EV Certificates through automation

Paul van Brouwershaven

CA/Browser Forum Server Certificate WG

February 1, 2024

ENTRUST

SECURING A WORLD IN MOTION

11.8.4. Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:

1. Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and
2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 11.8.3.

The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for:

i. authenticating the Certificate Approver when EV Certificate Requests are approved, ii. periodic re-confirmation of the EV Authority of the Certificate Approver, iii. secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and iv. such other appropriate precautions as are reasonably necessary.

API Keys

- An API key is directly linked to a Certificate Approver.
- The Certificate Approver has likely provided the API to a CLM system, Cloud Service Provider, or other system that will automate the requests, but **it will not use the API key as a human**.
- Each request from that API will be treated as originating of the Certificate Approver.

Does it matter who created the API key?

- The API key is **generated by the Certification Authority** and provided to the Certificate Approver, who provides it to a Cloud Service Provider.
- The API key is **generated by the Certificate Approver** and provided to both the Certification Authority and a Cloud Service Provider.
- The API key is **generated by the Cloud Service provider** and provided to the Certificate Approver who communicates with the Certification Authority to authorize that key on their behalf.

In the case of ACME auto discovery

- The Certificate Approver could download and authorize the ACME key from the **example.com** manual (i.e., authorizing a specific ACME public key), or;
  - Certificate Approver authorizes **example.com** to request EV certificates on their behalf.
  - The CA will authorize all ACME client keys for example.com by downloading them from:
    - https://example.com**/.well-known/acme/publickeys**.json

https://datatracker.ietf.org/doc/draft-vanbrouwershaven-acme-auto-discovery/

EVG: 11.8.1. Verification Requirements

11.8.1. Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

1. **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.
2. **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
3. **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:
4. A. Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and B. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and C. Approve EV Certificate Requests submitted by a Certificate Requester.

BR: 3.2.5 Validation of authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in Section 3.2.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

Thank You

Paul van Brouwershaven

paul.vanbrouwershaven@entrust.com

entrust.com

ENTRUST

SECURING A WORLD IN MOTION