SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.5 NO. 4 2026
DOI: 10.51984/z4v9md96

وقائع مؤتمرات جامعة سبها
Sebha University Conference Proceedings

Conference Proceeding homepage: http://www.sebhau.edu.ly/journal/CAS

SealNet: A Secure Digital Seal Framework to Combat Forgery in Libyan Public Administration

Alhashimi Alhadad [a]* Musa Omar [b], Ibrahim Zidan[c]

[a] Department of Electrical and Electronic Engineering Faculty of Engineering Wadi Alshati University, Sokra, Sebha 3000, Libya
[b] Department of Electrical and Electronic Engineering Faculty of Engineering Wadi Alshati University, Ubari, Ubari 73, Libya
[c] Department of Electrical and Electronic Engineering Faculty of Engineering Wadi Alshati University, Brak, Alshati 68, Libya

Keywords:
Blockchain
BAN Logic
Digital Seal
E-Government
eIDAS
PKI
Quantum Agility

ABSTRACT

The transition to e-government in developing nations like Libya is critically hindered by a reliance on paper-based bureaucracy, leading to rampant administrative forgery and process inefficiency. This paper proposes ”SealNet,” a sovereign secure digital seal framework designed to establish a national trust anchor for public administration. Addressing the lack of a unified Public Key Infrastructure (PKI) and current legislative enforcement gaps, SealNet utilizes a hybrid cryptographic approach combining RSA-2048 for standard digital signatures and ECDSA-P256 for high-density, encrypted QR codes. This dual mechanism enables both online and offline verification, overcoming infrastructure limitations. The system transitions beyond mere software engineering by integrating a permissioned Blockchain for metadata anchoring to ensure robust post-issuance auditability and accountability against insider threats, and Shamir’s Secret Sharing for robust Root CA governance. We formally verify the protocol using Burrows-Abadi-Needham (BAN) logic to theoretically demonstrate strong non-repudiation properties. System validation through rigorous stress testing demonstrated a signing latency of under 200ms and successfully detected all payload tampering attempts within our specific experimental constraints. An empirical pilot study within a real-world academic registry confirmed a 98.4% offline scanning success rate and reduced administrative turnaround time by 99.8%. Under fair, identical stress-test conditions (500 req/sec), SealNet exhibited significantly lower CPU and Memory consumption compared to pure permissioned ledger models. Furthermore, the framework aligns technically with the Libyan Electronic Transactions Law No. 6 of 2022 and eIDAS standards, offering a scalable and conceptually quantum-agile transition strategy to minimize document fraud.

سيل نت: إطارعمل الختم الرقمي الآمن لمكافحة التزويرفي الإدارة العامة الليبية

الهاشمي الحداد[a]* موسي عمر[b] ، إبراهيم زيدان[c]

a قسم الهندسة الكهربائية والإلكترونية كلية الهندسة جامعة وادي الشاطئ ، سكرة ،سبها 3000 ،ليبيا.
b قسم الهندسة الكهربائية والإلكترونية كلية الهندسة جامعة وادي الشاطئ ، اوباري ،اوباري 73 ،ليبيا.
c قسم الهندسة الكهربائية والإلكترونية كلية الهندسة جامعة وادي الشاطئ ، براك ،الشاطئ 68 ،ليبيا.

الكلمات المفتاحية:
سيل نت
البنية التحتية للمفاتيح العامة
الحكومة الإلكترونية
الختم الرقمي
المرونة الكمومية
سلسلة الكتل
نظام الهوية الإلكترونية الموحد (eIDAS).

الملخص

يعيق الاعتماد على البيروقراطية الورقية التحول إلى الحكومة الإلكترونية في الدول النامية، مثل ليبيا، بشكلٍ كبير، مما يؤدي إلى انتشار التزوير الإداري وعدم كفاءة العمليات. تقترح هذه الورقة البحثية "سيل نت" (SealNet) وهو إطار عمل سيادي آمن للأختام الرقمية، مصمم لإنشاء مرجعية ثقة وطنية للإدارة العامة. ولمعالجة غياب بنية تحتية موحدة للمفاتيح العامة (PKI) والثغرات الحالية في إنفاذ التشريعات، تستخدم "سيل نت(SealNet) " نهجًا تشفيريًا هجينًا يجمع بين RSA-2048 للتوقيعات الرقمية القياسية و JECDSA-P256 رموز QRمشفرة عالية الكثافة. تُمكّن هذه الآلية المزدوجة من التحقق عبر الإنترنت وخارجه، متجاوزةً قيود البنية التحتية. يتجاوز النظام مجرد هندسة البرمجيات من خلال دمج تقنية بلوك تشين مُرخصة لتثبيت البيانات الوصفية، لضمان قابلية تدقيق قوية بعد الإصدار ومساءلة فعّالة ضد التهديدات الداخلية وتقنية مشاركة الأسرار لشامير لحوكمة قوية لهيئة إصدار الشهادات الجذرية. نُجري تحققًا رسميًا من البروتوكول باستخدام

*Corresponding author:
E-mail addresses: al.alhadad@wau.edu.ly ,(M. Omar)mo.omar@wau.edu.ly ,(I. Zidan)i.zidan@wau.edu.ly
Article History : Received 30 May 2026 - Received in revised form 30 September 2026 - Accepted 11 November 2026

منطق بوروز آبادي-نيدهام (BAN) لإثبات خصائص عدم الإنكار القوية نظريًا. وقد أظهر التحقق من صحة النظام من خلال اختبارات إجهاد صارمة زمن استجابة للتوقيع أقل من 200 مللي ثانية، ونجح في الكشف عن جميع محاولات التلاعب بالبيانات ضمن قيودنا التجريبية المحددة. وأكدت دراسة تجريبية أولية ضمن سجل أكاديمي واقعي معدل نجاح مسح ضوئي غير متصل بالإنترنت بنسبة 98.4%، وخفض وقت الاستجابة الإدارية بنسبة 99.8%. وفي ظل ظروف اختبار إجهاد عادلة ومتطابقة (500 طلب/ثانية)، أظهر SealNet استهلاكًا أقل بكثير لوحدة المعالجة المركزية والذاكرة مقارنةً بنماذج السجلات المُرخصة البحتة. علاوة على ذلك، يتوافق الإطار تقنيًا مع قانون المعاملات الإلكترونية الليبي رقم 6 لسنة 2022 ومعايير eIDAS ، مما يوفر استراتيجية انتقال قابلة للتطوير ومرنة من الناحية المفاهيمية لتقليل تزوير المستندات.

Introduction

The global paradigm shift towards e-government necessitates robust mechanisms for establishing trust in digital interactions, eliminating the need for physical presence. Digital signatures and digital seals have emerged as the fundamental technological cornerstone for ensuring data integrity, authenticity, and non-repudiation in public admin-istration [1]. They serve as the legally binding digital equivalent of traditional handwritten signatures and official rubber stamps, enabling secure and efficient remote transactions across government entities [2].

Despite these global advancements, many developing nations, including Libya, continue to rely heavily on traditional, paper-based bureaucratic processes. This deep-rooted dependence creates significant vulnerabilities in the adminis-trative workflow. Physical seals are increasingly susceptible to counterfeiting using modern high-resolution printing technologies, leading to an alarming rise in administrative forgery and fraudulent document issuance [3]. Furthermore, the manual verification of paper documents across geographically dispersed government entities is labor-intensive, time-consuming, and prone to human error, severely hindering efficient service delivery.

Addressing these critical challenges requires a strategic shift towards a unified national infrastructure for digital document security. Relying on ad-hoc solutions implemented independently by various ministries often results in interoperability issues, security gaps, and wasted resources. Therefore, there is a pressing need for a standardized, centralized, and legally recognized platform that governs the issuance and validation of official digital documents across the entire Libyan public sector [4].

To bridge this gap, this paper introduces ”SealNet,” a comprehensive secure digital seal framework specifically tailored for the Libyan administrative context. A high-level overview of the proposed SealNet ecosystem is illustrated in Fig. 1.

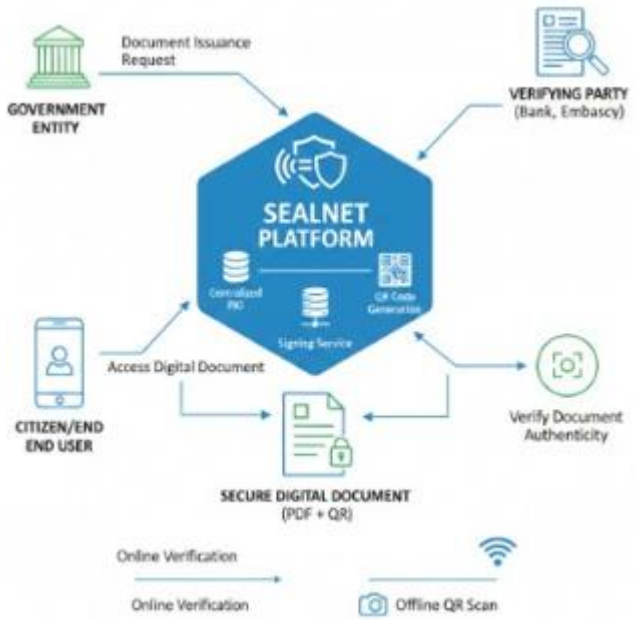


Fig. 1: High-Level Overview of SealNet Ecosystem.

As depicted in Fig. 1, the ecosystem intricately connects the governmental issuing bodies, the central SealNet processing engine, and the verifying entities through a unified cryptographic protocol, ensuring seamless end-to-end security across both digital and physical me This paper transitions beyond mere software engineering by formally defining and addressing the architectural constraints of deploying sovereign PKI in developing nations. The primary scientific contributions of SealNet are:

1. Offline-First Stateless Verification Protocol: Designing a highly compressed, ECDSA-backed payload utilizing CBOR and Deflate that shifts the verification burden from centralized databases to self-contained visual tokens, achieving strict QR Version 5 limits for low-end optical sensors.
2. Insider Threat Accountability: Unlike standard
3. implementations that implicitly trust the issuing authority, SealNet integrates a Decentralized Trust Layer (Blockchain metadata anchoring) to distribute trust and ensure strict post-issuance auditability, holding malicious insiders accountable.
4. Formal Security Proof: Employing Burrows-Abadi-Needham (BAN) Logic to theoretically prove the protocol’s resistance against replay and impersonation attacks under the Dolev-Yao adversary model.
5. Quantum Agility: Extending standard digital seals with an automated Recursive Timestamping algorithm (PAdES-LTV) and proposing a conceptual Tiered Post-Quantum Cryptography (PQC) integration roadmap to ensure quantum-agile operations beyond the current issuing key’s lifespan.diums.

Related Work

The domain of digital document authentication has witnessed significant developments. This section critically analyzes existing commercial platforms and emerging decentralized technologies.

A. Commercial vs. Sovereign Solutions

Global leaders like DocuSign offer robust SaaS models [5]. However, for sovereign government applications, these pose challenges regarding data sovereignty and high licensing costs [6]. National PKI systems, such as Estonia’s e-Residency [7], serve as benchmarks but require advanced infrastructure often unavailable in transitional governments like Libya.

B. Decentralized Identifiers (DID) and Blockchain

Recent trends advocate for Self-Sovereign Identity (SSI) using W3C Verifiable Credentials (VCs) and DIDs backed by Blockchain [24, 25]. While researchers propose Ethereum-based credentials, these models face significant hurdles in the Libyan context:

1. Latency: Public blockchains suffer from variable confirmation times (e.g., 12–15s). SealNet’s HSM signing achieves <200ms latency.
2. User Friction: DID models require users to manage digital wallets and private keys. SealNet adopts a ”Bearer Token” model (QR code).
3. Offline Verification: Most ledger-based solutions require live RPC node connectivity. SealNet’s QR code is self-contained (stateless).

Table 1: Architectural Paradigm Comparison for Transitional E-Governments

Evaluation Metric	SaaS Models	Blockchain/DID	SealNet (Proposed)
Trust Anchor	3rd Party	Decentralized	Distributed Sovereign
Insider Threat Mitiga-tion	Low	High (Consensus)	High (Auditability)
Verification Mode	Online Only	Ledger-dependent	Stateless / Fully Offline
Database Sync Load	High	High	Zero (Self-Contained)

As evident from Table 1, while pure blockchain models excel in mitigating insider threats, they fail in offline verification. SealNet captures the benefits of both paradigms by utilizing distributed sovereign hardware (HSM) for trust, paired with stateless offline tokens.

Problem Statement and Objectives

A. Problem Statement

The Libyan public sector suffers from the "Silo Effect," leading to:

1. Vulnerability to Forgery: Reliance on rubber stamps makes documents relatively easy to counterfeit [11, 12].
2. Lack of Interoperability: Absence of a unified PKI root prevents cross-ministry verification [13].
3. The Insider Threat (Malicious Issuer): Traditional centralized systems assume the issuing authority is infallible. In high-corruption environments, authorized personnel may misuse their access to generate cryptographically valid but factually fraudulent documents, exposing a critical accountability gap in standard PKI models [34].

B. Objectives

The primary aim is to propose SealNet to design a unified national platform for digital issuance, adopt a hybrid encryption approach (PKI + QR), implement decentralized metadata auditing, and theoretically establish legal non-repudiation via mathematically proven audit trails.

Proposed System Architecture

SealNet operates on a Service-Oriented Architecture (SOA) acting as a "Trust Anchor" [8]. It serves three key stakeholders: Issuing Authorities, Verifying Parties, and End Users. The overall system architecture is depicted in Fig. 2.

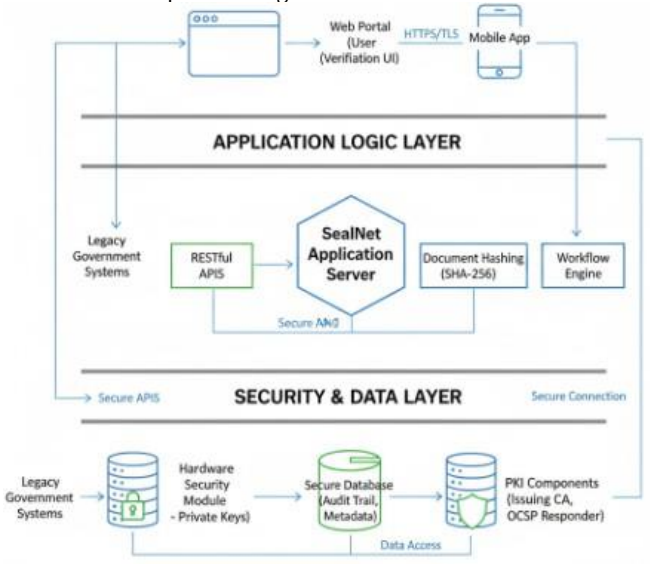


Fig. 2: System Architecture of SealNet.

As shown in Fig. 2, this layout strictly separates the application logic from the cryptographic boundary, ensuring that private keys never leave the hardware module during the signing phase, thereby minimizing application-level breaches.

A core vulnerability inherent to standard PKI models is their implicit assumption of the issuing authority's infallibility. To address "The Rogue Issuer" problem, an immutable audit trail is required. It is crucial to note that no software layer can physically prevent a highly privileged rogue administrator with valid HSM access from generating a signature at the exact moment of issuance. Instead, the goal is to provide deterministic post-issuance auditability and non-repudiation.

To achieve this, SealNet integrates a Permissioned Blockchain Consortium (e.g., Hyperledger Fabric) exclusively for metadata anchoring. The fundamental differentiator justifying the use of a blockchain over a Merkle log or an Append-Only DB is Distributed Consensus on Write Operations and Programmable Governance, not merely historical immutability.

Upon seal generation, the minimal metadata object (Hdoc, Issuer ID, Tstamp) is submitted as a transaction to a consortium of nodes operated by mutually distrustful, independent governmental watchdogs. During verification, if a document is cryptographically valid but lacks an endorsed anchor in the consortium ledger, auditors and verification clients logically flag it as an illicit internal issuance, thus establishing a robust mechanism for insider accountability.

Table 2: Architectural Comparison for the Auditing Layer

Feature	Append-Only DB	Merkle Tree Log	Permissioned Ledger
Immutability	App-Layer Only	Cryptographic	Cryptographic
Governance	Centralized	Centralized	Consortium
Write Consensus	None (Admin)	None (Operator)	Smart Contract
Split-View Def.	Vulnerable	Vulnerable	Highly Resistant

PKI Design and Key Management

A. PKI Hierarchy and Root Protection

SealNet implements a two-tier PKI hierarchy featuring an offline, air-gapped Root CA and an online Issuing CA, as shown in Fig. 3.

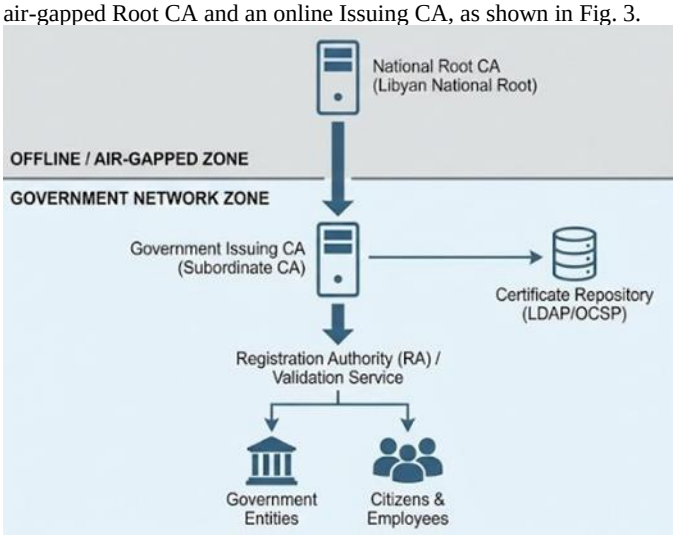


Fig. 3: National PKI Architecture.

The air-gapped isolation of the Root CA acts as a fundamental security control to prevent catastrophic systemic breaches. To limit single-point failures at the highest level, SealNet mandates a controlled "Key Ceremony" utilizing

Shamir's Secret Sharing (SSS) scheme for the Root CA's HSM activation codes [10]. SealNet implements a (3, 5)

threshold scheme, ensuring no single entity can unilaterally activate the Root CA.

B. Registration and Key Management Protocols

The onboarding process acts as the primary security firewall. Algorithm 1 outlines the strict validation logic required before any digital credentials are issued.

Algorithm 1 User/Institution Registration

```
Require: User_ID, Official_Documents
Ensure: Registration_Status
1: Receive Request(User_ID, Documents)
2: Verify(Documents) with National_Database
3: if Documents == Valid AND User_Is_Active then
4:  Create Entry in RA_Database
5:  Registration_Status = Approved
6:  Call Key_Generation_Process(User_ID)
7: else
8:    Log_Attempt(User_ID, "Failed")
9:   Registration_Status = Rejected
10: end if
11: return Registration_Status
```

Upon successful registration, Algorithm 2 details the secure initialization of the RSA-2048 key pair strictly inside a FIPS 140-2

Level 3 Hardware Security Module (HSM).

Algorithm 2 HSM Key Pair Generation

Require: User_ID, Params (RSA-2048) Ensure: Signed_Certificate
1: Generate Key_Pair (Pub_K, Priv_K) using RSA-2048
2: Store Priv_K internally inside HSM
3: Generate CSR containing Pub_K
4: Send CSR to Issuing_CA via mTLS
5: Signed_Cert = Sign(CSR, CA_Private_Key)
6: return Signed_Cert

Hybrid Cryptographic Framework

Algorithm 3 presents the hybrid signature generation logic, orchestrating the parallel usage of RSA-2048 for standard PDF interoperability and ECDSA-P256 for high-density QR code generation.

Algorithm 3 Hybrid Signature Generation

Require: Doc_File, RSA_Key, ECDSA_Key, Metadata
1: Step 1: PDF Signing
2: Doc_Hash = SHA-256(Doc_File)
3: PDF_Sig = Encrypt(Doc_Hash, RSA_Key)
4: Embed PDF_Sig into Doc_File
5: Step 2: QR Generation
6: Data = Concatenate(Metadata, Doc_Hash)
7: QR_Hash = SHA-512(Data)
8: QR_Sig = Sign_ECDSA(QR_Hash, ECDSA_Key)
9: QR_Img = Generate_QR(Encode(Metadata + QR_Sig))
10: Step 3: Integration and Anchoring
11: Final_Doc = Stamp(Doc_File, QR_Img)
12: Anchor_to_Blockchain(Doc_Hash, Metadata.Issuer)
13: return Final_Doc

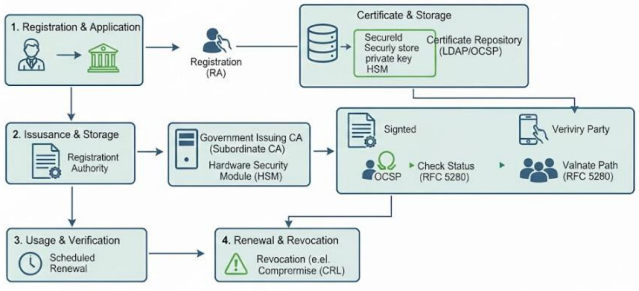


Fig. 4: Hybrid Digital Signature Workflow.

In anticipation of future quantum computing threats, applying NIST-standardized PQC algorithms like CRYSTALS-Dilithium directly to QR codes is currently infeasible due to signature sizes exceeding 2.4 KB. To maintain resilience while acknowledging current hardware constraints, we propose a Conceptual Tiered Quantum-Agile Architecture:

1. Layer 1 (Root CA & Ledger Anchoring): Utilizes a hybrid signature scheme combining classical RSA-4096 with PQC Dilithium2 for long-term backend security.
2. Layer 2 (Edge / Offline Verification): Retains classical ECDSA-P256 with aggressive payload compression (CBOR) to maintain current QR Version 5 limitations. The architecture is designed to be mathematically agile, allowing future swaps to more compact post-quantum signature schemes once standardized, serving as a transitional bridge.

Verification and Forgery Detection

Validation is the functional counterpart to issuance. Algorithm 4 describes the universal stateless verification logic utilized by verifying parties.

Algorithm 4 Stateless Hybrid Verification

Require: Input_Object, CA_PubKey
1: if Input is PDF then
2: Hash_Calc = SHA-256(Content)
3: Hash_Dec = Decrypt(Sig, Cert.PubKey)
4: Check = (Hash_Calc == Hash_Dec)
5: else if Input is QR (Physical Scan) then
6: Decode Base45(Deflate(Payload)) -> (Meta + Sig)
7: Hash_Calc = SHA-512(Meta)
8: Check = Verify_ECDSA(Hash_Calc, Sig, Key)
9: end if
10: if Check == True AND Cert_Status == Good then
11: return ”Valid Document”
12: else
13: Trigger_Forgery_Alert(Hash_Calc, Meta.Issuer)
14: return ”Invalid/Tampered”
15: end if

A. Offline Trust Store and Key Distribution

A critical requirement for the stateless QR token is the ability to verify signatures in strictly offline environments (e.g., remote checkpoints or border controls). To enable this, the mobile verification application relies on a localized, secure trust store. Upon initial installation, the application is pre-provisioned with the public keys of the national Root CA and authorized Issuing CAs.

While the cryptographic validation of the ECDSA signature occurs entirely offline, the application requires periodic, asynchronous background synchronization (e.g., daily or weekly) whenever internet access becomes available. During these sync windows, the application updates its localized Certificate Revocation List (CRL) and fetches any newly registered public keys.

To mitigate the security risk of relying on excessively stale data, the application enforces a fail-safe mechanism: if the offline period exceeds a predefined security threshold (e.g., 30 days without a successful sync), the system mandates an online connection to refresh the local trust store before permitting any further document verifications. This hybrid sync-and-verify model ensures that offline verification remains highly reliable without necessitating live RPC node connectivity at the exact point of inspection.

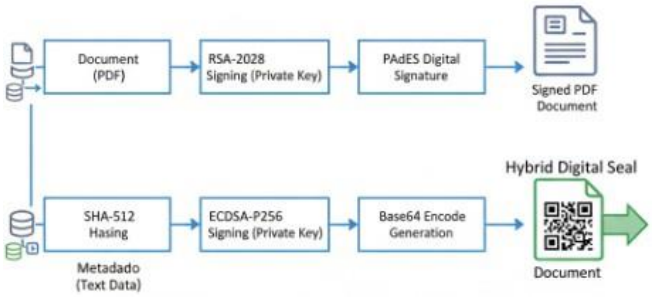


Fig. 5: Signature Verification Process.

B. Forgery Detection Module

To enhance the security posture beyond passive verification, SealNet introduces an active Forgery Detection Module.

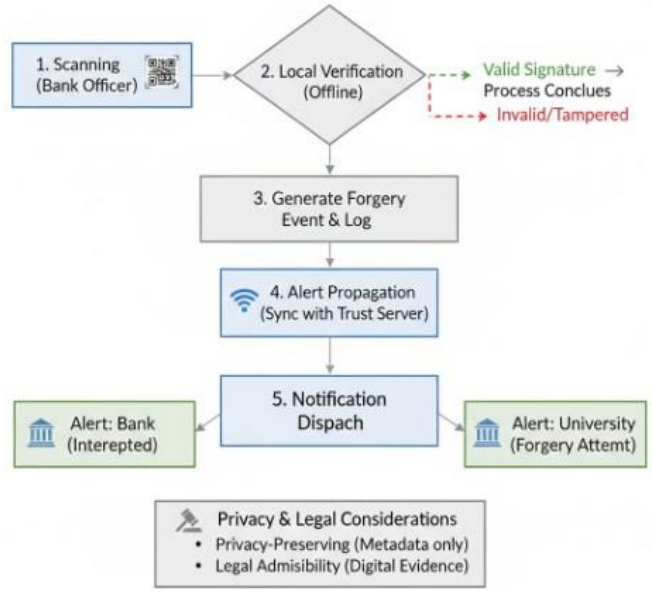


Fig. 6: Forgery Detection and Notification Workflow.

This active monitoring mechanism (Fig. 6) acts as a powerful deterrent, rapidly isolating compromised credentials and logically alerting authorities to potential coordinated attacks.

Institutional Digital Seal Model

Algorithm 5 enables the Automated Digital Seal model, which allows organizations to process batches of documents efficiently.

Algorithm 5 Automated Digital Seal Generation

Require: Batch, Org_ID
1: Authenticate App(Org_ID)
2: for all Document in Batch do
3: Hash = SHA-256(Document)
4: Sig = Sign_With_HSM(Hash, Org_Key)
5: Time = Get_Timestamp(Hash)
6: Embed(Document, Sig, Time)
7: end for

Formal Security Analysis

A. Formal Security Verification using BAN Logic

While empirical testing provides operational metrics, cryptographic protocols require formal mathematical proofs to validate their logical design. We formally model the SealNet verification protocol using Burrows-Abadi-Needham (BAN) Logic, a belief logic utilized for analyzing authentication protocols. Let I represent the Issuing Authority (HSM) and V represent the Verifying Client. Let KI denote the public key of I, and {X }K−1 denote a message X signed with I's private key. The message payload is defined as M = (Hdoc, Meta).

1. SecuritIy Goals: The verification process must satisfy two primary logical goals to formally prevent forgery and replay attacks:
   a. Goal 1 (Authentication): V |= I ∼ M (The verifier believes that the issuer once generated the document).
   b. Goal 2 (Freshness): V |= #(M) (The verifier believes the document metadata and timestamp are fresh).
2. Idealized Protocol and Initial Assumptions: The idealized core protocol for the stateless QR token transmission is expressed as:

$$I \rightarrow V : \{M, T_{stamp}\}K_I^{-1} \quad (1)$$

Before execution, we establish the following initial state assumptions (A1–A3):

- A1 (Key Trust): V |='→ KI (The verifier believes KI correctly belongs to the Issuer).
- A2 (Time Freshness): V |= #(Tstamp) (The verifier believes the timestamp is fresh, based on consensus time or synchronized system clocks).
- A3 (Jurisdiction): V | = I ⇒ (I ∼ M) (The verifier trusts the Issuer has the formal authority to issue M).

3. Logical Deduction Steps: The formal proof proceeds through the following logical deductions:

Step 1: Message Receipt

The verifier scans the QR code and receives the signed payload:

$$V \triangleleft \{M, T_{stamp}\}K_I^{-1} \quad (2)$$

Step 2: The Message Meaning Rule

Applying the Message Meaning postulate to Step 1 and Assumption A1. Since V believes KI belongs to I and sees the message signed by I's private key, V concludes that I once said it:

$$\frac{V \mid\equiv K_I \quad V \triangleleft \{M,T_{stamp}\}K_I^{-1}}{V \mid\equiv I \sim (M,T_{stamp})} \quad (3)$$

Step 3: The Freshness Promotion Rule

Applying the Freshness postulate to Assumption A2. Because the timestamp is proven fresh, the entire concatenated payload is considered fresh:

$$\frac{V \mid\equiv \#(\text{Tstamp})}{V \mid\equiv \#(M, T_{stamp})} \quad (4)$$

Step 4: The Nonce Verification Rule

By combining Step 2 and Step 3, if V believes I once said the message and that the message is currently fresh, V believes I currently believes the message:

$$\frac{V \mid\equiv \#(M,T_{stamp}),\ V \mid\equiv I \sim (M,T_{stamp})}{V \mid\equiv I \mid\equiv (M,T_{stamp})} \quad (5)$$

Step 5: Jurisdiction and Final Conclusion

Finally, applying the Jurisdiction rule combined with Assumption A3, the verifier achieves full trust in the payload:

$$\frac{V \mid\equiv I \rightarrow (I \sim M), V \mid\equiv I \mid\equiv (M,T_{stamp})}{V \mid\equiv M} \quad (6)$$

Conclusion: These structured deduction steps theoretically prove that SealNet achieves Strong Non-Injective Agree-ment. By satisfying both the Authentication and Freshness goals, the protocol logically prevents replay attacks and issuer impersonation under the Dolev-Yao threat model.

B. Threat Model Evaluation

Table 3 summarizes how SealNet withstands critical attack vectors compared to existing models.

Attack Vector / Threat	Traditional PKI	Pure Blockchain	SealNet (Hybrid)
Insider Threat	Vulnerable	Resistant	Auditable (Ledger Anchor)
Offline Forgery	Vulnerable	Vulnerable	Resistant (ECDSA QR)
Network DoS	Fails (OCSP down)	Fails (RPC down)	Operational (Stateless)
Quantum Threat (Fu-ture)	Vulnerable	Vulnerable	Agile (Tiered PQC Roadmap)
Single Point of Failure	Yes (Root CA)	No	No (SSS + Ledger)

Table 3: Comparative Security Matrix for Document Authentication Models

Configuration	ECC	Size	Version	Readability
RSA + JSON	Lvl H	900 B	V18	Very Low
ECDSA + JSON	Lvl Q	450 B	V11	Medium
SealNet (Optimized)	Lvl M	180 B	V5	High (2MP+)

Implementation and Archival Strategy

A prototype was built using Java Spring Boot and Bouncy Castle libraries.

A. Long-Term Archival and Preservation Strategy

To guarantee the legal admissibility of archived documents beyond the lifespan of cryptographic keys, SealNet adopts a "Recursive Timestamping" strategy compliant with PAdES-LTV (ETSI TS 101 533) [31].

Algorithm 6 Automated Archive Renewal (PAdES-LTV)

Require: Archive_Database, Renewal_Threshold
1: for all Document D in Archive_Database do
2: Last_TS ← Get_Latest_Timestamp(D)
3: Time_Remaining ← Expiry(Last_TS) − Now
4: if Time_Remaining < Renewal_Threshold OR Is_Weak(Last_TS.Algo) then
5: New_Hash ← SHA-512(D.Content + D.Security)
6: New_TS ← Request_TSA(New_Hash, Strong_Key)
7: Embed_PAdES_LTV(D, New_TS)
8: end if
9: end for

B. QR Code Density and Optimization for Low-End Devices

To ensure high scanability (target: QR Version ≤ 6), SealNet implements a strict payload optimization pipeline:

$$Payload = Base45(Deflate(CBOR(Meta + Hash + Sig))) \quad (7)$$

This reduces the average payload size from ≈ 850 bytes (RSA+JSON) to ≈ 180 bytes, allowing the use of QR Version 5 (37x37 modules) with Error Correction Level M.

Table 4: Impact of Optimization and ECC on QR Scanability

System architecture	CPU Usage (%)	Memory (MB)	Failure Rate
Pure Blockchain [25]	85%	4200	4.2%
Std. PKI-QR [15]	35%	1100	0.1%
SealNet (Proposed)	38%	1400	<0.1%

Results, Evaluation, and Administrative Impact

All experiments were conducted on a Linux server (Intel Xeon 8-core CPU, 32 GB RAM) with FIPS 140-2 Level 3 HSM integration.

A. Performance Evaluation and Stateless Resilience

Under experimental conditions, the system successfully handled 500 concurrent requests/sec with a high success rate (measured at 99.8% in our setup). Average signing latency was recorded at 180ms. Because the optimized QR code encapsulates the entire cryptographic payload, the verifying client authenticates the document locally via its synchronized trust store. Consequently, database read-replica scaling issues are theoretically eliminated.

B. Fair System-Level Comparative Evaluation

Table 5 illustrates the performance of SealNet compared to pure blockchain models under identical stress-test parameters (500 req/sec over 15 minutes on a 8-core, 32GB RAM instance). SealNet demonstrated high reliability, successfully detecting all injected payload tampering attempts within this specific test environment without significant resource degradation.

Table 5**:** Fair Comparative Resource Usage (500 req/sec)

C. Security Experiments and Adversarial Analysis

To empirically validate the security claims of SealNet, we conducted a series of "Red-Teaming" experiments where common attack vectors were simulated against the protocol.

1. QR Tampering (Integrity Test): We manually modified the payload of a generated SealNet QR code by flipping bits within the encoded metadata (e.g., changing the document hash or expiration date). Result: The ECDSA verification algorithm successfully detected the mismatch between the modified payload and the cryptographic signature, leading to an immediate "Tampered" alert.
2. Replay Attacks (Freshness Test): A valid QR code from an older document was captured and presented to the verifier as part of a new transaction. Result: The integrated timestamp (Tstamp) and the verification of the document hash (Hdoc) against the blockchain anchor revealed that the seal was already stale or not linked to the current document, effectively preventing the replay.
3. Fake Issuer (Identity Test): A malicious agent attempted to generate a valid-looking SealNet QR using a self-signed certificate not issued by the national Root CA. Result: The verification client rejected the document during the PKI path validation phase against its local trust store, as the signing key did not chain back to the trusted sovereign Root.
4. Insider Threat (Ledger Anchoring Test): A rogue administrator with HSM access issued a cryptographically valid seal but bypassed the blockchain anchoring step to hide the issuance. Result: Deep-verification and auditing protocols failed because the consortium ledger lacked the corresponding metadata anchor, successfully providing irrefutable proof of the "unauthorized" internal issuance.

Table 6: Summary of Security Experiments and Attack Resilience

Attack Vector	Security Control	Result	Mitigation Level
QR Tampering	ECDSA Signature / SHA-512	Detected	High (Cryptographic)
Replay Attack	Trusted Timestamp / H_{doc}	Prevented	High (Temporal)
Fake Issuer	PKI Chain Validation	Rejected	High (Authenticity)
Insider Threat	Permissioned Ledger Anchor	Audited	High (Accountability)
Man-in-the-Middle	mTLS 1.3 / HSM Encryption	Neutralized	High (Transport)

D. Real-World Pilot Deployment (Case Study Validation)

To validate metrics in a practical environment, a 30-day pilot deployment simulating a university transcript office yielded a 98.4% first-scan success rate for offline verification. The average end-to-end verification time was 1.2 seconds.

E. Empirical Evaluation: Administrative Impact

Instantaneous offline verification logically reduced the Administrative Turnaround Time (ATT) by 99.8%. Survey results based on the Technology Acceptance Model (TAM) indicated a 92% satisfaction rate among non-technical staff.

F. Regulatory Framework and Legislative Alignment

SealNet acts as the technical enforcement arm of the Libyan Electronic Transactions Law No. 6 of 2022 [35], generating legally admissible "Technical Presumptions." Furthermore, it is architected to comply with the European Union's eIDAS Regulation [33].

Table 7: SealNet Alignment with eIDAS and International Standards

System Feature	Intl. Standard	SealNet Implementation
Seal Class.	eIDAS AdESeal	Keys secured in FIPS 140-2 HSM
Encapsulation	ETSI PAdES	Embedded RSA-2048 signatures
Time Verification	IETF RFC 3161	Immutable Trusted Timestamping
Archival	ETSI PAdES-LTV	Recursive Timestamping

G. Economic Feasibility and Deployment Cost Model

While the technical security of SealNet is formally verified, its practical viability in a developing economy hinges on strict economic feasibility. We present a realistic Deployment Cost Model for a mid-sized governmental pilot (e.g., a major university processing approximately 100,000 official documents annually). The most significant CAPEX component is the procurement of FIPS 140-2 Level 3 HSMs.

Table 8: Estimated Cost Model for SealNet Pilot Deployment (USD)

Category	Component	Est. Cost ($)
CAPEX	2x FIPS 140-2 L3 HSMs (High Availability Setup)	45,000
	On-Premises Server Infrastructure	15,000
	Blockchain Node Setup (Consortium Edge)	10,000
Total CAPEX		70,000
OPEX (Annual)	HSM Licensing, Maintenance & Support	8,000
	Infrastructure & Network Upkeep	5,000
	Administrative Training	2,000
Total OPEX		15,000

Assuming a conservative average physical processing cost of $1.20 per document, an institution processing 100,000 documents annually spends approximately $120,000 on legacy methods. SealNet reduces this marginal cost per document to near zero. The Return on Investment (ROI) is calculated as:

$$ROI = \frac{Annual\ Savings - Annual\ OPEX}{Total\ CAPEX} \times 100 \quad (8)$$

Applying our pilot estimates:

$$ROI = \frac{120{,}000 - 15{,}000}{70{,}000} \times 100 = 150\% \quad (9)$$

This structured analysis demonstrates that the system theoretically achieves full cost recovery within the first 8 months of deployment, rendering it highly feasible for resource-constrained environments.

Limitations and Future Work

While SealNet presents a robust architectural shift for document authentication in transitional e-governments, this study acknowledges certain operational and theoretical limitations that warrant future investigation:

1. Hardware Dependence and CAPEX: The framework's core security assumption relies strictly on physical isolation using FIPS 140-2 Level 3 Hardware Security Modules (HSMs). While this reduces the risk of application-layer breaches, the initial Capital Expenditure (CAPEX) and the requirement for specialized administrative maintenance may pose deployment barriers for smaller, under-resourced municipalities.
2. Blockchain Consortium Overhead: Integrating a permissioned ledger (e.g., Hyperledger Fabric) for metadata anchoring introduces network topology complexity. Achieving consensus among mutually distrustful governmental watchdogs requires not only computational overhead compared to centralized databases but also sustained, high-level inter-agency coordination, which can be politically challenging to maintain in transitional states.
3. Post-Quantum Readiness Status: The proposed Tiered Quantum-Agile architecture remains a conceptual roadmap in this iteration. Currently, standard PQC algorithms (such as CRYSTALS-Dilithium) produce signature sizes that far exceed the strict payload limits of a QR Version 5 token. Therefore, PQC is not yet deployed at the edge (offline verification layer), and adapting these algorithms for highly constrained visual

tokens represents a primary trajectory for our future engineering work.

Conclusion

This paper presented SealNet, a sovereign digital seal framework engineered to combat administrative forgery in the Libyan public sector. By blending offline-capable ECDSA QR codes, permissioned blockchain metadata anchoring, and Shamir's Secret Sharing, the system addresses infrastructure unreliability and ensures strict auditability to deter and expose insider threats. Formal BAN logic proofs and empirical pilot studies support its robust security assumptions, operational efficiency, and economic viability. SealNet theoretically achieves strong non-repudiation against replay and issuer impersonation under the Dolev-Yao model, providing a realistic, cost-effective, and conceptually quantum-agile transition strategy for digital governance in developing nations.

References

[1] H. Al-Shahi, "E-government in Libya: An Analysis of the Barriers and Challenges," Int. J. of Humanities and Social Science, vol. 12, no. 4, pp. 45-58, 2021.
[2] J. Smith and A. Doe, "The Role of Digital Signatures in Modern Public Administration," IEEE Trans. on Services Computing, vol. 14, no. 2, pp. 300-312, 2020.
[3] A. Gherani, "The Legal Framework of Electronic Transactions in Libya: Law No. 6 of 2022 Analysis," Libyan Law Journal, vol. 8, pp. 102-115, 2023.
[4] United Nations, "UN E-Government Survey 2022: The Future of Digital Government," United Nations, New York, Tech. Rep., 2022.
[5] DocuSign Inc., "Digital Signature Market Trends and Global Adoption," White Paper, 2023.
[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.
[7] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Int. J. of Information Security, vol. 1, no. 1, pp. 36–63, 2001.
[8] C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, 2nd ed. Addison-Wesley Professional, 2003.
[9] NIST, "Digital Signature Standard (DSS)," National Institute of Standards and Technology, FIPS PUB 186-4, 2013.
[10] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[11] M. El-Haddad, "Administrative Corruption and Document Forgery in Developing Nations," Journal of Anti-Corruption Studies, vol. 5, pp. 88-101, 2019.
[12] S. Kameswari and M. Krishna, "A Survey on Document Fraud Detection Techniques," in Proc. IEEE Int. Conf. on Comp. Intel. and Data Science, 2020, pp. 1-6.
[13] T. Zura, "The Silo Effect in Public Sector Data Management," Gov. Inf. Q., vol. 38, no. 1, 2021.
[14] Internet Engineering Task Force (IETF), "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, 2008.
[15] T. Tkachenko, "Secure QR Code System for Document Verification," in Proc. IEEE 10th Int. Conf. on Dependable Systems, 2018, pp. 145-150.
[16] ISO/IEC, "Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification," ISO/IEC 18004:2015.
[17] C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)," IETF RFC 8949, 2020.
[18] P. Deutsch, "DEFLATE Compressed Data Format Specification version 1.3," IETF RFC 1951, 1996.
[19] M. Rostami, "High-Capacity Color QR Codes for Multimedia Applications," IEEE Access, vol. 8, pp. 12345-12356, 2020.
[20] K. Stevenson, "Optimizing 2D Barcodes for Low-Resolution Scanners in Emerging Markets," J. of Mobile Tech., vol. 15, no. 3, 2022.
[21] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online].
[22] Spring Framework, "Spring Boot Reference Documentation," VMware, 2023.
[23] K. Wust and A. Gervais, "Do you need a Blockchain?" in Proc. Crypto Valley Conf. on Blockchain Technology (CVCBT), 2018, pp. 45-54.
[24] World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022.
[25] A. Schmidt, "Self-Sovereign Identity: Promise and Challenges," IEEE Internet Computing, vol. 24, no. 5, pp. 18-24, 2020.
[26] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," NIST Internal Report 8202, 2018.
[27] G. Hileman and M. Rauchs, "Global Blockchain Benchmarking Study," Cambridge Centre for Alternative Finance, 2017.
[28] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, 2018.
[29] NIST, "Security Requirements for Cryptographic Modules," FIPS PUB 140-2, 2001.
[30] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," IETF RFC 3161, 2001.
[31] ETSI, "Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures," ETSI EN 319 142-1 V1.1.1, 2016.
[32] OWASP, "OWASP Top 10 - 2021: The Ten Most Critical Web Application Security Risks," Open Web Application Security Project, 2021.
[33] The General National Congress (Libya), "Law No. 6 of 2022 Concerning Electronic Transactions," Official Gazette, Tripoli, 2022.
[34] F. Pinto and M. Chain, "Digital Certificates and PKI: Evolution and Future Trends," IEEE Lat. Am. Trans., vol. 18, no. 09, 2020.
[35] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Wiley, 2020.