Implementation of ACMEv2-based Automated Centralized Wildcard Certificates System

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

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

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

***Abstract*— This paper describes the implementation of Automated Centralized Wildcard Certificates System based on Automatic Certificate Management Environment (ACMEv2) protocol within the Academic Scientific Research Computer Network of Armenia (ASNET-AM). Digital certificates are one of the major instruments, used for most network services today. The work done in ASNET-AM is based on the availability of free LetsEncrypt wildcard SSL certificates. The concept of implementing centralized certificate server was presented at CSIT 2019 and this paper summarizes its implementation done during past years. The system described is now actively used in production and provides centralized secure and automated free digital certificates service for different types of network services such as web servers, mail servers, etc. in ASNET-AM.**

***Keywords*— Networking, Security, Digital Certificate, SSL, LetsEncrypt, Wildcard, ACME, Automation**

I. Introduction

During last several years, the Academic Scientific Research Computer Network of Armenia (ASNET-AM) [1] gave up the wide use of paid digital SSL Certificates, issued and signed by commercial Certificate Authorities (CA) for securing the network services and authenticating network servers.

Instead, the concept of implementing own automated centralized certificate server, based on the free LetsEncrypt [2] wildcard SSL certificates with use of Automatic Certificate Management Environment (ACMEv2) protocol was developed and implemented. As a result, the system described here is now actively used in production and provides centralized secure and automated free digital certificates service for different types of network services in ASNET-AM.

The Automated Centralized Wildcard Certificates System consists of central server part and simple client part, that can be installed at each network server, where the certificate should be delivered. Each client has the possibility to get several certificates from a central server. And a copy of the same wildcard certificate can be provided to several client servers. Renewal of digital certificates is done centrally for all certificates, and distribution of them is secured per-client server with SSH public-key.

II. Central Server Part

Central certificate server part is mainly based on Dehydrated Automation Script [3]. It does all the required steps to centrally request, get and renew the certificate. But first the DNS zone needs to be modified for Wildcard SSL certificates according to ACMEv2. So, the same central server runs a DNS service for centralized certificate server configuration to do the DNS-01 challenge [4] for each domain. Each domain or subdomain for which the wildcard SSL certificates is to be provided by the central server should have the "_acme-challenge.<domain>" zone delegation configured. Dehydrated and DNS zone delegation configuration is described in previous concept paper [5]. Additional automated cleanup to get rid of old unused certificate files is periodically scheduled at the central server.

Distribution of server certificates per-client is implemented by periodically scheduled local rsync process, which has configuration of corresponding client-certificate and places copies of requested certificates to the home directory of each client.

Such approach ensures both regular update of certificates centrally as well as target clients getting their copies in their home directories. Confirmation status of each process is sent by email to the predefined addresses after completion.

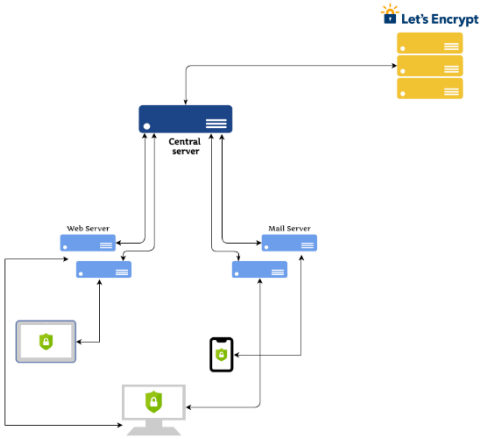
"Client" servers next can securely connect to the central server and fetch their separate certificate copies via remote rsync/ssh as described in the next section. None of the clients has access to other certificates than those specifically provided to each of them.

III. Client Part

Each network server (web server, mail server, etc.) can obtain multiple certificates from the central certificate server. Presence of "rsync" & "openssl" packages is required at the "client" server. Secure data transfer is done by rsync tool by means of ssh connection. Ssh keypair should be generated at "client" server with "ssh-keygen", and the public key of generated keypair should be provided for installation at the central certificate server under separate ssh user. Thus, each "client" server gets isolated copies of its certificates.

Detailed configuration of “client” server is presented in “Script to update certificate from central cert server” Github Wiki page [6].

The described Automated Centralized Wildcard Certificates System structure is presented in Picture 1.



Picture 1.

IV. Conclusion

Described implementation is working in production in ASNET-AM and provides centralized secure and automated free digital certificates service for multiple domains to different types of network services such as web servers, mail servers, etc.

SSL certificates are being centrally obtained and updated from Let’s Encrypt and then can be made securely and internally available at the centralized certificate server. Each “client” server can securely access the central certificate server to get and use the certificate it requires.

Such automated system allows provision and update SSL certificates on multiple servers from one centralized certificate server.

In case of ASNET-AM network services, this approach is highly effective, since it allows to use the same wildcard certificates to secure multiple services like, webhosting (HTTPS), Email (SMTPS/IMAPS/POP3S) and others.

Given the fact that several domains are in use at ASNET-AM, the automation of the process mentioned above increases the effectiveness of securing the network services.

References

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

[2] Let's Encrypt - free, automated and open CA https://en.wikipedia.org/wiki/Let%27s_Encrypt

[3] Dehydrated Automation Script - https://dehydrated.io

[4] DNS-01 challenge – https://letsencrypt.org/docs/challenge-types/

[5] SSL Certificate Deployment Automation Concept for ASNET-AM Network Services - Arthur Petrosyan, Gurgen Petrosyan, Robert Tadevosyan Proceedings of the Conference CSIT’2019, pp. 228-229, Yerevan, 23-27.09.2019 https://csit.am/2019/proceedings/TN/TNp6.pdf

[6] Script to update certificate from central cert server - https://github.com/arthur7373/dehydrated/wiki/Script-to-update-certificate-from-central-LECERT-server