Mitigating CA Rate Limits during Renewals in the Automated Centralized Certificates System

Arthur Petrosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: arthur@sci.am

Gurgen Petrosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: gurgen@sci.am

Robert Tadevosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: robert@sci.am

Abstract **- Some Certificate Authorities nowadays provide free wildcard certificates, but at the same time, enforce strict rate limits on certificate issuance and renewal to prevent abuse and maintain system stability. However, in large-scale network environments, where numerous services rely on automated certificate management, these limits pose operational challenges. This paper proposes a centralized strategy to mitigate CA rate limits during mass certificate renewals. The approach includes centralized certificate issuance, caching and sharing of wildcard certificates, intelligent scheduling, and multi-CA fallback mechanisms. The paper is a continuation of previous work in this area to build a production system using open-source tools, which was done within the Academic Scientific Research Computer Network of Armenia (ASNET-AM) and presented during past CSIT conferences.**

Keywords **- Certificate authority, rate limiting, ACME, TLS, SSL, certificate renewal, automation, DNS-01 challenge, dehydrated**

I. INTRODUCTION

The widespread adoption of the HTTPS protocol [1], HTTP Strict Transport Security (HSTS) made as a policy [2], secured access to Email service, and other TLS-based protocols has made the use of digital SSL certificates essential. At the same time, to take advantage of free certificates use of automated certificate management is needed. Public CAs such as Let's Encrypt [3] and ZeroSSL [4] utilize the ACME (Automated Certificate Management Environment) protocol [5] and freely provide even wildcard certificates. But they enforce rate limits on certificate issuance and renewal to prevent abuse. In environments with dozens or hundreds of dependent systems, exceeding these limits can lead to service outages.

This paper introduces a framework designed to mitigate CA rate limits during automated certificate renewal processes. The goal is to ensure continuity and reliability of TLS-based services in environments where many endpoints rely on frequent and timely certificate updates. This is an advancement of previous work in this area to build a production Automated Centralized Certificate Management System [6] using open-source tools, which was done within the Academic Scientific Research Computer Network of Armenia (ASNET-AM) [7]. The Automated Centralized Certificate Management System is now working in production in ASNET-AM and provides a centralized, secure, and automated free digital certificates service for multiple domains to different types of network services such as web servers, mail servers, etc.

II. BACKGROUND

Currently, free wildcard certificates are only being provided by a few CAs, each of them having its own appropriate rate limits. For example, Let's Encrypt CA enforces strict rate limits to ensure fair usage and system stability, especially for high-volume users and large organizations.

Current Let’s Encrypt rate limits are [8]:

- Certificates per Registered Domain - 50 per week
- New Orders per Account (3 hours) - 300
- Names per Certificate - 100
- Duplicate Certificates (per week) - 5
- Failed Validations (per hostname/hour) - 5
- Requests per Second - 20
- Accounts per IP (3 hours) - 10
- Accounts per IPv6 /48 (3 hours) - 500
- Label Depth (subdomain levels) - 10

Another CA - ZeroSSL, claims to impose significantly fewer rate limits than Let’s Encrypt [9]:

- Certificates per Registered Domain - No limit
- New Orders per Account (3 hours) - No limit
- Names per Certificate - No limit
- Duplicate Certificates (per week) - No limit
- Failed Validations (per hostname/hour) - No limit
- Requests per Second - 7
- Accounts per IP (3 hours) - No limit
- Accounts per IPv6 /48 (3 hours) - No limit
- Label Depth (subdomain levels) - 6

https://doi.org/10.51408/csit2025_75

It is clear that ZeroSSL offers much more relaxed rate limits, making it attractive for use, though its ACME API is limited to 7 requests per second.

During the past months of production use of the Automated Centralized Certificate Management System in ASNET-AM, it became obvious, that it is not so safe to rely on a single CA. Because, despite the published rates, the fact remains that when CA provides free services, it reserves the right to temporarily reject some requests at its discretion. And the above statement was proved by our tests, when even with a small load, periodical sequential requests for multiple certificates to the CA resulted in unexpected refusals (like with HTTP code 504 - Gateway Timeout).

Therefore, as an advancement of previous work in this area to build a production system using open-source tools, which was done within the ASNET-AM network and presented during past CSIT 2019 and CSIT 2021 conferences [10, 11], we currently design the improvement of our system by implementing multi-CA switching to mitigate CA rate limit issues.

III. Proposed Mitigation Strategies

In our Automated Centralized Certificate Management System, we already have a central server that handles certificate issuance and renewal, reducing the number of redundant ACME requests. The end-user systems (agents) retrieve certificates via secure channels.

Also, use of wildcard certificates (via DNS-01 challenge [12]) enables securing multiple subdomains with a single issuance. Wildcard certificates are renewed centrally and securely distributed to multiple agents.

In addition to that, we now propose to add two new improvements:

1. Intelligent Renewal Scheduling.

Certificates to be renewed at staggered intervals rather than all at once. The central server can maintain a renewal calendar and queue the system to throttle and distribute requests so as not to hit any of the CA limits.

2. Multi-CA Fallback Mechanism.

In case of refusal from some primary CA, the system can have fallback logic to switch to a secondary CA.

According to the above rate limit information and our experience, ZeroSSL CA can be treated as the primary CA, and the Let’s Encrypt CA as a secondary one. The system can be configured to maintain CA-specific ACME accounts and keys for several CAs.

IV. Conclusion

The described improvement to ASNET-AM Automated Centralized Certificate Management System will ensure scalable, uninterrupted certificate management at scale and smoothly fit into the already working certificate system, because of its modular structure.

It means multiple services like webhosting (HTTPS), Email (SMTPS/IMAPS/POP3S), and others, that are currently using the digital certificates provided by our system, have nothing to change at their level. The only improvements to be done are in the central server part.

Such an approach would balance CA rate limits, operational simplicity, and reliability. Using a multi-CA fallback strategy would leverage existing infrastructure seamlessly and continuously provide wildcard certificate support.

References

[1] HTTPS protocol. [Online]. Available: https://en.wikipedia.org/wiki/HTTPS

[2] HTTP Strict Transport Security Policy. [Online]. Available: https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

[3] Let's Encrypt Certificate Authority. [Online]. Available: https://letsencrypt.org/

[4] ZeroSSL Certificate Authority. [Online]. Available: https://zerossl.com/

[5] R. Barnes, J. Hoffman-Andrews, D. McCarney; J. Kasten, “Automatic Certificate Management Environment (ACME)”, *IETF*. doi:10.17487/RFC8555. RFC 8555

[6] ASNET-AM Automated Centralized Certificate Management System. [Online]. Available: https://asnet.am/services.php?art=SSL_Certificates&lang=en

[7] The Academic Scientific Research Computer Network of Armenia (ASNET-AM). [Online]. Available: http://www.asnet.am

[8] Let’s Encrypt Rate Limits. [Online]. Available: https://letsencrypt.org/docs/rate-limits/

[9] Advantages over Using Let's Encrypt – ZeroSSL. [Online]. Available: https://help.zerossl.com/hc/en-us/articles/17864245480093-Advantages-over-Using-Let-s-Encrypt

[10] A. Petrosyan, G. Petrosyan and R. Tadevosyan, “SSL Certificate Deployment Automation Concept for ASNET-AM Network Services”, *Proceedings of International Conference Computer Science and Information Technologies*, Yerevan, Armenia, pp. 228--229, 2019. [Online]. Available: https://csit.am/2019/proceedings/TN/TNp6.pdf

[11] A. Petrosyan, G. Petrosyan and R. Tadevosyan, Implementation of ACMEv2-based Automated Centralized Wildcard Certificates System", *Proceedings of International Conference Computer Science and Information Technologies*, Yerevan, Armenia, pp. 207--208, Yerevan, 2021. [Online]. Available: https://csit.am/2021/proceedings/TN/TN_4.pdf

[12] DNS-01 challenge. [Online]. Available: https://letsencrypt.org/docs/challenge-types/