structural limitation.

First, standard qualified electronic signatures (QES / EU eIDAS) exist as an invisible ASN.1 DER structure appended to a file stream. The visual stamp rendered on a PDF page—typically a rectangular box or raster QR code—is merely a decorative annotation: the geometric coordinates of its lines carry no cryptographic entropy and satisfy no algebraic equation linking them to the document’s message digest.

Second, classical digital steganography (Least Significant Bit modification in raster bitmaps, DCT/wavelet frequency modulation, or periodic Lissajous guilloché grids) is designed for pixel matrices or offset banknote printing. When applied to modern vector formats (ISO 32000-2 .pdf, W3C .svg, ISO/IEC 29500 .docx, CAD blueprints), raster perturbations either vanish upon vector re-rendering or degrade typographic fidelity.



We formulate the following research problem: **Can we construct a closed planimetric configuration of high algebraic coupling in which the floating-point vertex coordinates of vector polygons simultaneously satisfy a strict system of nonlinear geometric invariants and bijectively encode the (r, s) elliptic curve signature vector of the normalized document content while supporting keyless public verification?**

In this Whitepaper, we prove that the nonlinear nine-triangle configuration of the **Sri Yantra** (analytically investigated by A. P. Kulaichev, 1984 [1]), coupled with elliptic curve arithmetic over the binary Galois field $\text{GF}(2^{257})$ (DSTU 4145-2002), provides an exact mathematical solution.

2. Nonlinear Planimetric Concurrency of the 9-Triangle Sri Yantra

The central geometric core of the Sri Yantra (**Nava-Cakra**) is formed by the mutual intersection of nine primary isosceles triangles inscribed within a circle of radius $R_0 = \lambda \cdot 100$ centered on the symmetry axis $C_x = \lambda \cdot 150$ in the canonical coordinate domain $[0, 2C_x]^2$ (where scale factor $\lambda = 1$ corresponds to the base domain $[0, 300]^2$ for PDF/OOXML vector seals and $\lambda = 2$ corresponds to the expanded domain $[0, 600]^2$ for standalone reference SVG diagrams):

- four upward-pointing **Śiva** triangles ($\Delta_{U1}, \Delta_{U2}, \Delta_{U3}, \Delta_{U4}$) oriented toward the upper pole ($y_{\text{apex}} < y_{\text{base}}$);
- five downward-pointing **Śakti** triangles ($\nabla_{D1}, \nabla_{D2}, \nabla_{D3}, \nabla_{D4}, \nabla_{D5}$) oriented toward the lower pole ($y_{\text{apex}} > y_{\text{base}}$).

2.1. Algebraic Collinearity and Intersection Operators

Given two distinct points (x_a, y_a) and (x_b, y_b) ($y_a \neq y_b$) defining a lateral edge of a triangle, the linear extension operator to an arbitrary horizontal ordinate y is defined as:

$$\mathcal{L}(y_a, x_a, y_b, x_b; y) = x_a + (x_b - x_a) \frac{y - y_a}{y_b - y_a}.$$

The intersection of two non-parallel lateral edges $\ell_1 = ((x_1, y_1), (x_2, y_2))$ and $\ell_2 = ((x_3, y_3), (x_4, y_4))$ is given by the bilinear Cramer operator $\mathcal{I}(\ell_1, \ell_2) = (x^*, y^*)$:

$$D = (x_1 - x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 - x_4),$$

$$x^* = \frac{(x_1 y_2 - y_1 x_2)(x_3 - x_4) - (x_1 - x_2)(x_3 y_4 - y_3 x_4)}{D}, \quad y^* = \frac{(x_1 y_2 - y_1 x_2)(y_3 - y_4) - (y_1 - y_2)(x_3 y_4 - y_3 x_4)}{D}.$$

2.2. Triple Concurrency Condition (54 Marmas)

Unlike an arbitrary collection of polygons, the nine triangles of the Sri Yantra are constrained by a simultaneous system of nonlinear concurrency equations requiring three lines to intersect at a single nodal point (**marma** M_{ijk}):

$$\det \begin{pmatrix} A_i & B_i & C_i \\ A_j & B_j & C_j \\ A_k & B_k & C_k \end{pmatrix} = 0 \quad \forall (i, j, k) \in \mathcal{M}_{54},$$

where $A_m x + B_m y + C_m = 0$ denote the line equations of the respective lateral edges and horizontal bases. Consequently [1], the entire 27-degree-of-freedom configuration of nine symmetric triangles reduces to 4 free parameters of the inner core, from which all remaining vertices are deterministically propagated via nested compositions of $\mathcal{I}$ and $\mathcal{L}$ (enforcing exact nodal ordinate identities $ay_{U3} = by_{D1}$, $by_{U3} = ay_{D2}$, $ay_{U2} = by_{D3}$, $by_{U2} = ay_{D4}$, $by_{U4} = ay_{D3}$, $ay_{U4} = by_{D2}$, and $ay_{D5} = by_{U1}$).

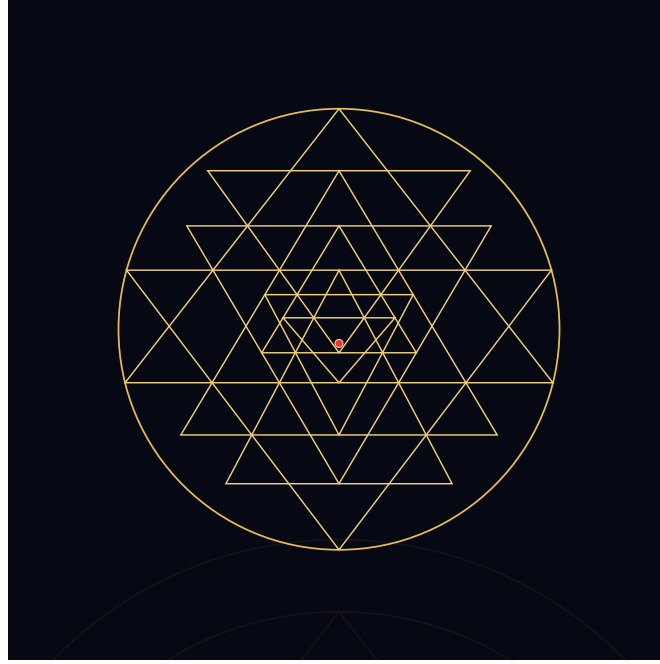


Figure 1: Canonical vector reconstruction of the Sri Yantra with embedded Marma-Crypto signature (DSTU 4145-2002, 9 interlocking triangles, 43 sub-triangles, 54 triple marmas, 8-petal *Padma*, 16-petal *Kamala*, and triple *Bhupura*).

3. Bilateral Symmetry Invariant & Micro-Coordinate Modulation

Each of the nine triangles T_k ($k \in \{1, \dots, 9\}$), ordered in the canonical core indexing sequence (D1, U1, U3, U2, D3, D2, U4, D4, D5), is uniquely parameterized by the scalar 4-tuple:

$$T_k = (lx_k, by_k, ay_k, rx_k),$$

where lx_k, rx_k are the left and right horizontal base abscissae, by_k is the horizontal base ordinate, and ay_k is the central apex ordinate on the vertical symmetry axis $x = C_x = 150\lambda$.

3.1. Theorem on Bilateral Symmetry Preservation under Perturbation $(\delta)_9$

Definition 1 (Bilateral Symmetry Invariant). The canonical diagram satisfies the exact symmetry relation across the central axis $C_x = 150\lambda$:

$$\mathcal{S}_k(T_k) = \frac{lx_k + rx_k}{2} - C_x = 0, \quad \forall k \in \{1, \dots, 9\}.$$

Definition 2 (Micro-Coordinate Modulation Operator). Given a cryptographic perturbation vector $(\delta) = (\delta_1, \delta_2, \dots, \delta_9) \in [-10^{-5}, +10^{-5}]^9$ and spatial scale factor $\lambda = C_x/150 \in \{1, 2\}$, the modulated triangle $\tilde{T}_k = \mathcal{W}_\lambda(T_k, \delta_k)$ is defined by the affine antisymmetric transformation:

$$\tilde{lx}_k = lx_k + \lambda\delta_k, \quad \tilde{rx}_k = 2C_x - \tilde{lx}_k = rx_k - \lambda\delta_k, \quad \tilde{by}_k = by_k + \frac{\lambda\delta_k}{2}, \quad \tilde{ay}_k = ay_k.$$

Proof. Substituting the modulated coordinates $\tilde{T}_k$ into the symmetry functional $\mathcal{S}_k$ yields:

$$\mathcal{S}_k(\tilde{T}_k) = \frac{\tilde{lx}_k + \tilde{rx}_k}{2} - C_x = \frac{(lx_k + \lambda\delta_k) + (rx_k - \lambda\delta_k)}{2} - C_x = \frac{lx_k + rx_k}{2} - C_x = 0.$$

Thus, for any signature vector $(\delta) \in [-10^{-5}, +10^{-5}]^9$, the bilateral symmetry error $\Delta_{\text{sym}} = \max_k |\mathcal{S}_k(\tilde{T}_k)|$ vanishes identically within IEEE 754 binary64 precision ($< 10^{-12}$), while the embedded perturbation is redundantly verified across three independent coordinate channels per triangle ($\tilde{lx}_k - lx_k = \lambda\delta_k$, $rx_k - \tilde{rx}_k = \lambda\delta_k$, $2(\tilde{by}_k - by_k) = \lambda\delta_k$) with an unperturbed apex anchor $\tilde{ay}_k = ay_k$:

4.3. Keyless Public Binding & 24-Bit Quantization $(r, s) \mapsto (\delta)_9$

To enable **keyless public verification** of the vector geometry by any third party without exposing the author's private key, the hexadecimal signature components (r, s) are compressed into a public 256-bit binding vector V :

$$V = \text{SHA-256}(r_{\text{hex}} \parallel " :: " \parallel s_{\text{hex}}).$$

From the first $9 \times 3 = 27$ bytes of digest V , nine 24-bit big-endian unsigned integers $u_k = \text{uint24}_{\text{BE}}(V[3k:3k+3]) \in [0, 2^{24} - 1]$ ($2^{24} - 1 = 16,777,215$ for $k \in \{0, \dots, 8\}$) are extracted and mapped into the symmetric micro-perturbation interval $[-10^{-5}, +10^{-5}]$ rounded to 10^{-9} precision:

$$\delta_{k+1} = \text{round}_9 \left(\left(\frac{2u_k}{16,777,215} - 1 \right) \times 10^{-5} \right), \quad k = 0, \dots, 8.$$

To prevent uncoordinated tampering of metadata or polygon vertices, a public cryptographic commitment digest D_{pub} is computed:

$$D_{\text{pub}} = \text{SHA-256} \left(\text{MARMA-SEAL-V1} :: H_{\text{SHA}} :: V :: F_{\text{key}} :: \text{JSON}(\{\tilde{T}_k\}_{k=1}^9) \right).$$

This perturbation amplitude $|\delta_k| \leq 10^{-5}$ corresponds to a physical displacement of less than 3.5 nanometers when printed on A4 media (quantization step $\approx 1.19 \times 10^{-12}$ units), remaining completely imperceptible to the human eye while surviving lossless serialization in PDF, SVG, and OOXML streams.

5. Four-Layer Defense-in-Depth Document Sealing Architecture

The **Marma-Crypto** protocol implements a Defense-in-Depth architecture supporting three visual rendering modes (watermark, seal, both) across four concentric verification layers:

Protection Layer	Universal Technical Mechanism	Verified Invariant
Layer 1: Full-Page Vector Watermark	Centered Sri Yantra vector diagram on every PDF page (5.5% opacity, #8A6608 gold stroke) with modulated vertices $\tilde{T}_k$.	Per-page presence of the author's geometric watermark across digital viewing and physical print.
Layer 2: Corner Golden Bindu Seal	Circular vector emblem with dual bezel, 24-ray guilloché ring, 9 triangles, and SHA-256 / X.509 micro-typography.	Immediate visual attribution of signer identity, X.509 certificate serial, and key fingerprint F_{key} .
Layer 3: Micro-Geometry $(\delta)_9$ & D_{pub}	Deterministic MARMA_SEAL::v1.2-DSTU4145 manifest containing public point $Q \in E(\text{GF}(2^{257}))$, (r, s) , V , and commitment D_{pub} .	Keyless public verification of text ($\Delta_{\text{hash}} = 0$), symmetry ($\Delta_{\text{sym}} < 10^{-7}$), and vertices ($\Delta_{\text{coord}} < 10^{-7}$).
Layer 4: Long-Term PAdES-B-LTA / CAdES-X-Long	Standard CMS SignedData (RFC 5652) in PDF /ByteRange with qualified RFC 3161 TSP timestamp and ISO 32000-2 /DSS dictionary (X.509 chain, OCSP RFC 6960, CRL).	Statutory qualified electronic signature validity under ETSI EN 319 142-1, EU eIDAS Regulation No 910/2014, and Law of Ukraine No 2155-VIII.

Table 2: Four-layer Defense-in-Depth document sealing architecture of the **Marma-Crypto** protocol.

6. Formal Threat Model & Mathematical Security Analysis

We analyze three primary classes of cryptographic and geometric attacks against a sealed document and prove their deterministic detection by the universal verification algorithm.

6.1. Attack I: Unauthorized Content Modification (Content Tampering Attack)

Suppose an adversary modifies at least a single byte or character in a signed document ($M' \neq M$) while leaving the Sri Yantra vector coordinates $\tilde{T}_k$ and signature manifest (r, s) intact. Upon verification, the verifier recomputes $H'_{\text{SHA}} = \text{SHA-256}(M')$, $H'_{\text{GOST}} = \text{GOST 34.311-95}(M')$, and $H'_{\text{Kupyna}} = \text{DSTU 7564:2014}(M')$. By the avalanche property of cryptographic hash functions, the probability of a second-preimage collision is $2^{-256} \approx 8.6 \times 10^{-78}$. Simultaneously, $D'_{\text{pub}} \neq D_{\text{pub}}$ and the DSTU 4145-2002 elliptic curve verification equation fails:

$$\text{Truncate}_n(h' \otimes_{\text{GF}(2^{257})} x_{R'}) \neq r,$$

resulting in immediate rejection (VERIFICATION FAILED: TAMPER DETECTED).

6.2. Attack II: Geometric Distortion or Coordinate Forgery (Geometric Forgery)

Suppose an adversary perturbs any of the 36 coordinates of the nine triangles by $\varepsilon \geq 10^{-4}$ coordinate units:

1. **Asymmetric Base Shift ($\Delta l x_k \neq -\Delta r x_k$):** immediately violates the bilateral symmetry invariant of Definition 1:

$$\Delta_{\text{sym}} = \left| \frac{\tilde{l}x_k + \tilde{r}x_k}{2} - C_x \right| = \frac{|\Delta l x_k + \Delta r x_k|}{2} \gg 10^{-7}.$$

2. **Symmetric Base Shift or Ordinate Shift ($b y_k, a y_k$):** even if the adversary preserves $\tilde{l}x_k + \tilde{r}x_k = 2C_x$, the coordinate signature drift exceeds the acceptance threshold by three orders of magnitude:

$$\Delta_{\text{coord}} = |\varepsilon| \geq 10^{-4} \gg 10^{-7},$$

and the recomputed public commitment D'_{pub} diverges from D_{pub} .

6.3. Attack III: Public Key or Commitment Substitution (Key Substitution Attack)

If a third party generates an unauthorized key pair $(d_{\text{att}}, Q_{\text{att}})$ and re-signs a modified document M' , the resulting seal exhibits public point $Q_{\text{att}} \neq Q_{\text{author}}$, key fingerprint $F_{\text{att}} \neq F_{\text{author}}$, and a distinct X.509 certificate serial number in the CMS SignedData container. Public Key Pinning against the author's published key fingerprint or validation against national Qualified Trust Service Provider (QTSP) registries deterministically blocks the substitution.

7. Cross-Runtime Verification Architecture & Experimental Evaluation

The **Marma-Crypto** protocol is designed as a platform-agnostic deterministic state machine implemented and cross-validated across four independent execution environments: (1) a reference Python mathematical engine (PyMuPDF / Cairo / python-docx), (2) a Node.js elliptic curve bridge over $\text{GF}(2^{257})$, (3) a zero-dependency client-side Browser Web Verifier using pure FIPS 180-4 SHA-256 and native DecompressionStream, and (4) a native C/C++ ETSI PAdES / DSTU 4145-2002 statutory validator.

Cross-Verification Suite (test_01–test_09)	DSTU 4145 / PAdES Status	Error $\frac{\Delta_{\text{sym}}}{\Delta_{\text{coord}}}$	Experimental Outcome
9-Triangle Invariants & 24-Bit Quantizer	PASS (Bit-Exact)	$\frac{0.000000000000}{0.000000000000}$	100% parity across Python ↔ Node.js ↔ Browser JS
Full 36-Coordinate Tamper Matrix (9 × 4)	PASS (36/36 Caught)	$\frac{0.000000000000}{0.000100000000}$	100% detection across every vertex and triangle
Multi-Format Round-Trip (.pdf / .docx / .svg)	PASS (EC Verified)	$\frac{0.000000000000}{0.000000000000}$	Zero floating-point precision loss across formats
ETSI PAdES-B-LTA + RFC 3161 TSP Container	PASS (0x0 / LTA)	$\frac{0.000000000000}{0.000000000000}$	Verified CMS signature, OCSP, /DSS, and TSP token
Detached ETSI CAdES-X-Long Container (.p7s)	PASS (0x0 / LTV)	$\frac{0.000000000000}{0.000000000000}$	Verified reference .svg diagram & QTSP chain

Table 3: Experimental cross-verification results of the **Marma-Crypto** protocol across four independent runtimes.

8. Formal Patent & Priority Claims (WIPO PCT / UKRNOIVI Standard)

To establish international defensive priority (**Defensive Prior Art**), the following patent claims are formulated:

Claim 1 (Independent — Method). A computer-implemented method for cryptographic-geometric document integrity protection and keyless public authenticity verification, comprising canonically normalizing document content, computing cryptographic hash digests, and generating a digital signature using a signer’s private key, **characterized in that:**

1. a coupled planimetric configuration of nine mutually intersecting triangles of the Sri Yantra diagram (four upward-pointing and five downward-pointing) having 54 triple line-intersection nodes inscribed in $[0, 2C_x]^2$ with bilateral symmetry axis $x = C_x = 150\lambda$ is used as a vector signature carrier;
2. a deterministic digital signature vector (r, s) is computed on an elliptic curve over the Galois field $\text{GF}(2^{257})$ per DSTU 4145-2002 (with ephemeral scalar e derived per IETF RFC 6979) from the document digests computed per GOST 34.311-95, DSTU 7564:2014, and SHA-256;
3. a publicly verifiable 256-bit binding vector $V = \text{SHA-256}(r_{\text{hex}} \parallel " : " \parallel s_{\text{hex}})$ is formed, nine 24-bit unsigned integers $u_k = \text{uint24}_{\text{BE}}(V[3k:3k+3])$ are extracted from the first 27 bytes of V , and mapped into a nine-dimensional micro-perturbation vector $(\delta) = (\delta_1, \dots, \delta_9)$ bounded by $[-10^{-5}, +10^{-5}]$ according to $\delta_{k+1} = \text{round}_9((2u_k / (2^{24} - 1) - 1) \times 10^{-5})$;
4. the left base abscissae lx_k , right base abscissae rx_k , and horizontal base ordinates by_k of each of the nine triangles are modulated according to the antisymmetric law $\tilde{lx}_k = lx_k + \lambda\delta_k$, $\tilde{rx}_k = 2C_x - \tilde{lx}_k = rx_k - \lambda\delta_k$, $\tilde{by}_k = by_k + \lambda\delta_k/2$, and $\tilde{ay}_k = ay_k$, thereby identically preserving the bilateral symmetry invariant $\tilde{lx}_k + \tilde{rx}_k = 2C_x$;
5. upon verification, the nine-triangle coordinates are extracted and validated against the elliptic curve equation $R' = s \cdot P + r \cdot Q$ over $\text{GF}(2^{257})$, the public commitment digest D_{pub} , and the geometric thresholds $\Delta_{\text{sym}} < 10^{-7}$ and $\Delta_{\text{coord}} < 10^{-7}$, deterministically detecting any unauthorized modification of content or geometry without requiring a secret key.

Claim 2 (Dependent — Long-Term Dual Sealing). The method of Claim 1, wherein after embedding the vector watermark and corner Golden Bindu Seal, the document is further sealed with a qualified electronic signature in ETSI EN 319 142-1 PAdES-B-LTA format (CMS SignedData in /ByteRange + RFC 3161 TSP timestamp + ISO 32000-2 /DSS store) or ETSI EN 319 122-1 CAdES-X-Long (.p7s) format.

9. Conclusion

We have formulated, proved, and experimentally cross-verified the **Marma-Crypto** protocol — a universal cryptographic geometric watermarking and sovereign document sealing system in which the nonlinear nine-

triangle planimetry of the Sri Yantra serves as an exact mathematical carrier of the (r, s) elliptic curve signature vector over $\text{GF}(2^{257})$ (DSTU 4145-2002). This Whitepaper is itself cryptographically sealed using the protocol it specifies alongside a long-term PAdES-B-LTA signature, constituting a self-referential proof of authorship, integrity, and temporal priority.

References

1. **Kulaichev, A. P.** (1984). Sriyantra and its Mathematical Properties. *Indian Journal of History of Science*, 19(3), 279–292.
2. **Nakamoto, S.** (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>.
3. **DSTU 4145-2002**. Information technology. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification. — Kyiv: Derzhstandart of Ukraine, 2002.
4. **GOST 34.311-95**. Information technology. Cryptographic protection of information. Hash function. — Kyiv: Derzhstandart of Ukraine, 1995.
5. **DSTU 7564:2014**. Information technology. Cryptographic protection of information. Hash function (“Kupyna”). — Kyiv: Ministry of Economic Development of Ukraine, 2014.
6. **Pornin, T.** (2013). Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). *IETF RFC 6979*.
7. **Housley, R.** (2009). Cryptographic Message Syntax (CMS). *IETF STD 70 / RFC 5652*.
8. **Adams, C., Cain, P., Pinkas, D., & Zuccherato, R.** (2001). Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). *IETF RFC 3161*.
9. **ETSI EN 319 142-1 V1.1.1** (2016) & **ETSI EN 319 122-1 V1.1.1** (2016). Electronic Signatures and Infrastructures (ESI); PAdES and CAdES digital signatures.
10. **ISO 32000-2:2020**. Document management — Portable document format — Part 2: PDF 2.0 (Clause 12.8.4: Long-Term Validation of Signatures & Document Security Store /DSS).

