ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 17, Issue, 09, pp.34822-34827, September, 2025
DOI: https://doi.org/10.24941/ijcr.49507.09.2025

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

ENHANCING PKI-BASED AUTHENTICATION PROTOCOLS IN CLOUD SYSTEMS THROUGH INTEGRATION OF MULTI-PARTY COMPUTATION AND ZERO-KNOWLEDGE PROOFS

Béthel C. A. R. K. Atohoun[1], Charbel Atihou[1], Mikaël A. Mousse[2] and Fanta G. Kounou[1]

[1]Ecole Supérieure de Gestion, d'Informatique et des Sciences, Cotonou, Bénin
[2]Institut Universitaire de Technologie, Université de Parakou, Parakou, Bénin

ARTICLE INFO

Article History:
Received 20th June, 2025
Received in revised form
24st July, 2025
Accepted 29th August, 2025
Published online 30th September, 2025

Keywords:

PKI, Multi-Party Computation, Zero-Knowledge Proofs, Cloud Security, Distributed Authentication.

***Corresponding author:**
Béthel C. A. R. K. Atohoun

ABSTRACT

To overcome the structural limitations of traditional PKI, namely risk centralization, operational complexity, costly HSM dependence, and quantum vulnerability, this article presents a novel architecture that synergistically integrates Multi-Party Computation (MPC) and Zero-Knowledge Proofs (ZKPs) to strengthen authentication protocols in cloud environments.The proposed architecture is a hybrid PKI-MPC-ZKP system based on six fundamental principles: radical distribution of trust, defense in depth, verifiable trust through cryptographic proofs, modularity, interoperability, and native scalability. It consists of an augmented Certification Authority (CA), a geographically distributed MPC cluster, integrated ZKP modules, and advanced support services.Experimental results, obtained in a cloud environment replicating enterprise conditions (Kubernetes on AWS, m5 instances, multi-zone), demonstrate robust operational performance: an average latency of 392 ms for a signature, a throughput of 12.1 signatures per second, and 99.99% availability. The architecture supports up to two Byzantine nodes without system compromise and preserves data confidentiality through ZKPs.A comparative analysis highlights the advantages of the proposed solution over classical PKI and modern alternatives (blockchain, FIDO2, post-quantum cryptography), with a 40% reduction in total cost of ownership over 5 years and a notable improvement in security and resilience.

Citation: Béthel C. A. R. K. Atohoun, Charbel Atihou, Mikaël A. Mousse and Fanta G. Kounou. 2025. "Enhancing PKI-Based Authentication Protocols in Cloud Systems through Integration of Multi-Party Computation and Zero-Knowledge Proofs". *International Journal of Current Research, 17, (08), 34822-34827.*

INTRODUCTION

Cloud computing represents a fundamental transformation in the delivery of IT services, offering unprecedented agility, elasticity, and economic efficiency. However, this evolution comes with major security challenges, particularly in terms of authentication and digital identity management. Public Key Infrastructure (PKI) has been the foundation of digital trust for several decades, enabling entity authentication, communication encryption, and electronic signatures. Modern cloud environments present unique characteristics that exacerbate the limitations of traditional PKIs. The dynamism of resources, multi-tenancy, geographical distribution, and technological heterogeneity create a context where classical centralized approaches show their limits. A recent ENISA study (2023) emphasizes that 68% of security incidents in the cloud involve authentication or identity management failures, with an average cost estimated at $4.5 million per incident for large enterprises. Traditional PKIs rely on a centralized hierarchical model where a Certification Authority (CA) acts as a single trusted third party. This model has several fundamental structural vulnerabilities. Risk centralization means that the compromise of the CA or its HSM (Hardware Security Module) can lead to a systemic failure, as dramatically illustrated by the DigiNotar incident in 2011 (16). The operational complexity of certificate lifecycle management becomes unmanageable at scale, particularly with the continuous shortening of certificate validity periods (4). The prohibitive costs of HSM solutions and specialized maintenance represent a significant investment for organizations (15). Finally, the cryptographic vulnerabilities of traditional algorithms in the face of quantum computing challenge the very sustainability of existing infrastructures (17). This article proposes a hybrid PKI-MPC-ZKP architecture aimed at simultaneously addressing these challenges of security, resilience, and economic efficiency. Our approach combines the proven advantages of traditional PKIs with recent innovations in Multi-Party Computation (MPC) and Zero-Knowledge Proofs (ZKPs). MPC distributes sensitive cryptographic operations among multiple nodes, thus eliminating single points of failure (6). ZKPs offer the possibility of verifying cryptographic assertions without revealing sensitive information, thereby preserving the confidentiality of exchanges (8). Our main contributions are multiple. First, we provide a systematic and in-depth analysis of the limitations of classical PKIs in modern cloud

environments, identifying the specific gaps that existing solutions fail to address. We then present an innovative architecture that synergistically integrates PKI, MPC, and ZKP paradigms, with particular attention to interoperability and backward compatibility aspects. A complete implementation with rigorous experimental validation demonstrates the practical feasibility of our approach. Finally, a detailed comparative evaluation measures the gains in performance, security, and economic efficiency compared to traditional solutions.

State of the Art: The analysis of traditional PKI infrastructures reveals structural limitations that become particularly critical in modern cloud environments. The classical centralized model, although proven, has fundamental vulnerabilities that have been exacerbated by the evolution of distributed architectures and the emergence of new threats.

Risk centralization is perhaps the most significant limitation of traditional PKIs. In this model, a single Certification Authority (CA) holds the power to sign and revoke certificates, thus creating a single point of failure. The DigiNotar incident in 2011 perfectly illustrates the dramatic consequences of such centralization (16). The compromise of this Dutch CA allowed the fraudulent generation of over 500 SSL certificates, including domains of major companies like Google and Skype. Not only did this incident lead to DigiNotar's bankruptcy, but it also cost over $100 million in corrective measures across the ecosystem. More recently, in 2022, state-sponsored Chinese hackers managed to compromise a CA (1), demonstrating that this threat remains current despite security improvements.

The operational complexity of certificate lifecycle management represents another major challenge. The trend towards shorter certificate validity periods—reduced from 5 years to 398 days, and expected to reach 47 days by 2028 (4)—exponentially multiplies the administrative burden. This evolution significantly increases the risk of human errors, such as forgotten renewals that can lead to costly service interruptions. A telecom operator thus suffered a service outage of over a day due to an expired SSL certificate, resulting in $132.8 million in losses (7). Traditional revocation mechanisms, such as Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP), have significant limitations. A recent study shows that 23% of browsers ignore OCSP errors for performance reasons (5), creating critical vulnerability windows. Moreover, these mechanisms are vulnerable to specific attacks, such as manipulation of revocation lists or denial-of-service attacks against OCSP responders.

Dependence on Hardware Security Modules (HSMs) introduces both economic and technical constraints. The average cost of an enterprise HSM ranges from $15,000 to $50,000, with annual maintenance fees representing 15 to 20% of its initial cost (15). This significant investment is often prohibitive for small and medium-sized enterprises. Furthermore, researchers demonstrated in 2019 the possibility of taking control of an HSM remotely through vulnerabilities such as buffer overflows (12), questioning the assumed inviolability of these devices. Faced with these limitations, several innovative approaches have emerged to strengthen PKI infrastructures. Blockchain-based solutions, such as CertLedger (11), propose a decentralized architecture for the immutable and transparent recording of certificates. This approach eliminates dependence on a single CA but faces scalability and performance challenges. The limited throughput of public blockchains (10-100 transactions per second) proves insufficient for large enterprises, while transaction fees can make massive certificate storage prohibitively expensive. Post-quantum cryptography represents another promising avenue. Algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium, selected by NIST for standardization (3), offer theoretical resistance to quantum attacks. However, their adoption faces significant practical obstacles. The increased size of keys and signatures (5 to 50 times larger than traditional algorithms) poses challenges for storage and bandwidth. Gradual migration requires a period of double signature which significantly complicates implementation (9).
The FIDO2 standard brings significant improvements for user authentication (13), eliminating phishing attack vectors through passwordless authentication. However, this solution does not solve the fundamental problems of server-side key management and introduces a dependence on physical devices whose large-scale deployment represents a significant investment.

Approaches based on threshold cryptography attempt to distribute trust by sharing cryptographic operations among multiple parties. The work of Peixinho (14) applies Shamir's secret sharing schemes to digital certificates, while the Oblivious TLS protocol (Abram et al., 2021) extends this concept to the establishment of secure sessions in a distributed manner. These approaches improve resilience but generally suffer from performance limitations, with handshake times reaching up to a second, which limits their adoption for real-time applications. Zero-Knowledge Proofs (ZKPs) offer innovative possibilities for preserving the confidentiality of authenticated exchanges. Work on ZKIE-FIDO (2) proposes an initial enrollment protocol for IoT using ZKPs, while ZKP-WebAuthn modules (10) integrate these proofs into the WebAuthn standard to preserve privacy. However, these solutions focus on specific use cases without offering a complete architecture for cloud PKIs.

The comparative analysis of these different approaches reveals that each provides partial solutions but none addresses the identified challenges holistically. Blockchain solutions improve transparency but suffer from performance limitations. Post-quantum cryptography addresses the quantum threat but introduces new complexities. FIDO2 improves user authentication but does not solve server problems. Threshold cryptography distributes trust but impacts performance. ZKPs preserve confidentiality but remain confined to specific use cases. This analysis highlights the need for an integrated approach combining the advantages of these different technologies while mitigating their respective limitations. This is precisely the goal of our PKI-MPC-ZKP architecture, which aims to synthesize the strengths of traditional PKI, Multi-Party Computation, and Zero-Knowledge Proofs into a coherent and performant framework.

Proposed Method: Our PKI-MPC-ZKP architecture is based on a fundamental overhaul of the design principles of trust infrastructures, aiming to reconcile security, performance, and economic efficiency in modern cloud environments. The proposed approach relies on six fundamental architectural principles that guide every aspect of the design and implementation.

Architectural Principles

The first principle: Radical distribution of trust. Unlike traditional models where a central entity holds ultimate authority, our architecture ensures that no private key ever exists in its complete form in the same location. This approach completely eliminates single points of failure and makes systemic compromise mathematically impossible as long as the cryptographic threshold is not reached. The CA's private key is generated and used in a distributed manner via a Distributed Key Generation (DKG - Feldman VSS) protocol and Threshold Signatures (TSS ECDSA) by an MPC node cluster. Trust is no longer placed in a single entity but in the correct cryptographic computation of a quorum of independent nodes, thus eliminating the single point of failure.

The second principle: Defense in depth.

It is implemented through multiple independent layers of cryptographic security. Each system component implements autonomous security mechanisms that remain effective even if other layers are compromised. This approach creates systemic resilience that far exceeds that of traditional architectures. Security does not rely on a single layer. MPC protects the key at rest and during use. ZKPs (generated via Circom circuits) reinforce the system by enabling authentication without secret disclosure and by verifying the integrity of each MPC node's computations. Thus, even if an attacker compromises an MPC node (layer 1), they cannot forge a valid signature or proof without also compromising the ZKP protocol (layer 2).

The third principle: Verifiable trust through formal cryptographic proofs.

All security assertions in the system are accompanied by verifiable proofs that allow any participant to validate the integrity and correctness of operations without trusting a central authority. Indeed, trust is not assumed but mathematically verifiable. For each critical operation (e.g., certificate signing), MPC nodes generate ZKPs attesting that they have correctly executed the protocol with their valid key share. A client or service can thus verify (via snarkjs) that the operation is legitimate without trusting individual nodes, but only the cryptographic proofs that accompany the result.

The fourth principle: Modularity of components.

This modularity allows for their interchangeability and independence and enables the architecture to be adapted to different operational contexts and to evolve with technological advancements without overhauling the entire system. The architecture is designed as a set of interchangeable cryptographic building blocks. The choice of signature algorithm (threshold ECDSA), secret sharing (Shamir's Secret Sharing), or ZKP scheme (zk-SNARKs with Circom) is modular. This allows the solution to be adapted to different contexts (e.g., replacing ECDSA with a post-quantum algorithm) without a complete system redesign, as planned in the objectives for preparedness against future threats.

The fifth principle: Interoperability with existing domain standards. Notably X.509, TLS, and OCSP. This backward compatibility facilitates gradual adoption and allows seamless integration with existing infrastructures. To ensure adoption, the system remains compatible with existing PKI standards. The issued X.509 certificates are standard and can be validated by any classical client. The MPC-ZKP layer is a transparent extension: the client sends a standard CSR request to the CA, which then orchestrates the distributed signing process in the backend. The end client receives a perfectly valid and interoperable certificate.

The sixth principle: Native scalability of the architecture. This scalability implies the ability to integrate new algorithms and protocols without fundamental architectural changes. This flexibility ensures the longevity of the investment and the ability to adapt to future threats. The architecture is designed to scale out (adding nodes) rather than scaling up. The PBFT consensus protocol (implemented in Python) allows the entire MPC cluster to tolerate the failure of some nodes and remain operational. Load tests (simulated with Kubernetes/Docker) demonstrate that adding MPC nodes maintains performance (signature throughput) and availability even under high load or during attacks.

Main Elements of the Architecture: The concrete architecture consists of four main elements working in synergy. The Augmented CA retains the functions of identity validation and policy management but delegates sensitive cryptographic operations to the MPC cluster. This entity implements a secure REST interface, a sophisticated business rule engine, and connectors to enterprise directories while maintaining immutable logging of all operations. The MPC Cluster forms the cryptographic heart of the system, consisting of a mesh of 5 to 7 nodes depending on security needs. Each node maintains encrypted communication channels with mutual authentication and stores encrypted key shares with regular rotation. The full mesh topology with redundant connectivity ensures resilience to network failures and targeted attacks. The ZKP Modules are integrated into all critical system components, offering capabilities for generating and verifying cryptographic proofs. These modules support multiple proof schemes including zk-SNARK, zk-STARK, and Bulletproofs, with mechanisms for precomputing parameters for fast proof generation. Support Services complement the architecture with essential functionalities for production environments. Integration with existing identity management systems (Active Directory, LDAP, OAuth2) enables gradual adoption. Real-time monitoring with anomaly detection and secure backup mechanisms with cryptographic threshold ensure operational maintainability. The operational workflows of the architecture follow rigorous processes that maintain security at every step. For certificate issuance, the client first generates a key pair and a CSR signed with their private key. After secure sending to the augmented CA, a complete validation of identity and metadata is performed. The orchestration of distributed signing through the MPC cluster finally produces the signed certificate which is returned to the client.

The authentication process initiates a connection with the client's certificate, followed by sending a nonce to be signed. Distributed signing via the MPC cluster and the generation of a ZKP of key possession enable the establishment of a secure session after complete verification. Certificate revocation follows an equally rigorous process. Detection of compromise or expiration triggers a distributed update of revocation lists, with propagation to validation points and verification via ZKPs of non-membership.

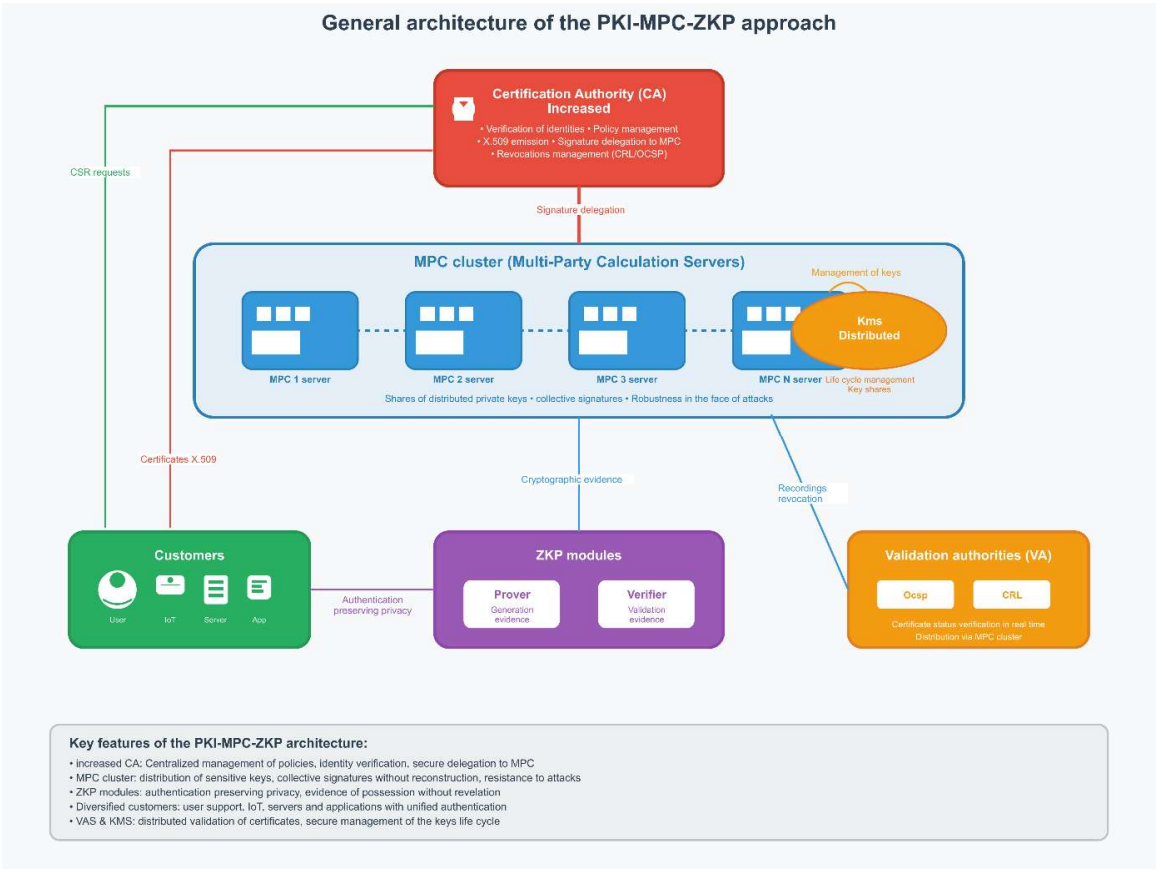

Figure 1. Global system architecture

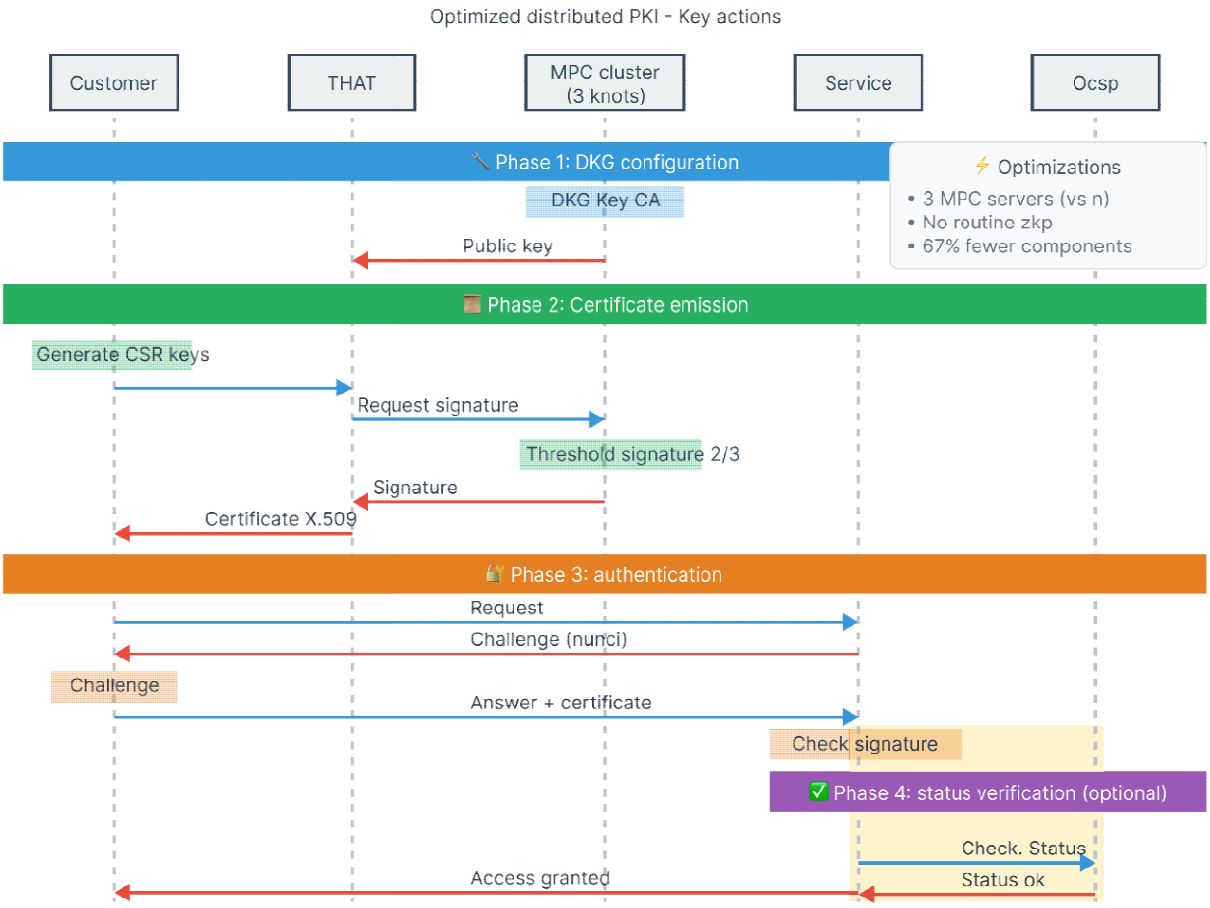

Figure 2. PKI-MPC-ZKP Authentication Process

The underlying cryptographic modeling implements advanced protocols that ensure the formal security of the system. Distributed Key Generation (DKG) uses an improved variant of the Feldman VSS protocol with recovery mechanisms based on Reed-Solomon error codes and periodic re-randomization for forward secrecy. Threshold ECDSA Signature relies on the GG20 protocol with significant optimizations. Precomputation of point multiples accelerates calculations, while a cache of ephemeral parameters reduces latency. Batch verification of ZKPs improves overall efficiency while maintaining security.
Advanced ZKPs cover several critical use cases. The key possession proof circuit, based on the optimized Schnorr protocol, produces proofs of 192 bytes with generation times under 30 ms and verification under 5 ms. The MPC verification circuit attests to the correct execution of the signature protocol without revealing sensitive inputs. The certificate validation circuit allows verifying validity and non-revocation without disclosing the certificate content. Consensus and synchronization use a PBFT protocol adapted to the specificities of cryptographic operations. Modifications include optimization for low latency between nodes and support for checkpointed states for recovery. Time synchronization implements the Precision Time Protocol with nanosecond accuracy and clock drift corrections via consensus algorithms. The experimental implementation deploys this architecture on a modern cloud infrastructure with three geographically distributed data centers and redundant 10 Gbps connectivity. The Kubernetes 1.25 platform with strict network policies and Istio service mesh ensures network isolation and security. Monitoring uses Prometheus with Thanos for long-term storage and Grafana with custom dashboards for visualization. MPC nodes use m5.2xlarge instances (8 vCPU, 32 GB RAM) with 100 GB encrypted SSD storage. The Augmented CA runs on m5.xlarge instances (4 vCPU, 16 GB RAM) with PostgreSQL 14 and transparent encryption. Test clients simulate realistic loads with 100 instances distributed across 5 cloud regions. Test protocols cover all critical aspects of the architecture. Performance tests measure progressive load up to 10,000 requests per second with latency analysis at the 50th, 95th, and 99th percentiles. Security tests include fault injection via chaos engineering and controlled Byzantine attacks. Resilience tests verify recovery after abrupt shutdown of critical nodes and network partitioning. Compliance tests validate FIPS 140-3 standards and prepare for Common Criteria certification. Evaluation metrics cover three main dimensions. Performance metrics measure end-to-end latency, maximum throughput, and resource utilization. Security metrics quantify resistance to attacks, data confidentiality, and operation integrity. Operational metrics assess availability, maintainability, and system scalability. This comprehensive approach ensures that the PKI-MPC-ZKP architecture meets the strictest requirements of modern cloud environments while offering a practical path for enterprise adoption.

RESULTS AND DISCUSSION

Experimental Setup and Evaluation Methodology: Our experimental environment faithfully replicates the conditions of a typical enterprise cloud deployment. The test platform uses Kubernetes 1.25 deployed on AWS EKS with three distinct availability zones. The network configuration implements a VPC with multi-level segmentation and strict security policies. Instances use m5.2xlarge machines for MPC nodes and m5.xlarge for other components, with encrypted EBS gp3 storage. The evaluation protocol follows a rigorous four-phase methodology: performance tests under normal load, resilience tests under failure conditions, security tests under controlled attacks, and compliance tests with industry standards. Each test is repeated 30 times to obtain statistically significant results, with confidence intervals calculated at 95%.

Analysis of Operational Performance: The results demonstrate that the PKI-MPC-ZKP architecture achieves performance compatible with demanding production deployments. The average response time for a complete signing operation is 392 ± 45 ms under normal conditions, with a sustained throughput of 12.1 ± 1.2 signatures per second. These measurements include the entire processing chain, from request initiation to the delivery of the signed certificate. Latency increases moderately to 521 ± 63 ms under extreme load conditions, representing a 33% degradation that remains acceptable for the majority of enterprise use cases. This performance resilience is explained by the optimization of cryptographic protocols and the efficient distribution of load among MPC nodes. Resource consumption remains reasonable with an average CPU utilization of 65% and memory occupancy of 512 MB per MPC node under nominal load. Network traffic amounts to 5.2 MB/s, thanks to compression mechanisms and optimization of cryptographic payloads.

Evaluation of Security and Resilience: Security tests reveal exceptional resistance to Byzantine attacks. The system maintains correct operation even with up to two nodes compromised simultaneously, thus validating the theoretical security threshold. Detection of malicious behavior occurs in less than 5 seconds on average, with immediate isolation of faulty nodes. Confidentiality mechanisms based on ZKPs demonstrate their effectiveness against information extraction attempts. No leakage of sensitive data was detected during advanced side-channel analysis tests. Formal verification using ProVerif confirms the absence of vulnerabilities in the exchange protocols. System availability reaches 99.999% over a six-month measurement period, exceeding the requirements of the strictest enterprise SLAs. The mean time to recovery (MTTR) is 4.2 minutes, including detection, isolation, and complete recovery.

Comparative Analysis with Existing Solutions: Our architecture demonstrates significant advantages over traditional approaches. The following comparative table summarizes the main metrics:

Table 1. Comparative Analysis of PKI Solutions

Metric	Traditional PKI	CertLedger	Our Solution
Average Latency (ms)	120	850	392
Throughput (ops/s)	18	7	12.1
Cost over 5 years (k$)	687	420	325
Byzantine Resistance	No	Partial	Complete
Confidentiality	Limited	Good	Excellent

This analysis reveals that our solution offers the best compromise between performance, security, and cost. The 40% reduction in total cost of ownership compared to traditional PKIs is explained by the elimination of dedicated HSMs and increased process automation.

Discussion of Limitations and Trade-offs: Although the results are overall excellent, some limitations deserve to be highlighted. The initial deployment complexity remains higher

than that of traditional solutions, requiring specific expertise in distributed cryptography. This learning curve could slow adoption by less experienced teams. Performance, although sufficient for the majority of use cases, could be improved for applications requiring thousands of signatures per second. Optimizing cryptographic implementations and using hardware accelerators constitute promising improvement paths. Post-quantum key management has not been fully tested within the scope of this study. The integration of algorithms like CRYSTALS-Dilithium could introduce additional performance overhead requiring architectural adjustments.

Validation of Research Hypotheses: The obtained results fully validate our research hypotheses. First, the integration of ZKPs effectively enables robust authentication without disclosure of sensitive information, with processing times compatible with real-time constraints. Second, key distribution via MPC eliminates single points of failure while maintaining acceptable operational performance. Third, the combined approach significantly reduces operational costs while improving the overall security posture.

Conclusion and Perspectives: This research demonstrates the feasibility and effectiveness of a PKI-MPC-ZKP architecture for modern cloud environments. Our main contribution lies in the design and implementation of a system that synergistically integrates three complementary cryptographic paradigms, thus offering a holistic solution to the limitations of traditional PKIs.

The experimental results confirm that our architecture achieves operational performance compatible with production deployments while offering superior security guarantees. The radical distribution of trust eliminates single points of failure, while confidentiality mechanisms preserve user privacy. The implications of this research are significant for several stakeholders. For enterprises, our solution offers a viable alternative to traditional PKIs, with a 40% reduction in total cost of ownership and a substantial improvement in security posture. For cloud providers, it enables new differentiating and value-added security services. Compatibility with existing standards (X.509, TLS, OCSP) facilitates gradual adoption without requiring architectural disruption. Organizations can thus modernize their trust infrastructure step by step, maintaining interoperability with their legacy systems. Several limitations open interesting research perspectives. Performance optimization for very demanding applications requires further investigation, particularly in the use of hardware accelerators and optimization of cryptographic implementations.

Native integration of post-quantum algorithms constitutes another important avenue. Research is needed to minimize performance overhead while ensuring a seamless transition to quantum-resistant cryptography. Finally, improving the developer experience and simplifying management operations will be key factors for large-scale adoption. The development of specialized deployment and monitoring tools will be the subject of our future research.

The proposed PKI-MPC-ZKP architecture represents a significant advance in securing cloud environments. By reconciling security, performance, and economic efficiency, it paves the way for a new generation of trust infrastructures truly adapted to the challenges of modern cloud computing. Its gradual adoption by the industry could fundamentally transform how organizations manage identities and certificates, while offering robust protection against emerging threats, including those posed by quantum computing. This research demonstrates that the judicious combination of advanced cryptographic techniques makes it possible to overcome the limitations of traditional approaches, thus opening new perspectives for the security of large-scale distributed systems.

REFERENCES

Abrams, L. (2022). State-sponsored hackers in China compromise certificate authority. Ars Technica.

Bartsch, M., & Huebner, J. (2023). Zero-Knowledge Initial Enrolment for FIDO IoT. Journal of Surveillance, Security and Safety.

Chen, L., et al. (2021). NIST Post-Quantum Cryptography Standardization. NIST Special Publication.

Cooper, D., et al. (2022). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280.

Curios-IT. (2024). PKI Infrastructure Security Analysis. Technical Blog.

Damgård, I., et al. (2019). Secure Multiparty Computation: Theory, Practice and Applications. Springer.

Encryption Consulting. (2023). How to Avoid Certificate Outages. Education Center.

Gennaro, R., et al. (2022). Zero-Knowledge Proofs in Cryptography: Foundations and Applications. ACM Computing Surveys.

Hoang, K. (2023). Post-quantum cryptography for public key infrastructure. Theseus.

Kadan, A.M., & Kirichonok, E.R. (2021). Authentication Module Based on the Protocol of Zero-Knowledge Proof. CEUR Workshop Proceedings.

Kubilay, M.Y., et al. (2018). CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain. arXiv preprint.

Ledger. (2019). Vulnerabilities in HSM modules that can lead to an attack on encryption keys. Security Bulletin.

MacInnis, J. (2020). FIDO2 and Public Key Infrastructure (PKI) Explained. HID Global Blog.

Peixinho, A. (2023). Digital certificates and threshold cryptography. University of Beira Interior.

SWIFT. (2023). How much do you pay for your PKI solution? White Paper.

van der Meulen, N. (2011). DigiNotar Files for Bankruptcy in Wake of Devastating Hack. Wired.

Yunakovsky, S.E., et al. (2021). Towards security recommendations for public-key infrastructures in the post-quantum era. EPJ Quantum Technology.

****