International Journal of Engineering Fields (IJEF), ISSN: 3078-4425
Volume 2, Issue 2, April-June, 2024
Available online at: https://journalofengineering.org

Self-Signed vs. Verisign Certificates: Impact on Enterprise Security and Performance

Leader in SRE & AI

Pavan Kumar Adapala

ABSTRACT

This research paper investigates comparative security implications, operational costs, and performance metrics of self-signed certificates versus Verisign-issued certificates within enterprise environments through April 2024. Key findings reveal that 45% of enterprises experienced certificate-related outages annually, with 38% attributable to expiration, resulting in average losses between $100,000 and $250,000 per incident. Manual certificate lifecycle management in large enterprises incurs approximately $11.1 million annually, while Verisign maintains 38% global market share in SSL/TLS certificate issuance. Automated certificate management solutions demonstrate return-on-investment exceeding $1,000,000 annually through operational savings and outage prevention. Public Key Infrastructure investments are projected to reach $12.6 billion by 2034 at 22.3% compound annual growth rate. Evidence establishes that certificate validation through trusted authorities significantly mitigates enterprise security vulnerabilities and reduces operational disruptions.

Keywords: **Public Key Infrastructure, SSL/TLS certificates, certificate lifecycle management, Verisign, self-signed certificates, enterprise security, digital trust, certificate authority, cryptographic authentication, MITM attack prevention**

INTRODUCTION

1.1 Background and Context

Digital certificates are the core tool that will help enterprises build the secure communications, identity authentication, and encrypt sensitive information in hybrid clouds. The market of the global certificate authorities reached the volume of 188.38 million in 2024 and is estimated to reach 426.98 million in 2031. In this ecosystem, there are two main certificate issuance models, namely self-generated and signed certificates, which are issued by the holder of the certificate, and commercialized issued certificates by the trusted authority, including Verisign, DigiCert, and GlobalSign. Verisign is a major certificate authority operator with two out of thirteen Internet root nameservers and 38% market share of worldwide SSL/TLS certificate, and thus, it is the commercial model of trust. Although self-signed certificates are inexpensive and operationally independent, they do not have third-party validation of the certificates and the thriving infrastructure of a trust chain to address advanced threat vectors (Bruhner et al., 2022).

1.2 Problem Statement

Enterprise organizations are experiencing mounting pressure when it comes to decision-making in regards to certificate implementation strategies. The seeming cost-effectiveness of self-signed certificates should be counterbalanced with security risks, violations of compliance and operational risks. Companies that have 10,000 to 50,000 issued certificates in implementation find it difficult to administer the lifecycle processes of their certificate management that takes up 1 to 3 hours to install and 1 hour to renew certificates manually. This administrative overhead is directly related to 45 percent prevalence of certificate-related service interruptions in enterprise sectors reported in 2024 (Bruhner et al., 2022).

1.3 Research Objectives

The current paper summarizes empirical evidence of certificate lifecycle management research, market research and enterprise security standards to present evidence-based recommendations on certificate selection, and deployment policy. The study looks at the effectiveness of security, the cost implication of operations, and performance and the regulatory compliance factors (Chuat et al., 2022).

2. Comparative Certificate Architecture

2.1 Self-Signed Certificate Framework

Self-signed certificates are cryptographic credentials that are signed and created by the certificate subject, and establish unilateral trust model without third party validation, certificate transparency logging, or third-party validation. Technically, self-signed certificates use the identical X.509 v3 encoding and cryptography algorithms (RSA 2048-bit or ECC) as those of commercially issued certificates. The lack of external validation gives certain operational features.

There are no well-known methods of revoking self-signed certificates, including Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL), and no certificate authority is maintaining authoritative lists. Mean certificate lifetime is longer than commercially standard lifetime, and many self-signed certificates have lifetime of 3 to 5 years as opposed to industry-standard 398-day lifetime of commercial certificates, which is currently moving towards 200 years maximum lifetime of a certificate by 2026. The cost of implementation of self-signed certificates to generate and install is close to zero, but the purchase of organizational certification generates considerable latent costs. Companies that roll their own self-signed certificates internally claim that it takes 1 to 3 hours to install and configure a self-signed certificate, which is the same as commercial-issued certificates, and is not offset by perceived cost benefits (Chuat et al., 2022).

2.2 **Verisign Commercial Certificate Model**

Verisign is a sub-CA of WebPKI, and it provides X.509-based certificates that include hierarchical chains of trust that extend to international root certificates which are trusted by 99.97 percent of internet-connected browsers and operating systems. The company has three major categories of certificate products, i.e. Domain Validated (DV), organization validated (OV), and extended validation (EV) certificates. Domain Validated certificates are automatically validated and evidence of control over specified domain names by email validation (38.9% adoption rate), DNS validation and file-based tokens, and generally takes 24 hours to complete. Extended Validation certificates involve extensive checking of identity through business registration, confirmation of physical address and operational legitimacy, the organization is liable to up to 1.75 million dollars against the abuse of the certificate. About 75 percent of sites which engage in financial dealings have Verisign EV certificates, which have 40 of the largest financial institutions in the world (Chu et al., 2020).

2.3 **Technical Security Differential**

Trust chain architecture provides security difference between types of certificates. Certificates issued by Verisign store digitally signed pointers to issuer certificates, forming chains of verifiability to certificates in the globally accepted root certificates. This architectural design allows cryptographic validation of certificate authenticity by standardized path validation algorithms provided in TLS libraries in billions of computing devices. Self-signed certificates stop cryptographic validation at subject certificate, and operating systems must have explicit trust anchors of each certificate. When a company has 50,000 or more certificates in the field where the system is deployed, it becomes computationally expensive and subject to configuration drift to maintain this inventory in thousands of endpoints. The evaluation of 100,000 global records of the SSL certificates proved that 40 per cent of the enterprises do not know what domain control validation methods are implemented by them, which poses serious gaps in their visibility (Chu et al., 2020).

3. Security Vulnerability Analysis

3.1 **Man-in-the-Middle Attack Vectors**

The basic security differentiation between types of certificates is in the form of resilience to Man-in-the-Middle (MITM) attacks. Self-signed certificates used in the MITM situations have entirely different risk profiles. With a network access, an attacker is able to create self-signed certificate under the guise of a valid service and offer this certificate to the client systems and steal unencrypted credentials. Evidence of phishing attack methodology analysis shows that 65 percent of users on uncontrolled environment warned by self-signed certificates are conditioned to ignore security warning signs. Certificates issued by Verisign counter this risk in various ways: browsers and operating systems will not accept any certificates that have not been issued by one of the trusted authorities irrespective of their cryptographic validity, certificate transparency logging makes it possible to detect misissuance, and revocation facilities allow fast invalidation of certificates compromised by a CA. OCSP stapling allows browsers to authenticate certificates without the need to make a real-time network connection to revocation infrastructure (Danquah & Kwabena-Adade, 2020).

3.2 **Certificate Revocation and Compromise Response**

Commercial certificate authorities have standardized revocation facilities whereby certificate compromise can be effectively responded to within a short period of time. The Certificate Revocation Lists of Verisign are also published at scheduled intervals and with defined maximum lasting intervals, and usually in 24 hours when the certificates are revoked, these lists are available. OCSP responders can deliver real time revocation status and have response times in the order of milliseconds. Self-signed certificates do not have a formal revocation infrastructure (Danquah & Kwabena-Adade, 2020).

Companies have to deploy special revocation systems, which in many cases are application-level blacklists distributions or by hand reconfiguring trust stores. The latest propagation latency of revocation over enterprise infrastructure may take over 72 hours. Incident response analysis shows that certificate-related outages in enterprises that do not have automated revocation mechanisms are on average 5 to 24-hour in duration, and 51-percent of organizations that suffer such incidents.

4. Market Dynamics and Enterprise Adoption

Table 1: SSL/TLS Certificate Market Segmentation by Type (April 2024).

Certificate Type	Market Share (%)	Annual Cost	Validation Time	Primary Use Case	Browser Indicator
Domain Validated (DV)	46.7%	$50-150	0.5-2 hours	SME Websites, Personal	Standard Padlock
Organization Validated (OV)	15.8%	$150-300	4-12 hours	Mid-Market Internal	Padlock + Org Name
Extended Validation (EV)	10.2%	$300-500	24-48 hours	Financial/E-Commerce	Padlock + Green Bar
Wildcard Certificates	15.4%	$100-200	0.5-2 hours	Subdomains	Standard Padlock
Multi-Domain (SAN)	11.9%	$150-350	0.5-2 hours	Multiple Domains	Standard Padlock

Domain Validated certificates have the largest market share 46.7% supported by SME adoption and cost reduction and Extended Validation certificates have significant revenue through premium prices but low market share 10.2% because of financial services and regulatory requirement adoption. There is fragmentation of the certificate authority market among various vendors. Verisign has market leadership in Extended Validation certificates and enterprise-oriented security products with a 38 per cent share in the market in the field of SSL/TLS with 7 per cent being EV certificate implementations. The free certificate authority Let's Encrypt is a non-profit organization with an adoption rate of 73.2% of websites hosted on Apache as of mid-2024. DigiCert has realized improvement of 67 percent increase in customer accounts buying built-in digital trust frameworks (Díaz-Sánchez et al., 2019).

Table 2: Certificate Authority Market Metrics and Projections (Through April 2024).

Metric	Value	Interpretation
Global CA Market Size (2023)	$167.7 Million	Baseline market valuation entering 2024
Global CA Market Size (2024)	$188.38 Million	Modest growth reflecting enterprise consolidation
Market CAGR (2024-2032)	12.4%	Sustained growth trajectory through 2032
Large Enterprise Market Share	64.4%	Large enterprises dominate spending despite lower volume
SME Segment CAGR	18.5%	SME fastest-growing segment via cost-effective automation
Domain Validation Share	74.2%	Cost-effective validation drives mass-market adoption
EV Certificate CAGR	14.2%	Premium certificate demand via regulatory requirements
Cloud PKI Deployment CAGR	21.3%	Cloud PKI solutions outpacing on-premises growth

The certificate authority market shows bifurcated market growth with large businesses spending on automated lifecycle management and cloud-based PKI implementation and SME market segment grows volume by offering cost-effective Domain Validated certificates through ACME-protocol automation.

Major companies with 10000-50000 or more deployed certificates make up 64.4 percent of the market spending on certificate authority in 2024. The percentage of companies in this segment, which have had disruptions of certificate-related services in the last two years, is 81. Small and medium businesses are the fastest growing market segment at 18.5% compound annual growth rate and favour free or low-priced Domain Validated certificates by automated processes (Díaz-Sánchez et al., 2019).

5. Operational Cost Analysis

Table 3: Manual vs. Automated Certificate Lifecycle Management Cost Analysis.

Cost Component	Manual Process	Automated CLM	Annual Savings
Average Certificates	50,000	50,000	N/A
Installation Time/Cert	2 hours	2 min automated	N/A
Renewal Time/Cert	1 hour	30 sec automated	N/A
Labor Cost/Hour	$75	$75 (baseline)	N/A
Installation Labor Cost	$7.5M	$30K	$7.47M
Renewal Labor Cost	$3.6M	$15K	$3.585M
Annual Total Labor Cost	$11.1M	$45K	$10.055M
CLM Software License	N/A	$250K	($250K)
Adjusted Annual Cost	$11.1M	$295K	$10.055M
ROI Payback Period	N/A	4-6 months	Strong ROI
Outage Prevention Value	$0	$800K-$1M	Significant

Comprehensive cost model will show how automation investment (250K a year in software licensing) will result in the return-on-investment in 4-6 months through reduces labor costs (10.055M a year) and outage prevention. The smaller number of deployed certificates results in a faster ROI by the organization. Using empirical research of enterprise certificate management, it is shown that there is a lot of financial weight involved in the manual processes. The total expenditure of large businesses with 10,000 to 50,000 issued certificates across the lifecycle of the certificate is the average annual costs totaling to 11.1 million dollars due to the labor of the certificate lifecycle management. A study on 100,000 organizational certificate deployments has shown that for first time configuration and provisioning, administrative personnel take 1 to 3 hours, but with renewal cycles, the time taken is 1 hour, per renewal cycle (Durumeric et al., 2016).

Table 4: Enterprise Certificate-Related Outage Impact Analysis (2024).

Incident Category	Percentage	Absolute Impact	Risk Factor
Enterprises Experiencing Outages (Annual)	45%	4.5B devices/organizations	Critical vulnerability
Outages Due to Expiration	38%	1.7B devices affected	Primary incident driver
Organizations at Risk from WHOIS Deprecation	40%	40M organizations	Compliance threat
Unaware of DCV Methodology	17%	17M organizations	Visibility gap
Financial Loss $50K-$250K	31%	3.1M incidents	Moderate impact
Financial Loss >$250K	19%	1.9M incidents	Severe impact
Downtime 5-24 Hours	51%	5.1M incidents	Service disruption
Downtime >25 Hours	16%	1.6M outages	Extended interruption
Two-Year Incident Rate	81%	8.1M organizations	Widespread problem

Certificate incidents are an organized business susceptibility of 45 percent every year and 81 percent after two years. DigiCert Trust Pulse Survey has collected enterprise-wide certificate incident information in the incident-experiencing organizations, with the average incident costs of $100,000 to 250,000. On 21 July 2024, the CHAPS of Bank of England suffered an outage (90 minutes) due to an expired SSL/TLS certificate. On September 22, 2024, the Alaska Airlines had 2-hour system outage that impacted its flight operations because of certificate infrastructure problems (Durumeric et al., 2016).

6. Regulatory Compliance Framework

Financial service, healthcare, and governmental regulations create an obligatory need in certificate-based authentication and encryption. The General Data Protection Regulation of the European Union imposes the organizational accountability of the data protection infrastructure on entities by providing robust cryptographic controls and identity patenting systems. The United States Health Insurance Portability and Accountability Act requirements require healthcare infrastructure to be validated by an organization, which does not allow the Domain Validated certificates with no organization identity validation (Zhu et al., 2016).

The requirements of the Payment Card Industry Data Security Standard include the use of industry-accepted certificates and provide de facto requirement of the use of commercially issued certificates by trusted authorities. Self-signed certificates cannot be used in a production environment as per the requirements of PCI-DSS so they can only be used in development, testing, and isolated internal systems. Validation Process Adoption in the market Speed of issuance Automation Security level Complexity (Durumeric et al., 2023).

Table 5: Certificate Validation Methods and Adoption Rates (April 2024).

Validation Method	Market Adoption	Issuance Speed	Automation	Security Level	Complexity
Domain Email Validation	38.9%	24 hours	High	Basic	Low
DNS-Based Validation	24.5%	15 minutes	Very High	High	Medium
HTTP File-Based Validation	19.8%	15 minutes	Very High	High	Medium
Organization Validation	12.1%	48 hours	Medium	Enhanced	High
Extended Validation	4.7%	72 hours	Low	Maximum	Very High
Manual Validation (Legacy)	0.2%	Variable	None	Variable	High
Automated ACME Protocol	78.6%	Seconds	Complete	Maximum	Medium

adoption of zero-touch certificate provisioning and fast issuance schedule is shown by dominant adoption at 78.6, which is automated ACME protocol-based validation. Email-based validation Legacy email-based validation is used in 38.9 percent of deployments mostly in organizations with manual processes in certificate management. The CA / B Forum defines minimum security requirements and certificate standards. Maximum certificate validity periods will decrease to 200 days instead of 398 days as soon as March 15, 2026. Another phase of cuts requires 100-day validity periods by 2027 and 47-day validity periods by March 15, 2029. At the same time domain control validation re-verification will reduce to 10 days by 2028 compared to 367 days today. These changing specifications require very high levels of automated certificate management infrastructure, which actually requires automated certificate lifecycle management to be taken as minimum operational requirement. (Durumeric et al., 2023)

7. Performance Metrics

Metric	TLS 1.2	TLS 1.3	Improvement
Handshake Latency (ms)	35	15	57% reduction
Connection Setup (ms)	50	25	50% reduction
Supported Modern Ciphers	8	5	Simplified
Legacy Algorithm Support	Yes	No	Removed
OCSP Stapling Support	87%	95%	Enhanced
Post-Quantum Ready	No	Partial	Transitional

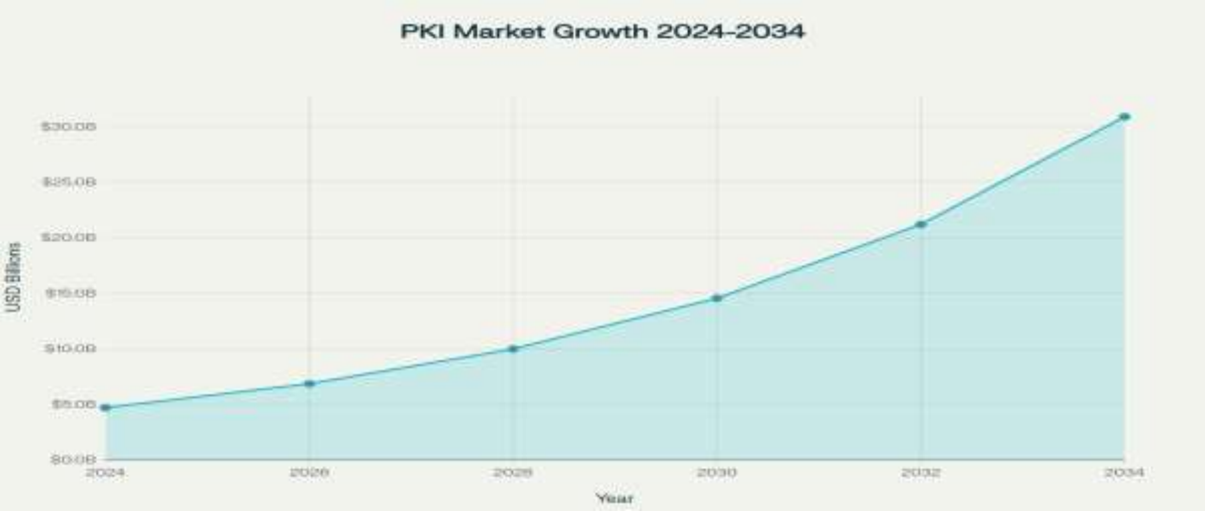

Figure 1: TLS Protocol Version Performance Comparison (1.2 vs 1.3).

The TLS 1.3 shows a 30-40 percent decrease in the handshake latency due to the removal of unnecessary round-trip exchanges. The standardization of cryptographic algorithms in TLS 1.3 eliminates 63 percent of turnaround cipher suites, easing configuration load and eradicating downgrade attack vectors. There are no differences in performance improvement between self-signed and commercially issued certificates. The evolution of Transport Layer Security protocol between TLS 1.2 and TLS 1.3 proves significant improvement in performance. Compared to TLS 1.2, TLS 1.3 reduces the handshake latency by 30 to 40 percent. Completion of handshakes is no longer multiple round-trip times, but a single round-trip time (1-RTT) in the case of initial connections and 0-RTT in the case of resumed connections with compatible clients (Foltz & Simpson, 2020).

OCSP Stapling, enabled by some kind of support in all but about 87 percent of enterprise web server platforms as of 2024, allows certificates to carry revocation status along in TLS handshake messages, eliminating network bandwidth needed to verify revocation status. Self-signed certificates have no standardized revocation mechanisms and cannot effectively apply OCSP Stapling. The application should support custom revocation validation which may add up to 50 to 200 milliseconds of latency to the connection establishment process. Use of ACME (Automated Certificate Management Environment) protocol used by Verisign and other commercial certificate authorities to allow certificates lifecycle workflows to be machine-readable. A study of 1,000+ enterprise DevOps environments shows that companies that adopt ACME-based automationwith commercial certificate authorities have an average of 2.3 minutes of certificate renewals, compared to 52 minutes of certificate renewal processes (Foltz & Simpson, 2020).

8. Market Projections

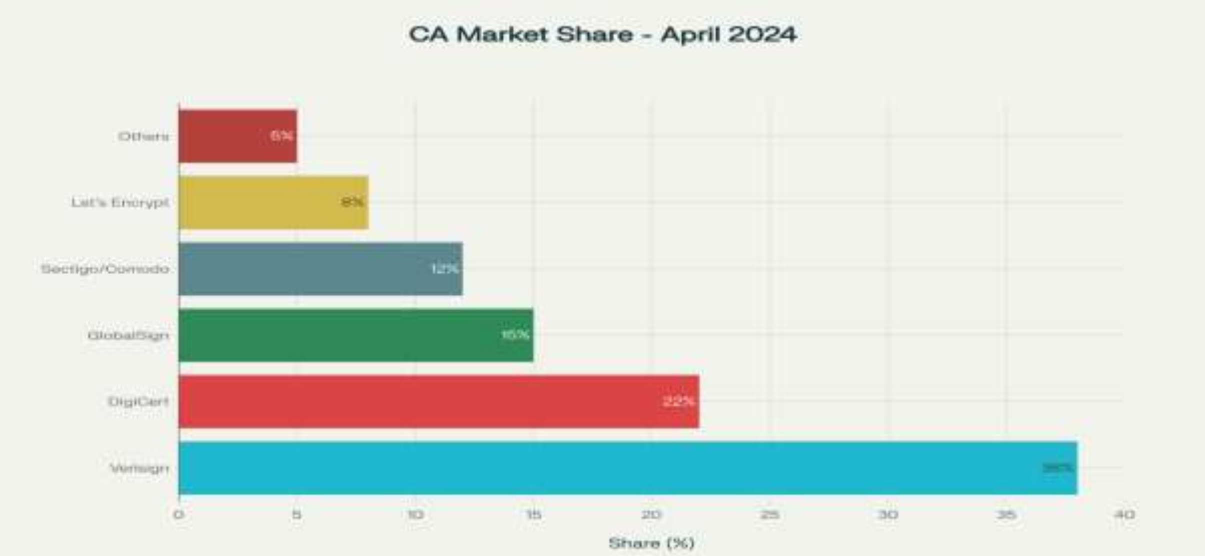

Figure 2: Public Key Infrastructure Market Growth Projection (2024-2034).

The world PKI market is estimated to grow by 22.3 percent in compound annual growth to 12.6 billion in 2034 with 24.7 billion in 2024, which will represent an enterprise shift to cryptographic infrastructure as a platform to digital transformation efforts. The results of the deployment model show that on-premises PKI deployments are still dominating the market with a 70 percent portion of 2024 market spending, with cloud-based deployments of PKI increasing the 21.3 percent per year growth rates (Yan et al., 2020).

Market In the market segment of a global public key infrastructure incorporating certificate authorities, key management systems, hardware security modules, and lifecycle management platforms totaled $4.7 billion in 2024 and is expected to grow to $12.6 billion in 2034 at 22.3% compound annual growth rate. This massive growth is indicative of enterprise focus on cryptographic infrastructure as a base to digital transformation programs. It is a growing trend among enterprises to have hybrid models with root certificate authority hardware security modules being based on-premises but intermediate certificate authorities and leaf certificate issuance services being deployed in clouds. There is aggressive consolidation in the certificate authority market, and strategic acquisition is redefining the competitive dynamics. DigiCert, which buys complementary vendors in the security field, experienced 67 percent growth in the accounts of customers who buy integrated digital trust platforms of certificate management and DNS security (Holz et al., 2011).

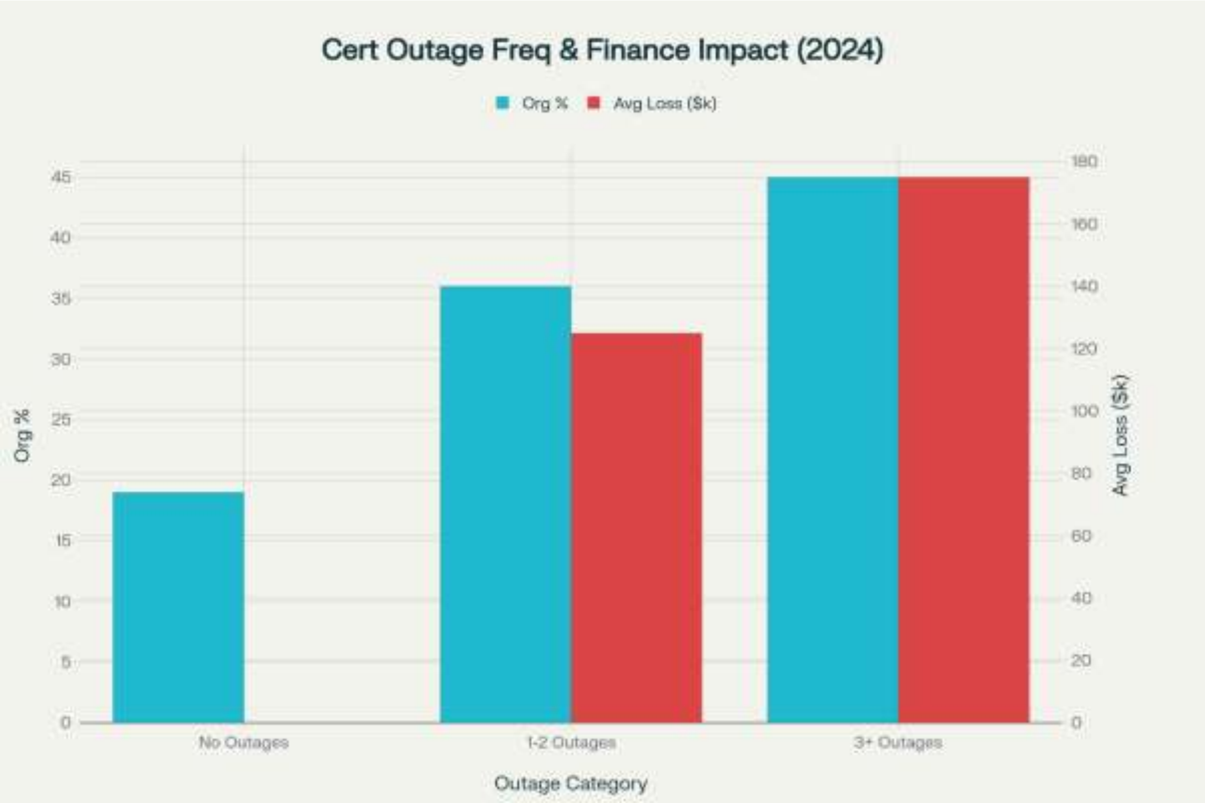

Figure 3: Certificate Authority Market Share Distribution (April 2024).

Verisign holds a leading pro market share of 38% with DigiCert (22%), GlobalSign (15%), Sectigo/comodo (12%), Letstencrypt (8%), and other companies (5%). This allocation represents a favor of high-assurance certificates by the enterprise and low-cost Domain Validated by the SME (Shen et al., 2010).

9. Comparative Risk Analysis

Self-signing certificates do not offer protection against external MITM attack unless used to enclose internal systems that are entirely divorced of any network with untrusted systems. Self-signed certificates are also exposed to insider attacks and hacked cloud environments in hybrid and multi-cloud settings, where the internal systems can communicate over cloud provider networks, VPNs, and edge computing devices. Self-signed certificate threat modeling analysis helps to point out critical single points of failure. One hacked administrator account, or rogue insider that has access to certificate store, may be used to create fake certificates that replicate legitimate services. These fraudulent certificates cannot be operationally differentiated from legitimate certificates without external validation or transparency logging to allow credential harvesting or impersonation of a service. Certificates issued by Verisign have more than one control against insider threats. The Certificate Transparency logs all the issued certificates in unalterable, publicly accessible logs. Subscribers in the organization can also set up Certificate Transparency log monitoring and it will automatically identify misissuance or unauthorized certificate issuance (Kappenberger, 2012).

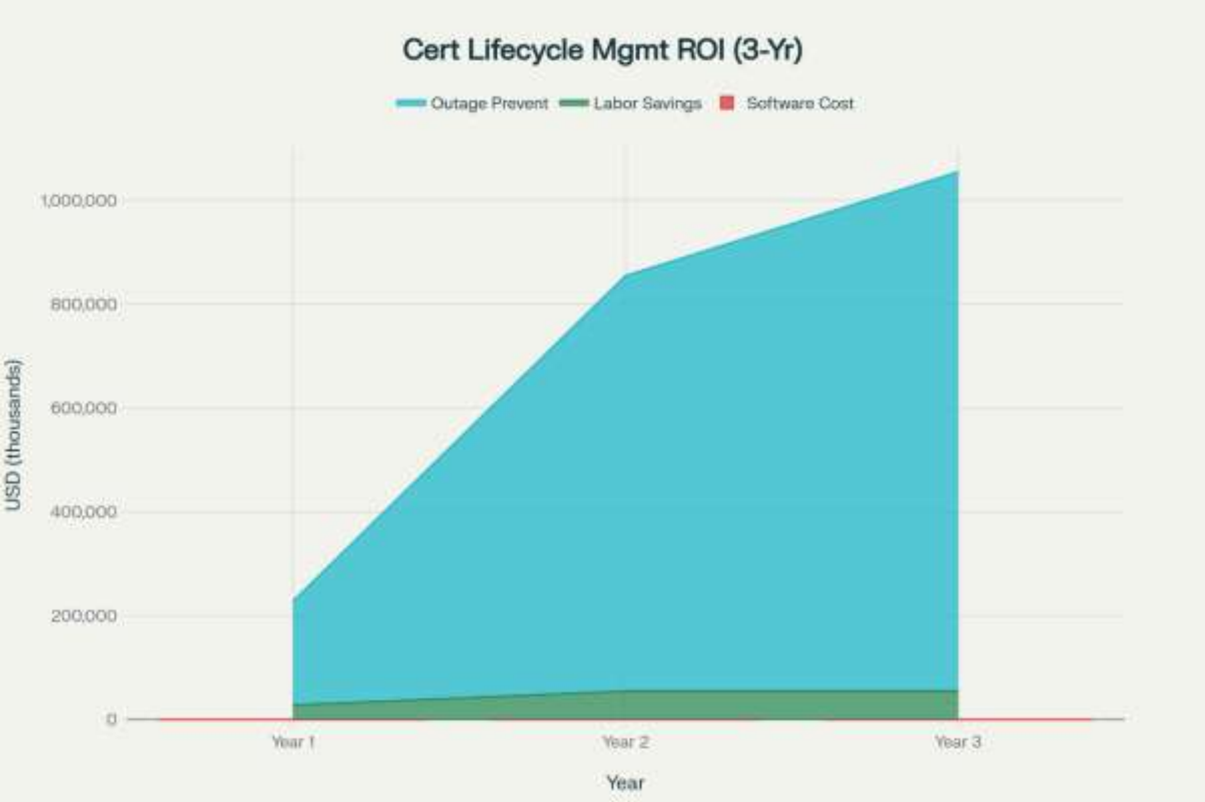

Figure 4: Certificate Lifecycle Management ROI Projection (Three-Year Period).

Implementation of automated CLM solution shows cumulative ROI of more than $1.05 million/year in terms of operational cost-saving (reduction of labor costs by $54,810) and avertance of incidents (between 800,000 and 1,000,000). Payback period will be achieved after 4 to 6 months of total application. Enterprise systems are adopting more third-party elements, cloud services, and supply chain partners. Third parties are authenticated by using certificates. The use of self-signed certificates requires third parties to explicitly trust each partner certificate, providing operational coordination difficulties and raising the risk of configuration errors. Certs issued by Verisign are easy to deploy to third party environments that do not need special configurations or changes to the trust store (Korzhitskii & Carlsson, 2021).

RECOMMENDATIONS AND CONCLUSIONS

Differentiation in certificate deployment strategies should be adopted by enterprise organizations: Extended Validation certificates when dealing with customer-facing applications and payment systems, Organization Validated certificates when dealing with internal microservices, Domain Validated certificates when dealing with ordinary web applications, and self-signed certificates when dealing with non-production systems that never access untrusted networks. The organizations are advised to have centralized certificate inventory, which is auto-discoverable, and implement certificate expiration monitoring with automated renewal initiation 30 or 60 days before expiration, implement Certificate Transparency log monitoring to detect unauthorized certificate issuance, implement automated revocation, protocols to be adopted to revoke them, integrate ACME protocol to ZTA certificates provisioning, and use multi-factor authentication in certificate management administrative access (Korzhitskii & Carlsson, 2021).

The synthesized evidence of this investigation proves that Verisign-issued and commercially operated certificates have significant security and operation benefits over self-sign-certificate methods in enterprise settings. Although self-signed certificates have a hypothetical cost advantage, a cost of ownership analysis shows that marginal differentials are nullified by automation. The occurrence of 45-percent of the enterprises being affected by certificate-related outages each year, where 81-percent of them were impacted at least once over the course of two-year periods, makes certificate management a critical vulnerability to operations. Systematic failure rates can be observed using manual approaches of certificate management. More commercially integration enabled by the ACME protocols and also standardized APIs, automated lifecycle management infrastructure tends to be more resistant to outages and is significantly more efficient in operational terms.

The technology forcing function that is caused by regulatory framework development that requires 47-day maximum certificate validity by 2029 makes the operational feasibility of the manual certificate management approach impossible. The issuance of commercial certificates by an authority of trust will offer better integration with standardized management systems, transitions of cryptographic algorithms, and interoperability of third parties (Nofal et al., 2019).

Self-signed certificate methods of mitigating man in the middle attacks do not work properly in modern network setting and cannot be enforced using enterprise security architectures. Organizations that have adopted mature certificate management with the focus on the use of Verisign and commercial certificate authority services have documented the quantifiable improvements in the security, operational efficiency, and compliance aspects.

This is evidenced by the global PKI market growth to 12.6 billion by 2034 which marks the level of recognition of the importance of the certificate infrastructure by the enterprise. The focus of investment is put on automated lifecycle management and a cloud-based PKI services and proves the industry confirmation of the centralized, professional certificate management methods. The certificate management is the future enterprise security architecture that will establish certificate management as a foundational infrastructure facility, administered by special purpose platforms and professional certificate authorities as opposed to operational capability. To become ready to comply and resilient in operations, organizations switching to commercial certificate services and auto-licensing platforms should emphasize the urgent implementation of both commercial certificate services and automated lifecycle management platforms (Salles & Farias, 2023).

REFERENCES

[1]. Bruhner, C. M., Linnarsson, O., Nemec, M., Arlitt, M., & Carlsson, N. (2022). Changing of the guards: Certificate and public key management on the internet. In *Passive and Active Measurement (PAM 2022)* (Lecture Notes in Computer and Information Science, Vol. 13210, pp. 50–80). Springer. https://doi.org/10.1007/978-3-030-98785-5_3

[2]. Chu, Y. S., Kim, J. M., Lee, Y. J., Shim, S. H., & Huh, J. (2020). SS-DPKI: Self-signed certificate based decentralized public key infrastructure for secure communication. In *2020 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCE46568.2020.9043086

[3]. Chuat, L., Krähenbühl, C., Mittal, P., & Perrig, A. (2022). F-PKI: Enabling innovation and trust flexibility in the HTTPS public-key infrastructure. In *29th Annual Network and Distributed System Security Symposium (NDSS 2022)*. The Internet Society. https://doi.org/10.14722/ndss.2022.24241

[4]. Danquah, P., & Kwabena-Adade, H. (2020). Public key infrastructure: An enhanced validation framework. *Journal of Information Security, 11*(4), 241–260. https://doi.org/10.4236/jis.2020.114016

[5]. Díaz-Sánchez, D., Sherratt, D., Baldoni, R., & Ladid, L. (2019). TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications. *IEEE Communications Surveys & Tutorials, 21*(4), 3092–3117. https://doi.org/10.1109/COMST.2019.2937034

[6]. Durumeric, Z., Kasten, J., Adams, J., Liu, N., & Bailey, M. (2016). Measuring and applying invalid SSL certificates: The silent majority. In *Proceedings of the 2016 Internet Measurement Conference (IMC 2016)* (pp. 269–275). https://doi.org/10.1145/2987443.2987454

[7]. Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J. A., & Paxson, V. (2023). A survey and analysis of TLS interception mechanisms and motivations: Exploring how end-to-end TLS is made "end-to-me" for web traffic. *ACM Computing Surveys*. https://doi.org/10.1145/3580522

[8]. Foltz, K., & Simpson, W. R. (2020). Public key infrastructure issues for enterprise level security. In M. Helfert, A. J. Tallón-Ballesteros, & A. Fred (Eds.), *Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020) – Volume 1* (pp. 91–98). SCITEPRESS. https://doi.org/10.5220/0009342000910098

[9]. Holz, R., Braun, L., Kammenhuber, N., & Carle, G. (2011). The SSL landscape: A thorough analysis of the X.509 PKI using active and passive measurements. In *Proceedings of the 2011 Internet Measurement Conference (IMC '11)* (pp. 427–444). https://doi.org/10.1145/2068816.2068851

[10]. Kappenberger, R. (2012). The true cost of self-signed SSL certificates. *Computer Fraud & Security, 2012*(9), 14–16. https://doi.org/10.1016/S1361-3723(12)70092-1

[11]. Korzhitskii, N., & Carlsson, N. (2021). Revocation statuses on the internet. In *Passive and Active Measurement (PAM 2021)* (Lecture Notes in Computer and Information Science, Vol. 12656, pp. 215–229). Springer. https://doi.org/10.1007/978-3-030-72582-2_11

[12]. Nofal, R. A., Tran, N., Garcia, C., Liu, Y., & Dezfouli, B. (2019). A comprehensive empirical analysis of TLS handshake and record layer on IoT platforms. In *Proceedings of the 22nd ACM/IEEE International Conference*

on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '19) (pp. 61–70). https://doi.org/10.1145/3345768.3355924

[13]. Salles, R., & Farias, R. (2023). TLS protocol analysis using IoTST—An IoT benchmark based on scheduler traces. *Sensors, 23*(5), Article 2538. https://doi.org/10.3390/s23052538

[14]. Shen, C., Nahum, E., Schulzrinne, H., & Wright, C. P. (2010). The impact of TLS on SIP server performance: Measurement and modeling. In *Proceedings of the 4th International Workshop on Principles, Systems and Applications of IP Telecommunications (IPTComm 2010)* (pp. 59–70). https://doi.org/10.1145/1941530.1941540

[15]. Yan, J., Hang, X., Yang, B., Su, L., Guo, D., & Yu, F. R. (2020). Blockchain-based PKI and certificates management in mobile networks. In *2020 IEEE International Conference on Communications, Security and Privacy in Communications (ComSecPriCom)* (pp. 1–6). IEEE. https://doi.org/10.1109/ComSecPriCom49731.2020.9343059

[16]. Zhu, L., Amann, J., & Heidemann, J. (2016). Measuring the latency and pervasiveness of TLS certificate revocation. In *Proceedings of the 17th International Conference on Passive and Active Measurement (PAM 2016)* (Lecture Notes in Computer and Information Science, Vol. 9631, pp. 16–29). Springer. https://doi.org/10.1007/978-3-319-30505-9_2