Extended ACME Protocol with Time-Limited VC Tokens for Automated Organization Validation

Toi Ooka*, Taisho Sasada*, Ryosuke Abe†, Yuzo Taenaka*, Youki Kadobayashi*, and Shigeya Suzuki†

*Graduate School of Science and Technology, Nara Institute of Science and Technology, Nara, Japan
†Graduate School of Media and Governance, Keio University, Kanagawa, Japan
{ooka.toi.or2, yuzo, youki-k}@is.naist.jp, taisho.sasada@naist.ac.jp, chike@sfc.wide.ad.jp, shigeya@wide.ad.jp

***Abstract*—The Public Key Infrastructure (PKI) plays an essential role in securing Internet communications by enabling Certificate Authorities (CAs) to issue TLS certificates to web servers. These certificates enable browsers to authenticate web servers, though their expiration can disrupt website availability. To mitigate the problem, the Automated Certificate Management Environment (ACME) protocol automates certificate issuance and domain certification. However, Organization Validation (OV) certificate management is not automated because organization validation involves validating an organization's legal status and intent that are manually conducted, and are challenging to automate. This paper proposes an extended ACME protocol using Verifiable Credentials (VCs) to automate organization validation. VCs are digitally signed credentials issued by trusted authorities containing verifiable information, such as identity or educational qualifications. Reusing a previously issued VC for organization validation can pose significant risks by potentially enabling malicious actors to bypass the validation process. The proposed protocol solves this challenge by forcing a client requesting an OV certificate to obtain a short-lived VC after initiating the organization validation process, thereby limiting the reuse of VC and preventing unauthorized use. Our experimental results demonstrate that this protocol enhances security by preventing misuse of invalid VC while minimizing delays in certificate issuance.**

***Index Terms*—Public Key Infrastructure, ACME, OV certificate, Verifiable Credentials**

I. Introduction

Public Key Infrastructure (PKI) provides secure communication by issuing public key certificates through Certificate Authorities (CAs), which authenticate the identity of the certificate holder. On the web, Transport Layer Security (TLS) certificates are issued for web server domains, allowing browsers to verify server authenticity. This verification ensures that the browser is communicating with the web server it intends to communicate with. However, manually renewing TLS certificates introduces the risk of human error and places a significant burden on organizations managing many web servers. The Automated Certificate Management Environment (ACME) protocol [1] mitigates this burden by automating the verification of domain ownership and the issuance process of the TLS certificate. The ACME protocol automates the verification processes through communication between the CA's server and the client requesting a TLS certificate. The ACME protocol significantly reduces the risk of TLS certificate expiration.

Despite these advancements, the ACME protocol cannot automate the issuance of Organization Validation (OV) certificates, which verify the legal existence of an organization and its intent to apply for the issuance. Organization validation links the real-world domain-holding organization to its Internet domain. OV certificates are rarely used in phishing sites, and they often use Domain Validation (DV) certificates [2], which only verify domain ownership, are low-cost, and can be issued through an automated process. In other words, OV certificates are crucial for distinguishing phishing sites from legitimate ones. However, the authenticity of organization validation is guaranteed through manual verification of an organization's legal existence, involving document reviews and phone calls. These processes impose a significant burden on domain-holder organizations and CA. Automating this process can significantly reduce the manual workload and ease the burden of certificate management [3].

Verifiable Credentials (VCs) [4] offer a potential solution for automating organization validation and digitally verifying organizational information such as identification and registration status. VC uses public key and digital signature technologies to confirm the accuracy of data such as identification and business registry information. However, a VC only guarantees the correctness of data at a specific point in time when the digital signature is signed. To ensure the authenticity of organization validation, it is necessary to verify the validity of the VC at the time of organization validation. Like the TLS certificate, VC also uses digital signatures and public keys, indicating that a revocation status check is important for confirming the validity of VC. However, Smith et al. [5] pointed out that the high overhead of TLS certificate revocation checking can interrupt browser processes and web server responses, potentially slowing them down. Similarly, a revocation status check for VC can interrupt or delay the verification processes of both VC and organization validation. It means that revocation status checks can compromise the availability of organization validation. The challenge is that verifying the validity of VC through a revocation status check can compromise the availability of organization validation. However, ensuring the validity of VC is crucial to maintaining the reliability of the OV certificate issued through VC validation checks.

To achieve the automatic issuance of OV certificates, David et al. [6] have proposed a protocol that automates organization

validation using Verifiable Presentations (VPs). A VP is a package that combines data from one or more Verifiable Credentials (VCs) to be presented to a data verifier. In David et al.'s protocol, the client's public key is sent to third-party software, which creates a VP containing the client's public key. The authenticity of the VP is ensured by confirming that the creator of the VP is the client, specifically the legitimate owner of the client's public key. However, because the protocol does not validate VP validation status at the time of organization validation, it cannot guarantee the authenticity of organization validation. Even if the validity of a VP is guaranteed through revocation status checks, the validation process can impose a high overhead and can compromise the availability of the issuance system. Additionally, this protocol is at risk of exploitation by malicious third parties, who can obtain the client's public key and create a fraudulent VP containing it, potentially exploiting both domain certification and organization validation.

We propose a secure extended ACME protocol designed to guarantee the authenticity of organization validation without requiring complex and burdensome processing for revocation status checks. In the proposed protocol, the validity and authenticity of organization validation are ensured by using a VC token with two specific constraints. Unlike typical VC, this VC is called a 'token' due to its short validity period and the requirement that it is acquired synchronously during the organization validation process. The short validity period restriction prevents the use of previously issued or illegally obtained VC tokens, ensuring the validity of the tokens. Expired VC tokens are automatically invalidated, eliminating the need for revocation status checks and ensuring token validity. When the client synchronously acquires and presents the VC token to the server, it guarantees that the client has obtained the VC token at the time of the organization validation. This constraint confirms that the client is the legitimate holder of the VC token and verifies the authenticity of the token. By accepting only synchronously acquired VC tokens with a short validity period, we ensure the validity and authenticity of VC tokens and therefore guarantee the authenticity of organization validation. Moreover, because our protocol does not disclose the public key to third parties to verify the authenticity of the VC, malicious third parties cannot obtain the client's public key to create a VP containing it at any arbitrary time. This prevents the attacker from bypassing domain certification and organization validation. Even if a VC token leaks, the short validity period significantly limits the period for unauthorized use, making exploitation difficult.

II. Related Work

Thompson et al. [7] have surveyed the challenges associated with manual certificate issuance processes, highlighting the burden nature of manual verification. Their findings indicate that when the verification process for issuing certificates is conducted manually, it requires significantly more human resources. Furthermore, if errors occur during verification, additional time is needed, placing a considerable burden on the entities involved. To address this issue, Olamide et al. [3] have suggested that automating the issuance process is effective. The automation significantly reduces the need for manual work by system administrators, easing the burden of certificate management.

To establish automated OV certificate issuance, David et al. [6] have proposed a protocol called vp-01 challenge, which uses Verifiable Presentations (VPs) [4] to automate organization validation. In the vp-01 challenge, an ACME client (software requesting a certificate) sends its account's public key to a VC wallet (an application that manages user identity information). The VC wallet then creates and signs a VP containing the public key and the Verifiable Credential (VC). This mechanism proves that the VP is created specifically for a particular ACME client, establishing a link between the VP and the client's request, and ensuring the authenticity of the VP. The ACME server (the party issuing the certificate) can verify that the presented VP corresponds to the ACME account by confirming that the public key in the received VP matches the public key associated with the ACME account.

However, this protocol has two problems. Firstly, this protocol cannot guarantee the authenticity of organization validation, as it does not verify the validity of a VP at the time of organization validation. If a VP is invalid, it means that the organization validation is verified based on incorrect information, and the OV certificate issued through this protocol cannot be trusted by web browsers. Even if the validity of a VP is ensured by a revocation status check, the availability of the issuance system can still be compromised. As Smith et al. [5] have pointed out, although revocation status checks are necessary for validity verification, they impose a significant burden on the validity check process. Secondly, this protocol also presents the risk of compromising domain certification and organization validation. In the ACME protocol, the ACME client's public key is used to calculate the hash value required for domain certification. The public key is confidential information that should only be known to the ACME client and the ACME server. However, in David et al.'s protocol, this public key is passed to a VC wallet provided by a third party, which is trusted by the CA. The third-party can calculate the hash value of the public key and create a VP containing the public key at any time. Therefore, if the third party has malicious intent, they can compromise domain certification and organization validation.

III. Requirement Definition

Based on the challenges identified in related works, this study aims to establish a secure and automated organization validation process without compromising the availability of the issuance system. In order to achieve automated issuance of OV certificates, two key requirements must be met: automation of certificate issuance, domain certification, organization validation, and the authenticity assurance of the organization validation.

a) Automation of Certificate Issuance, Domain Certification and Organization Validation: Automation of certificate

issuance and domain certification, have been established by the ACME protocol [1]. However, automated organization validation has not yet been achieved. Automating organization validation is a necessary extension of the ACME protocol to enable the automated issuance of OV certificates. Legal Entity Verifiable Credentials (LE-VCs), which are organization credentials that can be automatically obtained and verified over the Internet, provide an effective means of automating organization validation.

b) Authenticity Assurance of Organization Validation: Ensuring the authenticity of organization validation is essential to maintain the trustworthiness of OV certificates. To guarantee this authenticity, the validity and authenticity of the LE-VC must be verified. The LE-VC must be trusted as valid by the CA to ensure its validity, and the ACME client must be recognized as the legitimate owner of the LE-VC to confirm its authenticity. Similar to TLS certificates, since VCs [4] use public keys and digital signatures, the LE-VC must have either a short validity period or a revocation status check mechanism to ensure its validity. Expiration naturally occurs when the certificate's specified valid period passes. Revocation, on the other hand, is the process of invalidating a certificate due to security issues or at the owner's request, even if it has not yet expired. As noted by Smith et al. [5], processing revocation confirmations can be burdensome, so authenticity should be guaranteed through a short validity period rather than revocation. In addition to the constraint of a short validity period, synchronous acquisition ensures the authenticity of the LE-VC. When the LE-VC is obtained synchronously, certification and authorization occur with the LE-VC issuer, confirming the organization's legitimacy at the time of validation. LE-VCs that meet these constraints are referred to as LE-VC tokens, and these constraints can be implemented as time-based constraints.

IV. Protocol Proposal

In this study, we propose a secure and extended ACME protocol that automates organization validation using an LE-VC token. Figure 1 illustrates the configuration of the proposed system, which includes three entities: the LE-VC Issuer, the Domain-Holder Organization, and the CA. The domain-holder organization is the client that obtains an OV certificate. First, the client acquires the LE-VC token from the issuer and presents it to the CA. The CA then performs domain certification and organization validation using the presented LE-VC token. After these verifications, the CA issues an OV certificate to the client. In the following subsections, we explain the specific processes of domain certification and organization validation required for OV certificate issuance.

A. Automatic issuance of OV certificates

We describe the requirements and implementation of the system, along with the flow of the verification for automated OV certificate issuance. First, the domain holder's ACME client requests an LE-VC token from the VC wallet after initiating organization validation (Figure 1 (1)). Then, the VC wallet requests an LE-VC token from the LE-VC Issuance

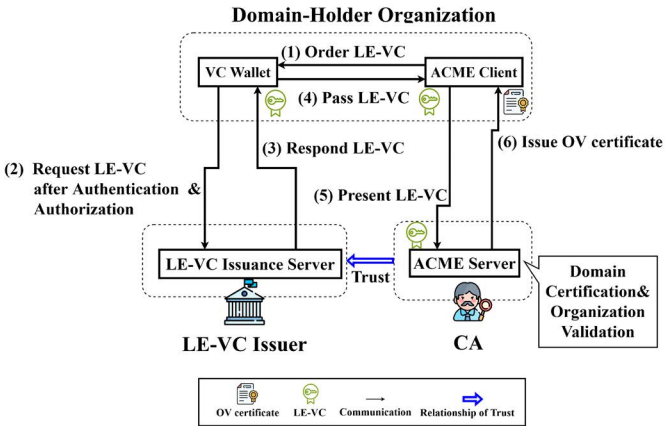

Fig. 1. System for automated OV certificate issuance

Server, and the server authenticates and authorizes the VC wallet to confirm that the client is legitimate (Figure 1 (2)). The LE-VC issuer issues the LE-VC token to the VC wallet (Figure 1 (3)), and the VC wallet passes the LE-VC token to the ACME client (Figure 1 (4)).

Next, the domain-holder organization presents the LE-VC token to the CA through the ACME client to initiate domain certification and organization validation (Figure 1 (5)). The CA completes the domain certification in the same manner as the ACME process and performs organization validation verifying the LE-VC token. For organization validation, the CA uses the public key of the LE-VC issuer to verify the digital signature and confirm that the data is guaranteed by the LE-VC issuer. Finally, the CA automatically issues the OV certificate using the ACME protocol.

The process of obtaining the LE-VC follows the OpenID for Verifiable Credentials Issuance (OID4VCI) [8] protocol, and the VC wallet can be the European Union Digital Identity Wallet (EUDIW) [9] or the Bifold Wallet [10] developed by the OpenWallet Foundation.

On the digital signature verification of the LE-VC token, the revocation status of the LE-VC issuer's public key is notified to the issuance system only in an emergency, like Google Chrome's CRLsets [11]. CA can verify a LE-VC token without checking revocation status at each verification, thus lowering the burden of the verification process.

B. ACME Protocol

The ACME protocol [1] automates domain certification and TLS certificate issuance. In the ACME protocol, all validation methods, including domain certification, are referred to as challenges. There are two domain certification challenges in ACME: HTTP-01 Challenge and DNS-01 Challenge. The HTTP-01 challenge involves the ACME server verifying domain ownership via the domain holder's web server. The DNS-01 challenge entails verification through the domain holder's DNS server.

Figure 2 illustrates the sequence diagram of the proposed protocol. In this section, we provide an overview of the common elements shared between the proposed protocol (LE-VC-01 Challenge) and the ACME protocol (Figure 2 (1), (2), (3), (4), (5), (8), (9), (10), (A), and (C)).

In Figure 2, the domain-holding organization carries out domain certification with the ACME server by using the ACME client's DNS server or web server. After proving domain ownership to the ACME server, the ACME client obtains a TLS certificate from the CA's ACME server. The CA in Figure 2 controls the ACME server and automatically issues TLS certificates.

a) Register for ACME Account: When an ACME client registers an account on the ACME server, it also registers the public key of the key pair (Figure 2 (a)) with the server. The requests (Figure 2 (1), (2), (3), (4), (8)) are signed with the private key of this key pair and sent to the ACME server, which verifies the signatures using the registered public key for authentication.

b) Start Issuance Process: First, the ACME client starts the process of issuing a TLS certificate. The ACME client requests the issuance of a new certificate (Figure 2 (1)). In response, the ACME server returns an Authz URL, which contains the status of the challenge (domain certification) and the challenge URL (Figure 2 (2)). The ACME client then requests the Authz URL (Figure 2 (3)) to obtain the challenge URL and token for domain certification. The ACME server responds with these details to the ACME client (Figure 2 (4)).

c) Prepare for Domain Certification: Next, the ACME client prepares for domain certification. It generates a key authentication message (Figure 2 (b)) by concatenating the token obtained from the Authz URL response (Figure 2 (4)) and the hash value of the public key. The ACME client sets the key authentication message on the DNS server or web server and instructs the server to publish it (Figure 2 (5), (A)). This completes the preparation for domain certification, and the ACME client notifies the ACME server that the preparation is complete (Figure 2 (8)).

d) Domain Certification: The ACME server requests the key authentication message from the DNS server or web server controlled by the ACME client (Figure 1 (9)). The server responds by presenting the key authentication message to the ACME server (Figure 1 (10)). The ACME server verifies the received key authentication message, confirms that the ACME client is the legitimate domain holder, and completes the domain certification (Figure 1 (C)).

C. LE-VC-01 challenge: Organization Validation Protocol

To automate organization validation in the proposed system, we introduce an organization validation protocol called the LE-VC-01 Challenge. This protocol is an extension of the ACME protocol. This section explains the organization validation flow, focusing on the changes and extensions made to the ACME protocol.

a) Certificate Issuance Request: The ACME client requests a new OV certificate from the ACME server to initiate the issuance process (Figure 2 (1)). The modifications from the standard ACME protocol include the Authz URL returning not only the Challenge URL but also details such as the start of the LE-VC-01 challenge, the format of the LE-VC token, the maximum validity period of the token, and the deadline for synchronous acceptance of the token.

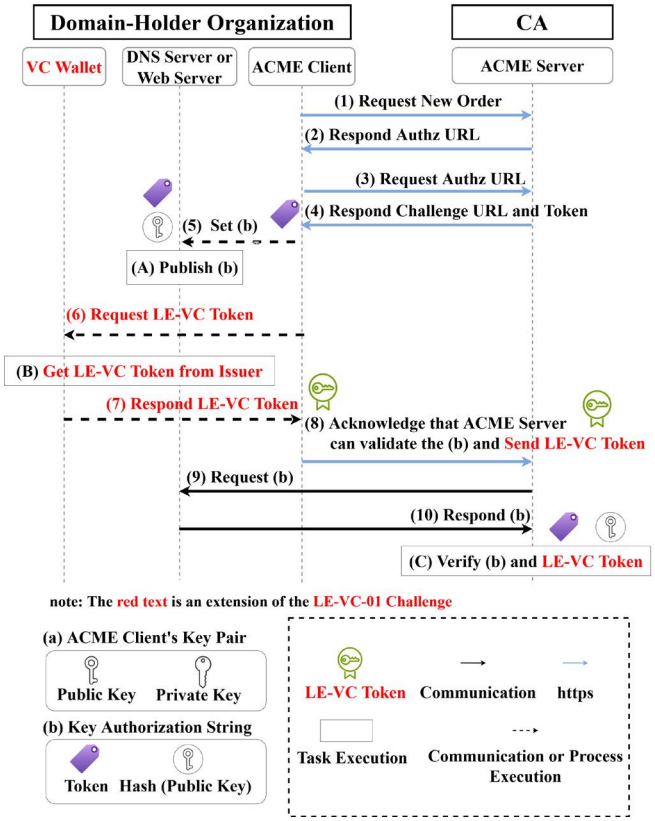

Fig. 2. Sequence diagram of ACME Extension Protocol

b) Preparing for Organization Validation: The ACME client prepares for organization validation in parallel with the preparation for domain certification. First, the VC wallet authenticates and authorizes the ACME client, and the ACME client requests the wallet to obtain the LE-VC token (Figure 2 (6)). In this request, the ACME client sends the format, the maximum validity period, and the deadline deadline for synchronous acceptance to the VC wallet to obtain an LE-VC token that meets these constraints. The VC wallet requests a new LE-VC token from the LE-VC issuer by sending the specified constraints. Based on these constraints, the LE-VC issuer issues an LE-VC token to the VC wallet (Figure 2 (B)). The VC wallet then passes the obtained LE-VC token to the ACME client. The fact that the LE-VC is newly issued ensures that it is created after the start of the LE-VC-01 challenge and is acquired synchronously. The ACME client presents the LE-VC token in its request for the domain certification challenge URL to the ACME server (Figure 2 (8)). The ACME client must complete the process of obtaining and presenting the LE-VC by the synchronous acceptance deadline.

c) Organization Validation: The ACME server confirms that the presented LE-VC token are valid, has a short validity period, are obtained synchronously, and ensures its validity and authenticity (Figure 2 (C)). Firstly, the ACME server checks that the public key of the LE-VC issuer is valid and verifies the digital signature. In this process, the server verifies the LE-VC token is issued by a trusted LE-VC issuer. The next step is to verify that the LE-VC complies with the constraints. The ACME server compares the current time with the validity

period of the LE-VC to confirm its validity. It then verifies that the LE-VC is obtained synchronously by checking that the issuance time of the LE-VC is after the start of the challenge and before the deadline for synchronous acceptance. The ACME server also checks the time interval between the issuance time and the expiration time of the LE-VC to confirm that the validity period is short. After these checks, the validity and authenticity of the LE-VC token are confirmed, and the organization validation is complete.

V. Evaluation

A. Security Evaluation

The threats to the ACME protocol are defined in RFC 8555 [1] as attacks targeting two channels: the communication between ACME clients and servers (ACME channel) and the communication for domain certification (validation channel). Bhargavan et al. [12] have conducted a formal security verification of the ACME protocol and have demonstrated that it is secure. Therefore, we conduct a security evaluation of the proposed protocol's extensions (LE-VC-01 Challenge) for both the ACME channel and the validation channel.

1) Attack against ACME Channel: RFC 8555 [1] identifies the risk of a man-in-the-middle (MITM) attack. If the CDN or reverse proxy used by the ACME server is compromised by an attacker, domain certification can be substituted by the victim's ACME client, posing a risk that TLS certificates can be fraudulently obtained by an attacker. In the context of the LE-VC-01 challenge, this attack can allow an attacker to steal the LE-VC token and obtain the victim's OV certificate. Under normal circumstances, communications over the ACME channel (Figure 2 (1), (2), (3), (4), and (8)) occur over https. The encryption provided by TLS and public key authentication prevent MITM attacks and ensure that attackers cannot steal the LE-VC token or obtain the OV certificate. However, if the ACME server side is compromised, an MITM attack cannot be prevented.

2) Attack against Validation Channel: One possible method for presenting the LE-VC token is to place it on a web or DNS server, concatenated with the key authentication message (Figure 2 (b)), and present it to the ACME server. In the case of the HTTP-01 challenge, the token for domain certification is included in the path. Only the ACME server that knows the token can access the message, ensuring that the LE-VC token remains secure and that organization validation is conducted securely. However, in the case of the DNS-01 challenge, the key authorization message is placed on the DNS server as a TXT record for the domain name (_acme-challenge.{domain name}), which is publicly accessible, allowing the LE-VC token to potentially leak and be stolen by an attacker. The DNS-01 challenge is required for issuing wildcard certificates, which are TLS certificates covering arbitrary subdomains. To address this, the LE-VC-01 challenge is designed to present the LE-VC token during communication (8) in Figure 2, extending organization validation to the ACME channel and separating it from the validation channel. Since the ACME channel uses https, the LE-VC token remains secure. However, because the LE-VC-01 challenge is conducted over the ACME channel, if the ACME server side is compromised, theft of the LE-VC token cannot be prevented.

In the verification process of LE-VC tokens, the ACME server checks that the validity period is short and that the tokens are obtained synchronously with data guaranteed by the issuer's digital signature. The issuance time of LE-VC tokens must be after the start of the LE-VC-01 challenge, the presentation time must be before the deadline for synchronous acceptance, and the validity period must be short. Therefore, any LE-VC token obtained before the start of the challenge by an attacker cannot be accepted. Additionally, because the LE-VC token obtained after the start of the challenge has a short validity period, it expires quickly, and any token submitted after the synchronous acceptance deadline is rejected, giving an attacker insufficient time to misuse it. However, if an attacker obtains the token within the time constraints, they can still succeed in compromising the organization validation.

B. Performance Evaluation

To evaluate the performance of the proposed protocol, we implemented the ACME protocol domain certification (HTTP-01 Challenge) and the proposed protocol (LE-VC-01 Challenge) and conducted experiments to measure the response time and processing time of the challenge validation processes. The ACME client and server were implemented using FastAPI, a web framework in Python. Specifically, we implemented the challenge notification acceptance API (Figure 2 (8)), the domain certification function (Figure 2 (9), (10)), and the LE-VC token verification function (Figure 2 (C)). The host machine used for the experimental environment was a laptop running Windows 10 OS with an Intel Core i7-8665U CPU and 16 GB of memory. We used Docker containers for the experimental setup, allocating one CPU core and 512 MB of memory for each ACME server and ACME client.

1) Response Time: The ACME client notifies the ACME server that it is ready for the challenge, and the ACME server returns an empty response while adding the challenge as a background task in FastAPI. The response times for the challenge notification (Figure 2 (8)) are shown in Figure 3 and Table I for individual validation and hybrid validation (HTTP-01 and LE-VC-01). We measured the response times and standard error from the same challenge start notification request sent 100 times per 1 second. In the cases of HTTP-01 and hybrid validation, the average response times were approximately 30 ms, while in the case of LE-VC-01, the time was approximately 2.5 ms. This difference occurs because the response time increases with the HTTP-01 challenge due to domain certification communications that occur after validation begins, whereas the LE-VC-01 challenge does not require additional communications. As a result, the LE-VC-01 challenge had a shorter response time than the HTTP-01 challenge. In summary, the LE-VC-01 challenge does not cause significant delays.

2) Validation Process Execution Time: The ACME server executes the domain certification (HTTP-01 challenge) and organization validation (LE-VC-01 challenge) separately. The

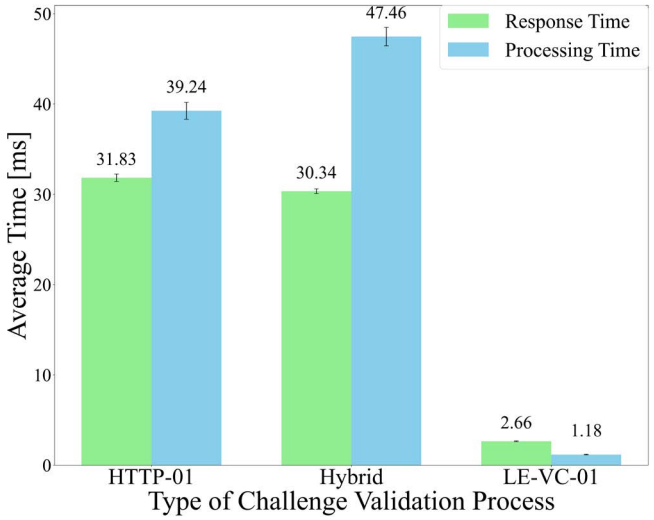

Fig. 3. Response and Processing Time Graph

TABLE I
RESPONSE AND PROCESSING TIME TABLE

Type of Processing	Response Time [ms]		Processing Time [ms]	
	Avg.	*Std Error*	*Avg.*	*Std Error*
HTTP-01	31.83	0.47	39.24	0.94
Hybrid	30.34	0.26	47.46	1.02
LE-VC-01	2.658	0.05	1.18	0.04

Note: Hybrid = HTTP-01 and LE-VC-01

processing times are shown in Figure 3 and Table I. The ACME server performed the validation process 100 times per 1 second. The HTTP-01 case took approximately 40 ms, and the hybrid case took approximately 45 ms. In contrast, the LE-VC-01 case took approximately 1 ms. This difference occurs because, in the validation process for domain certification (HTTP-01 challenge), the ACME server must communicate with the client's web server, whereas the LE-VC-01 challenge does not require any communication. From these measurements, we conclude that the delay in the validation processes due to the LE-VC-01 challenge is approximately 5 ms, which is minimal.

VI. DISCUSSION

A. Threat Model of LE-VC-01 Challenge

Government entities may pose a threat to PKI and the proposed protocol. For instance, the Kazakhstan government attempted to exploit PKI to intercept Internet communications in 2015, 2019, and 2020 [13]. In the proposed protocol, the government's role is limited to issuing the LE-VC token, which helps prevent PKI abuse. Additionally, the protocol avoids requiring CAs to request the revocation status from the issuer, mitigating the risk of government tracking LE-VC usage. However, governments can still issue LE-VCs for registered organizations and bypass organization validation. If a government compromises an organization's DNS or web server, it can obtain its OV certificate. To prevent this, LE-VC issuer transparency should be ensured by monitoring issuance logs, similar to the Certificate Transparency (CT) system [14].

B. Limitations of LE-VC-01 Challenge

The propose protocol has several limitations. First, if the time restrictions of the short validity period and synchronously obtaining of the LE-VC token were too strict, the ACME client could not meet the time restrictions due to the delay of networks and processing. On the other hand, soft restrictions of the LE-VC token may enhance the availability of the validation, however, it also diminish the authenticity of the organization validation.

VII. CONCLUSION

In this study, we propose a secure extended ACME protocol that guarantees the authenticity of organization validation. This is achieved by imposing a constraint that the LE-VC has a short validity period and is obtained synchronously, without requiring revocation status checks that can burden the proposed protocol. A security evaluation of the proposed protocol has demonstrated that it is secure. The performance evaluation revealed that it introduces no significant delay compared to existing ACME protocols. The proposed protocol will establish the automated issuance of OV certificates.

ACKNOWLEDGMENT

Part of this study was funded by the ICSCoE Core Human Resources Development Program and Japan Society for the Promotion of Science KAKENHI Grant Number JP24K03045, Japan.

REFERENCES

[1] R. Barnes, J. Hoffman-Andrews, D. McCarney, and J. Kasten, "Automatic Certificate Management Environment (ACME)," Mar. 2019.
[2] K. Hageman, E. Kidmose, R. R. Hansen, and J. M. Pedersen, "Can a TLS Certificate Be Phishy?," in *Proceedings of the 18th International Conference on Security and Cryptography*, pp. 38–49, SCITEPRESS Digital Library, 2021.
[3] O. Omolola, R. Roberts, M. I. Ashiq, T. Chung, D. Levin, and A. Mislove, "Measurement and Analysis of Automated Certificate Reissuance," in *Proceedings of the Passive and Active Measurement Conference 2022*, pp. 161–174, Springer, 2021.
[4] M. Sporny, D. Longley, D. Chadwick, and O. Steele, "Verifiable Credentials Data Model v2.0," March 2024.
[5] T. Smith, L. Dickinson, and K. Seamons, "Let's revoke: Scalable global certificate revocation," in *Network and Distributed Systems Security (NDSS) Symposium 2020*, 2020.
[6] D. A. C. Morales, A. S. Wazan, D. W. Chadwick, R. Laborde, A. R. R. Maramara, and K. Cabral, "Enhancing the ACME Protocol to Automate the Management of All X. 509 Web Certificates," in *Proceedings of the IFIP International Conference on ICT Systems Security and Privacy Protection*, pp. 265–278, Springer, 2023.
[7] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter, and A. P. Felt, "The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators," in *Proceedings of the 28th USENIX Security Symposium*, pp. 1715–1732, 2019.
[8] T. Lodderstedt, K. Yasuda, and T. Looker, "OpenID for Verifiable Credential Issuance - Draft 14," August 2024.
[9] The European Digital Identity Wallet Project, "European Digital Identity Wallet Architecture and Reference Framework ver 1.4," May 2024.
[10] Openwallet Foundation, "The Bifold Wallet," 2023. Last Accessed: 2024-10-13. Available from: https://github.com/openwallet-foundation/bifold-wallet.
[11] The Chromium Project, "CRLSets." Last Accessed: 2024-10-13. Available from: https://www.chromium.org/Home/chromium-security/crlsets/.
[12] K. Bhargavan, A. Bichhawat, Q. H. Do, P. Hosseyni, R. Küsters, G. Schmitz, and T. Würtele, "An In-Depth Symbolic Security Analysis of the ACME Standard," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2601–2617, 2021.
[13] I. Ristic, *Bulletproof TLS and PKI, Second Edition: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. Feisty Duck, 2022.
[14] B. Laurie, A. Langley, and E. Kasper, "Certificate Transparency." RFC 6962, June 2013.