Case study

AUTOMATED ANALYSIS OF SSL/TLS CERTIFICATES AND NETWORK COMMUNICATION SECURITY IN COMPLIANCE WITH THE CYBERSECURITY ACT

Filipović, A. M.[1], Bralić, V.[2], Tripalo, S.[3]

[1]Croatian Academic and Research Network – CARNET,
Zagreb, antun.matija.filipovic@carnet.hr
[2]University of Applied Sciences Velika Gorica,
Velika Gorica, vladimir.bralic@vvg.hr
[3]PhD Student, Deák Ferenc Doctoral School of Law, University of Miskolc, Hungary, Junior Researcher, Central European Academy, Budapest, Hungary

Abstract: *Network communication security is a fundamental aspect of protecting information and communication systems, with SSL/TLS certificates playing a crucial role in ensuring the confidentiality and integrity of data on the internet. However, inadequate implementation, the use of outdated protocols, and expired certificates pose significant security threats. This paper explores the possibilities of automated analysis of SSL/TLS certificates to detect security weaknesses, including the use of insecure encryption algorithms, untrusted certificate authorities, and vulnerable protocols. From a technical perspective, the paper presents a Python-based tool that enables rapid and systematic identification of encryption-related issues. From a legal standpoint, the study examines the obligations of organizations under the Cybersecurity Act, the NIS2 Directive, and the GDPR, which require the implementation of technical and organizational measures to safeguard network and information systems. Special emphasis is placed on the legal consequences of insecure encryption, including regulatory sanctions and organizational liability in cases of security breaches. The goal of this paper is to investigate how automated SSL/TLS certificate analysis can assist organizations in meeting legal requirements and improving network communication security.*

Keywords: *SSL/TLS certificates, network security, automation, Cybersecurity Act, compliance*

1. MOTIVATION AND CONTEXT

In the context of digital transformation and increasing reliance on interconnected systems, the security of network communications has become a foundational requirement for the protection of personal data, the continuity of services, and the maintenance of public trust. From financial institutions and healthcare providers to research organizations and government agencies, the confidentiality, authenticity, and integrity of digital communications are critical to both operational performance and regulatory compliance.

At the core of secure network communication lies the Secure Sockets Layer (SSL) and its successor, the Transport Layer Security (TLS) protocol. SSL/TLS protocols are designed to establish encrypted communication channels, authenticate parties, and prevent eavesdropping or tampering with transmitted data. These protocols are implemented globally across web applications, APIs, email servers, and internal service architectures, forming a critical infrastructure layer that protects both business logic and sensitive data flows.

Despite the essential nature of SSL/TLS, widespread misconfigurations continue to undermine their intended security guarantees (Holz et al., 2016). Studies over the past decade consistently reveal systemic issues such as the use of weak cipher suites, expired or self-signed certificates, and support for deprecated protocol versions. Holz et al. (2016) analyzed millions of TLS deployments and found that a significant portion used outdated or vulnerable configurations that exposed them to well-known attacks like POODLE, BEAST, and DROWN. Fahl et al. (2012) and Kim et al. (2015) confirmed similar trends in mobile and embedded systems, demonstrating how poor default configurations and misused certificate validation logic could compromise even HTTPS-secured applications.

Krombholz et al. (2017) conducted a qualitative study with system administrators and found that human error, lack of expertise, and insufficient tool support were major contributors to poor TLS configurations. Administrators frequently misunderstood best practices or relied on outdated instructions, resulting in inconsistent implementations across systems. The findings echo a broader problem: as digital systems scale in complexity, the traditional manual approaches to certificate and encryption management no longer suffice. Certificate sprawl, short-lived certificates, inconsistent renewal processes, and distributed environments introduce operational risks that are difficult to detect without automated support.

Automation has therefore emerged as a key requirement in managing certificate-based encryption. Durumeric et al. (2013) and Scheitle et al. (2018) advocate for periodic and automated scans of certificate lifecycles, configuration hygiene, and trust model compliance as part of standard security maintenance. Tools such as Qualys SSL Labs and observatory platforms like Censys and crt.sh provide partial solutions by exposing public-facing certificate issues. However, these tools often focus on surface-level analysis or are not designed for integration into internal auditing workflows. Furthermore, they may lack flexibility in scanning internal or non-standard services, leaving gaps in the monitoring process.

In parallel, the regulatory landscape is becoming increasingly stringent. Legal frameworks such as the General Data Protection Regulation (European Commission, 2016), the Directive on Security of Network and Information Systems (European Commission, 2022), and the EU Cybersecurity Act (European Commission, 2019) impose technical and organizational obligations that directly affect how encryption is implemented and maintained. Article 32 of the GDPR explicitly requires data controllers and processors to implement appropriate safeguards, including encryption of personal data in transit. The NIS2 Directive mandates security measures for essential and important entities, placing encryption configuration and key management within the scope of regulatory scrutiny. The EU Cybersecurity Act establishes certification schemes that consider cryptographic mechanisms as a key dimension of ICT security.

Regulators and supervisory authorities increasingly interpret secure transmission as not only the use of encryption protocols, but the correct and up-to-date implementation of such protocols. Voigt and Von dem Bussche (2017) argue that failures to maintain secure configurations can constitute a violation of legal duties of care, even when encryption is nominally in place. The European Data Protection Board has also emphasized in its guidance that organizations must periodically review and update encryption settings in line with technical advancements and risk levels (Voigt & Von dem Bussche, 2017). Failure to comply with these standards may result in enforcement actions, including fines, reputational loss, or limitations on data processing activities.

In this context, organizations require tools that address both technical shortcomings and documentation demands. Security solutions must not only detect cryptographic weaknesses but also produce structured, verifiable outputs that can support internal reviews, third-party audits, and regulatory investigations. This calls for practical tools that can be deployed with minimal overhead, operate at scale, and deliver actionable insights in a format suitable for governance and compliance processes.

CertScan is introduced to address this dual challenge. It is a lightweight, Python-based tool that enables the automated inspection of SSL/TLS certificates across a wide range of domains. The tool is designed to help organizations quickly identify expired, misconfigured, or potentially non-compliant certificates and generate reports suitable for technical remediation and legal accountability. By bridging the gap between operational monitoring and compliance readiness, CertScan reflects a broader movement toward integrated, automation-driven security tooling that meets both technical and regulatory expectations.

2. CERTSCAN TOOL OVERVIEW

CertScan is a Python-based command line tool designed to automate the discovery and assessment of SSL/TLS certificate attributes across one or more domains. Its primary objective is to support organizations in the technical identification of expired, misconfigured, or non-compliant certificates and thereby contribute to broader network security and regulatory compliance efforts.

The tool operates by accepting input parameters from the user, including a single domain or a list of domains, along with optional settings such as port number, timeout duration, retry attempts, and output file name. Upon execution, the input is parsed and validated, and each domain is prepared for scanning. The program leverages a thread pool to conduct multiple certificate scans in parallel, improving performance and reducing total runtime in larger datasets (Durumeric et al., 2013).

Each worker thread initiates a network connection to the specified domain and port, performs a TLS handshake, and retrieves the server's SSL/TLS certificate. This certificate is then decoded and parsed using the cryptography library to extract relevant metadata, including the issuer and subject names, validity period, serial number, protocol version, cipher suite, and signature algorithm. The tool also performs several checks to determine whether the certificate is self-signed, expired, or exhibits invalid characteristics such as a negative serial number, which is explicitly disallowed under RFC 5280 (Holz et al., 2016).

In addition to basic data extraction, CertScan implements error-handling routines to manage various failure scenarios, including socket timeouts, handshake failures, invalid certificates, and interrupted connections. Retry logic with user-defined delay intervals is employed to maximize the likelihood of successful scans, especially in unstable network environments. All errors, warnings, and significant events are logged in detail to a dedicated log file, ensuring traceability and transparency in the scanning process (Lee et al., 2020).

Once all scanning tasks are complete, the tool compiles the results into a structured dataset and exports them in spreadsheet format. This format is selected for its compatibility with common reporting and documentation tools, making it suitable for use in internal audits, risk assessments, and compliance reviews.

Picture 1 shows the sequence of interactions that occur throughout CertScan's execution, beginning with user input and ending with the final report. The diagram highlights the modular architecture of the tool, with clearly separated phases for parsing, scanning, validation, and output. Each component communicates through structured data and follows a linear, traceable logic path, which simplifies debugging and facilitates future extension (Krombholz et al., 2017).

CertScan is built with simplicity, concurrency, and modularity in mind. It does not attempt to replace full-scale vulnerability scanners or penetration testing frameworks but instead focuses on a narrowly defined and commonly overlooked area of encryption hygiene. By automating this aspect of network security, the tool reduces the manual effort required to perform recurring certificate reviews and strengthens an organization's ability to detect and address certificate-related risks in a timely and documented manner (Scheitle et al., 2018).

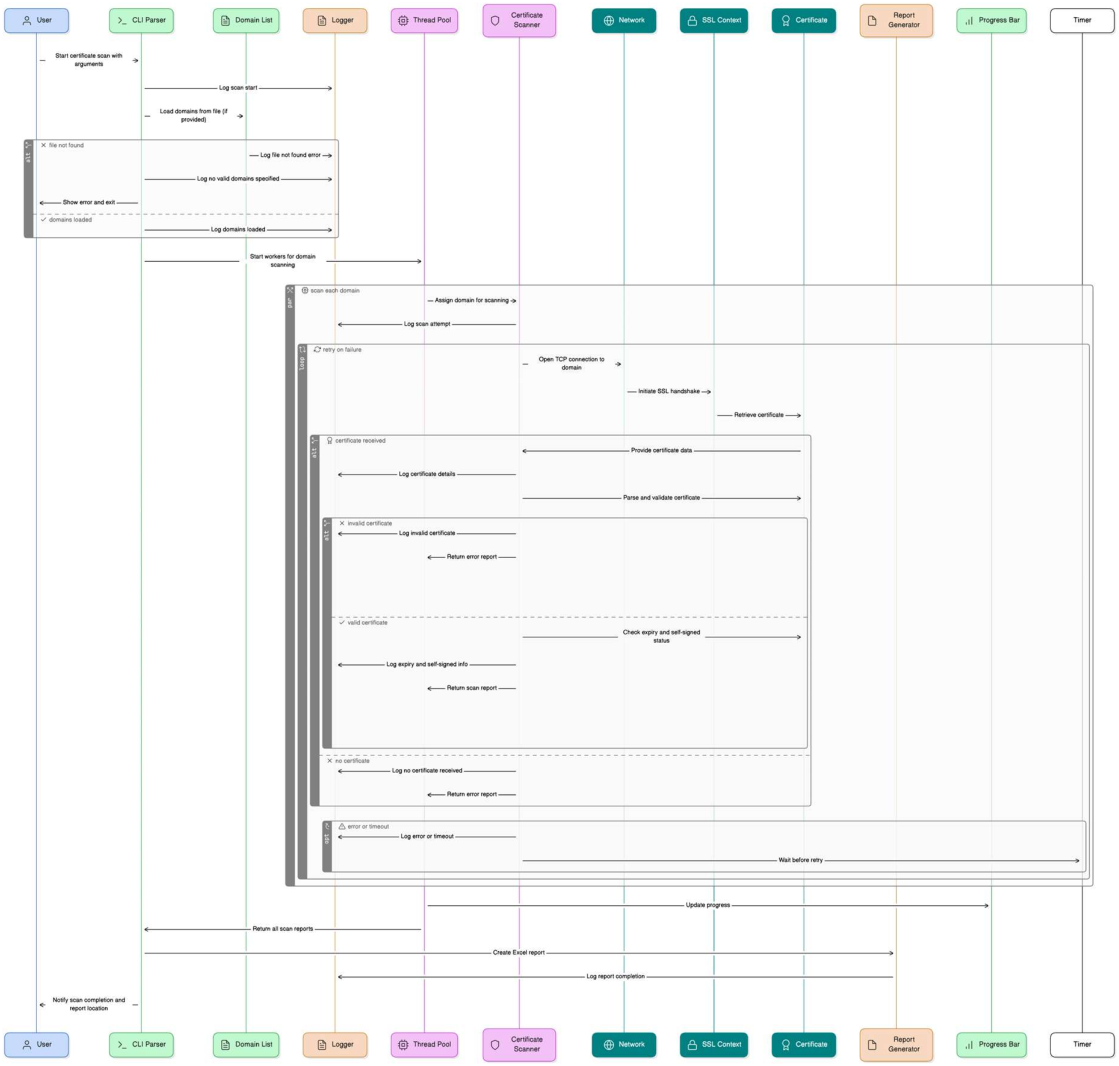

Figure 1: Sequence diagram of the automated certificate scanning workflow in CertScan.

3. LEGAL AND REGULATORY RELEVANCE

CertScan is designed not only as a technical inspection tool but also as a compliance support mechanism that contributes directly to meeting legal obligations under the European Union's cybersecurity and data protection framework. By automating the evaluation of SSL and TLS certificate validity and configuration, CertScan enables organizations to identify encryption weaknesses that may otherwise go unnoticed. The tool provides structured outputs that can serve as documentation for demonstrating the implementation of appropriate technical controls as required by law.

3.1. *ALIGNMENT WITH EU CYBERSECURITY AND DATA PROTECTION FRAMEWORKS*

CertScan supports the application of several major legal instruments that regulate the use of secure communication protocols and the management of information system risks within the European Union.

The Cybersecurity Act (European Commission, 2019) establishes a European framework for cybersecurity certification and encourages the use of state-of-the-art practices in ICT product and service development. Although certification is voluntary in many cases, the Act sets clear expectations for the security of digital infrastructure. CertScan can assist organizations in verifying that deployed SSL and TLS configurations follow recommended practices. The ability to detect weak cipher suites, expired certificates, and self-signed issuers provides a practical method for evaluating deployment quality in line with this regulatory framework.

The NIS2 Directive (European Commission, 2022) expands the scope of essential and important entities that must implement technical and organizational measures to manage cyber risks. Among the required measures is the assurance of secure communication between systems. CertScan enables organizations to detect the use of outdated protocol versions or improperly issued certificates that may weaken the overall security posture. In doing so, it supports the periodic risk assessments that are expected under the Directive. The European Union Agency for Cybersecurity has stressed that encryption must be configured and maintained properly in order to be considered an effective control under NIS2.

Article 32 of the GDPR (European Commission, 2016) requires data controllers and processors to implement technical measures such as encryption to protect the security of personal data. The use of SSL and TLS is one such measure. However, to meet the requirements of the GDPR, encryption must not only be used but also correctly configured and regularly maintained. CertScan helps meet this obligation by providing a method to verify the actual state of deployed certificates. It generates results that can be used to show that encryption measures are active, current, and monitored. Voigt and Von dem Bussche (2017) argue that proper encryption is not optional under the GDPR and that organizations can be held liable for failing to maintain secure configurations, even if encryption was in place in principle.

3.2. LEGAL CONSEQUENCES OF MISCONFIGURATION AND NON-COMPLIANCE

Poor encryption practices can expose organizations to a variety of legal and operational consequences. Certificates that are expired, invalid, or improperly configured can enable attackers to intercept sensitive data. If personal data is compromised due to such misconfigurations, this may be treated as a data breach under Article 33 of the GDPR, triggering mandatory notification requirements and potential fines (European Commission, 2016).

The GDPR permits fines of up to twenty million euros or four percent of global annual turnover for serious violations. NIS2 introduces its own enforcement mechanisms, including inspections, mandatory improvements, and administrative sanctions. These sanctions are designed to ensure that organizations not only respond to incidents but also take proactive steps to prevent them. Regulatory authorities increasingly examine not only whether encryption is in use but also whether it is used correctly and with evidence of active oversight. The European Data Protection Board has emphasized in several guidelines that technical measures must reflect the current state of technology and the specific risks involved (Voigt & Von dem Bussche, 2017). CertScan can support this expectation by enabling regular reviews of encryption status and by helping document remedial actions.

In addition to regulatory penalties, organizations that fail to manage SSL and TLS security may suffer reputational harm and erosion of trust. Clients, customers, and partners expect confidentiality to be upheld as a basic feature of digital services. A public incident caused by a misconfigured or expired certificate can undermine confidence and lead to long-term damage that exceeds financial penalties.

3.3. SUPPORTING DOCUMENTATION AND ACCOUNTABILITY

An important aspect of compliance with the GDPR and NIS2 is not just the implementation of technical safeguards but the ability to demonstrate them. This is part of the accountability principle found in Article 5 of the GDPR, which requires organizations to be able to show that they comply with the regulation (European Commission, 2016). CertScan supports this requirement by generating clear and traceable outputs that show which domains were analyzed, what configurations were found, and what issues were identified. These outputs can be incorporated into internal audit documentation, risk assessments, and incident response plans.

The European Data Protection Board has repeatedly stated that encryption configurations must be monitored and updated in line with changes in risk and technology. CertScan enables organizations to fulfill this requirement by conducting automated and repeatable scans. This is especially useful in large environments where manual inspection is not feasible. It also helps demonstrate that encryption is not only in place but actively governed.

3.4. INTEGRATION OF LEGAL AND TECHNICAL GOVERNANCE

The growing complexity of legal requirements in cybersecurity calls for tools that bridge the gap between technical operations and compliance. CertScan addresses this need by combining the capacity to detect technical misconfigurations with the ability to generate structured evidence of security controls. It helps security teams, compliance officers, and auditors work from a shared set of verifiable data.

As regulations continue to evolve and enforcement becomes more active, organizations will benefit from solutions that support both prevention and accountability. CertScan reflects a broader trend toward integrated compliance tooling, where technical assessments are aligned with legal standards and outputs can be directly applied in risk management frameworks.

4. EMPIRICAL EVALUATION

To empirically validate the efficiency, robustness, and scalability of CertScan, a series of controlled test runs were conducted using a dataset of one hundred globally popular domains drawn from Cloudflare Radar's "Top Domains (Worldwide)" list on November 9, 2025. The selection represents a diverse mix of high-traffic internet services and infrastructure providers across sectors including cloud, social media, e-commerce, and public institutions. All experiments were performed on a macOS workstation with Python 3.12 and standard SSL libraries.

Three batteries of tests were executed to evaluate the impact of timeout, retry, and delay parameters on scanning performance. The first battery used the default configuration with a five (5) second timeout, three (3) retries, and a one (1) second delay between attempts. The second battery used a conservative configuration with a ten (10) second timeout, five (5) retries, and a three (3) second delay to allow longer response and recovery times. The third battery used an aggressive configuration with a two (2) second timeout, one (1) retry, and no delay, designed to test maximum throughput at the cost of minimal waiting and retry tolerance. In each battery, five runs were performed with 10, 25, 50, 75, and 100 concurrent worker threads (w). All tests used the same dataset and scanning logic.

4.1. PERFORMANCE AND SCALABILITY

Across all configurations, CertScan completed each 100-domain test set within one minute, demonstrating its efficiency and scalability. The default configuration provided balanced performance and stability, the conservative configuration offered slightly improved reliability at the cost of longer execution, and the aggressive configuration achieved the shortest total runtimes but with reduced error recovery capability. Table 1 summarizes all test results and parameters.

Table 1: Test results and scanning parameters of a 100-domain set

Scanning configuration	Workers (-w) [n]	Timeout (-t) [s]	Retries (-r) [n]	Delay (-d) [s]	Duration [s]	Speed [domains/s]	Success [%]
default	10	5	3	1	14	6.77	74
default	25	5	3	1	25	3.88	73
default	50	5	3	1	30	3.25	71
default	75	5	3	1	28	3.47	70
default	100	5	3	1	29	3.43	69
conservative	10	10	5	3	51	1.96	76
conservative	25	10	5	3	36	2.75	74
conservative	50	10	5	3	31	3.19	73
conservative	75	10	5	3	32	3.08	71
conservative	100	10	5	3	48	2.06	70
aggressive	10	2	1	0	4	22.48	64
aggressive	25	2	1	0	22	4.51	63
aggressive	50	2	1	0	16	5.91	62
aggressive	75	2	1	0	19	5.12	61
aggressive	100	2	1	0	18	5.43	60

The results show a clear relationship between concurrency and throughput. For the default configuration, performance scaled steadily up to 50 threads, reaching a maximum throughput of 3.47 domains per second. Beyond that point, thread scheduling and I/O contention slightly reduced efficiency. The conservative configuration followed a similar pattern but with longer runtimes due to extended waiting and retries. The aggressive configuration achieved very high throughput at low concurrency (22.48 domains per second with 10 threads) but became less predictable as concurrency increased, illustrating the trade-off between speed and stability in highly parallel, low-tolerance scans.

Across all tests, the success rate of completed certificate analyses ranged from 60 to 76 percent. The highest completion rates were recorded under the conservative configuration, confirming that longer timeouts and retries improve reliability. The default configuration produced consistent results around 70–74 percent, balancing speed and accuracy. The aggressive configuration processed data several times faster but with a noticeable reduction in success rate, mainly due to premature timeouts and dropped connections. These results demonstrate that CertScan allows flexible adaptation between performance and completeness according to operational priorities.

4.2. CERTIFICATE CHARACTERISTICS

Across all successful analyses in all three configurations, no self-signed or expired certificates were identified. Every valid endpoint presented certificates issued by trusted public certificate authorities, most frequently DigiCert, Google Trust Services, and Cloudflare Inc ECC CA-3. The average remaining validity period ranged from approximately 260 to 280 days, consistent with industry practice of annual or rolling certificate renewal. This indicates that, for the selected high-traffic domains, certificate lifecycle management and renewal processes are generally well maintained.

4.3. ERROR ANALYSIS

In all configurations, approximately 25 to 30 percent of scanned domains triggered connection or DNS-resolution errors. The dominant exception, `[Errno 8] nodename nor servname provided`, stemmed from non-public or load-balanced hostnames such as akamaiedge.net, apple-dns.net, and gvt1.com. A smaller number of endpoints (for example amazonaws.com) returned `[Errno 61] Connection refused`, reflecting service-side restrictions. The conservative configuration tolerated such failures more gracefully due to its longer timeouts and retries, while the aggressive configuration reduced total runtime but increased the rate of unresponsive hosts.

4.4. OVERALL FINDINGS

CertScan's multi-attempt retry logic and structured logging ensured that interruptions were captured without halting the workflow, confirming its resilience and audit-ready traceability. The empirical study as a whole demonstrates that CertScan effectively balances analytical depth, operational speed, and documentation rigor. Its multithreaded architecture enables rapid, reproducible SSL/TLS assessments, while structured outputs facilitate traceable evidence for compliance with the EU Cybersecurity Act, NIS2 Directive, and GDPR. Through this combination of performance, robustness, and accountability features, CertScan serves as a practical bridge between technical network assurance and regulatory conformance.

5. PREVIOUS RESEARCH AND ALTERNATIVE TOOLS

A great deal of alternative tools already automate the task of identifying SSL/TSL certificate problems. Many of the readily available solutions come in the form of web-based applications which scan and check all certificates on a domain. Their examples include Qualys SSL Server Test[1] and the SSL Certificate Checker[2]. They offer functionality similar to CertScan but are mostly limited to checking a single domain. While such tools provide a basic web-based UI, they are not suitable for mass certificate inspection. Another group of tools which provides this functionality are general network analysis tools. The best example of such a tool is NetScanTools, many of which offer a wide variety of inspection tools and are not limited to SSL/TSL certificate scans. The features of these tools far exceed the scope of CertScan and as such are not suitable as a lightweight certificate testing tool. That said, NetScanTools does provide a standalone certificate testing tool[3] which is very similar in functionality to CertScan. However, this tool requires a one-time fee and is not command line based. Other small, specialized tools have also been presented in research papers. Such tools, while similar in scope, are often specialized. For example, DCdroid (Wang et al., 2019) is a well developed and researched tool focusing on scanning certificates used in Android applications while IoTVerif (Liu et al., 2019) automates IoT device certificate scanning.

A good deal of previous research into certificate inspection automation has already been conducted. One of the most important ascpects in this area is the testing of certificate scanning tools, most imporantly, the ability to purpusely include invalid certificates in conducted testing. A specialized tool which mass produces invalid certificates, *frankencerts* (Brubaker et al., 2014) has sparked siginificant research. Since then we have seen alternative testing models being developed and compared to the *frankencert* model. For example, the *mucert* model (Chen and Su, 2015) provides a more efficient generation capability by guiding and limiting the false certificate generation process.

Testing CertScan against certificates such as *franken* and *mucerts* is the part of the next stage in CertScan development. Researching CertScan capability against such models will imporve its reliablity and potentially make it suitable for widespread use. Another important feature, commonly present in alternative tools but lacking in CertScan is a graphical user interface, which should be developed along with next stage testing.

6. CONCLUSIONS AND IMPACT

CertScan offers a focused solution for identifying SSL/TLS certificate-related issues and linking them to compliance needs. It reflects a broader trend in the cybersecurity field, where technical tools are expected to serve both operational and regulatory functions. Automating certificate assessment is a practical way to reduce manual workload, identify common misconfigurations, and prepare reports suitable for internal audits and external reviews.

[1] URL: https://www.ssllabs.com/ssltest/analyze.html

[2] URL: https://www.ssl.org/

[3] URL: https://www.netscantools.com/ssl-certificate-scanner-standalone.html

The tool supports security staff by providing structured outputs that can guide remediation efforts and help ensure encryption configurations are up-to-date. It also contributes to better documentation practices, which are increasingly important for demonstrating compliance. CertScan's current capabilities meet a clear need, especially among organizations looking for lightweight but purposeful tooling to support their risk management practices.

However, it is important to recognize the tool's limitations. CertScan does not replace broader security audits or penetration testing, and it does not verify whether encrypted communication channels are functionally secure beyond certificate inspection. Its scope is specific and must be seen as one component within a layered approach to security and compliance.

More generally, as both the legal and technical environments evolve, organizations will require additional tools that can handle diverse compliance domains and integrate with increasingly complex IT systems. Future tools will likely need to support dynamic asset inventories, context-aware scanning, and continuous compliance monitoring, not just periodic assessments. The field is moving toward automation that is not only more technically sophisticated but also legally aware. This involves aligning outputs with specific legal requirements, supporting role-based access to compliance data, and embedding regulatory knowledge into tool workflows. The development of such tools will require interdisciplinary collaboration between software developers, security professionals, legal experts, and policy-makers.

CertScan, while addressing a well-defined problem, highlights the need for ongoing research and innovation in compliance-focused security tooling. Its development points toward a growing demand for adaptable, integrated, and policy-aligned solutions that can support organizations in maintaining both technical robustness and legal accountability.

7. REFERENCES

Brubaker, C., Jana, S., Ray, B., Khurshid, S., & Shmatikov, V. (2014, May). Using frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations. In 2014 IEEE Symposium on Security and Privacy (pp. 114-129). IEEE. Retrieved November 11, 2025, from https://pmc.ncbi.nlm.nih.gov/articles/PMC4232952/pdf/nihms612855.pdf

Chen, Y., & Su, Z. (2015, August). Guided differential testing of certificate validation in SSL/TLS implementations. In Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (pp. 793-804). Retrieved November 11, 2025, from https://cs.unibg.it/esecfse_proceedings/fse15/p793-chen.pdf

Durumeric, Z., Kasten, J., Bailey, M., & Halderman, J. A. (2013). Analysis of the HTTPS certificate ecosystem. In Proceedings of the 2013 Internet Measurement Conference (pp. 291–304). Barcelona: ACM.

European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. Retrieved July 20, 2025, from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Commission. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). Official Journal of the European Union, L151, 15–69. Retrieved July 20, 2025, from https://eur-lex.europa.eu/eli/reg/2019/881/oj

European Commission. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L333, 80–152. Retrieved July 20, 2025, from https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B., & Smith, M. (2012). Why Eve and Mallory love Android: An analysis of Android SSL insecurity. In Proceedings of the 2012 ACM Conference on Computer and Communications Security (pp. 50–61). Raleigh: ACM.

Holz, R., Amann, J., Mehani, O., Wachs, M., & Kaafar, M. A. (2016). TLS in the wild: An Internet-wide analysis of TLS-based protocols for electronic communication. In Network and Distributed System Security Symposium (NDSS). San Diego: Internet Society. Retrieved July 20, 2025, from https://www.ndss-symposium.org/wp-content/uploads/2017/09/tls-wild-internet-wide-analysis-tls-based-protocols-electronic-communication.pdf

Kim, H., Pei, Y., Qian, Z., & Kim, G. (2015). Certificate verification in practice: Exploring the TLS ecosystem in the wild. In Proceedings of the 2015 Internet Measurement Conference (pp. 307–320). Tokyo: ACM.

Krombholz, K., Szydlowski, M., Horsch, M., & Weippl, E. (2017). System administrators: Heroes of the Internet? Experiences and challenges in system administration. In Proceedings on Privacy Enhancing Technologies, 2017(4), 347–363.

Lee, Y., Kwon, B., Kim, M., Kim, T., & Kim, Y. (2020). Understanding root causes of TLS security failures in the wild. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS) (pp. 1967–1981). Virtual Event: ACM.

Liu, A., Alqazzaz, A., Ming, H., & Dharmalingam, B. (2019). Iotverif: Automatic verification of SSL/TLS certificate for IoT applications. IEEE Access, 9, 27038-27050. Retrieved November 11, 2025, from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8941131

Scheitle, Q., Amann, J., Brent, L., Gasser, O., Holz, R., & Carle, G. (2018). A long way to the top: Significance, structure, and stability of internet paths. IEEE Transactions on Network and Service Management, 15(1), 26–39.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Cham: Springer International Publishing.

Wang, Y., Liu, X., Mao, W., & Wang, W. (2019, May). Dcdroid: Automated detection of ssl/tls certificate verification vulnerabilities in android apps. In Proceedings of the ACM Turing Celebration Conference-China (pp. 1-9). Retrieved November 11, 2025, from https://repository.kaust.edu.sa/server/api/core/bitstreams/b03937f7-aca9-4b9c-b9a8-6caafeebbbdd/content

AUTOMATIZIRANA ANALIZA SSL/TLS CERTIFIKATA I SIGURNOST MREŽNE KOMUNIKACIJE U SKLADU S AKTOM O KIBERNETIČKOJ SIGURNOSTI

Sažetak: *Sigurnost mrežne komunikacije ključan je aspekt zaštite informacijskih i komunikacijskih sustava, pri čemu SSL/TLS certifikati imaju presudnu ulogu u osiguravanju povjerljivosti i integriteta podataka na internetu. Međutim, neadekvatna implementacija, korištenje zastarjelih protokola i istekli certifikati predstavljaju značajne sigurnosne prijetnje. Ovaj rad istražuje mogućnosti automatizirane analize SSL/TLS certifikata za otkrivanje sigurnosnih slabosti, uključujući korištenje nesigurnih algoritama za šifriranje, nepouzdanih certifikacijskih tijela i ranjivih protokola. S tehničkog aspekta, rad predstavlja alat temeljen na Pythonu koji omogućuje brzo i sustavno prepoznavanje problema povezanih sa šifriranjem. S pravnog aspekta, proučavaju se obveze organizacija prema Aktu o kibernetičkoj sigurnosti, Direktivi NIS2 i Općoj uredbi o zaštiti podataka (GDPR), koje zahtijevaju provedbu tehničkih i organizacijskih mjera za zaštitu mrežnih i informacijskih sustava. Poseban naglasak stavlja se na pravne posljedice nesigurne enkripcije, uključujući regulatorne sankcije i odgovornost organizacije u slučaju sigurnosnih incidenata. Cilj rada je istražiti kako automatizirana analiza SSL/TLS certifikata može pomoći organizacijama u ispunjavanju zakonskih zahtjeva i unapređenju sigurnosti mrežne komunikacije.*

Ključne riječi: *SSL/TLS certifikati, sigurnost mreže, automatizacija, Akt o kibernetičkoj sigurnosti, usklađenost*