Validation Working Group: Proposed Revisions to 3.2.2.4

Introduction

Current Baseline Requirements

For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN by:

Proposed Revision

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that the Fully-Qualified Domain Name (FQDN) has been validated by at least one of the methods below for each FQDN listed in a Certificate.

For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

Method: Applicant is Registrant

Current Baseline Requirements

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar;

Proposed Revision

1. Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Name Registrant directly with the Domain Name Registrar or Registry. This method may only be used if:

(a) The CA authenticates:

(1) the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, or

(2) the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; or

(b) The CA is also the Domain Name Registrar or Registry, or Affiliate of the Registrar or Registry, and directly confirms that the Applicant is the Domain Name Registrant; or

Definitions

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN starts with a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For gTLDs, the domain www.[gTLD] will be considered to be a Base Domain.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Method: Written Challenge

Current Baseline Requirements

2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;

3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;

Proposed Revision

2. Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar.

Each email, fax, SMS, or postal mail MAY confirm control of multiple FQDNs.

Each email, fax, SMS, or postal mail SHALL be sent to one or more recipients provided that every recipient SHALL be identified by the Domain Registrar as representing the Registrant for every Domain Name within whose Domain Namespace every FQDN falls.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail, however the email, fax, SMS, or postal mail MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation; or

Method: Telephonic Challenge

Current Baseline Requirements

2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar;

3. Communicating directly with the Domain Name Registrant using the contact information listed in the WHOIS record's "registrant", "technical", or "administrative" field;

Proposed Revision

3. Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number. The call must be placed to a phone number identified by either the Domain Name Registry or Domain Name Registrar as the contact information for the Domain Name registrant, Domain Name technical contact, or Domain Name administrative contact. Such identification MAY be made by consulting WHOIS information provided by the Domain Name Registry or Domain Name Registrar.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registry or Registrar as a valid contact method for every Domain Name within whose Domain Namespace every FQDN falls.

Method: Role Email Challenge

Current Baseline Requirements

4. Communicating with the Domain's administrator using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;

Proposed Revision

4. Confirming the Applicant's control over the requested FQDN by sending an email to an address created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, including a Random Value and receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs.

Each email SHALL be sent to one or more recipients provided that every recipient SHALL be identified as an administrator for each Domain Name within whose Domain Namespace every FQDN falls.

The Random Value SHALL be unique in each email, however the email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation; or

Method: Domain Authorization Document

Current Baseline Requirements

5. Relying upon a Domain Authorization Document;

Proposed Revision

5. Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from either the Domain Name Registrant (including any private, anonymous, or proxy registration service) or the Domain Name Registrar listed in the WHOIS. The CA MUST verify that the Domain Authorization Document was either (i) dated on or after the date of the domain validation request or (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space; or

Definitions

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

The derivation of the Request Token SHALL incorporate the key used in the certificate request.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

E.g.: A Request Token could be:

i) a SHA-256 hash of the public key;
ii) a SHA-256 hash of a CSR, provided that the CSR itself is signed with SHA-2 (or better);
iii) a SHA-384 hash over a concatenation of the Subject Public Key Info and the FQDN being validated; or
iv) a SHA-256 hash over a concatenation of the Subject Public Key Info and a sorted list of all of the FQDNs being validated for this certificate request.

Authorized Port: One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

Method: Content Accessed via HTTP

Current Baseline Requirements

6. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN; or

Proposed Revision

6. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token (contained in the name of the file, the content of a file, on a web page in the form of a meta tag, or any other format as determined by the CA) under "/.well-known/pki-validation" directory on the Authorization Domain Name that can be validated over an Authorized Port.

Either:

a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or

b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or

c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control; or

Method: Any other

Current Baseline Requirements

7. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described.

Proposed Revision

<removed>

New Method: DNS

7. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS TXT or CAA record for an Authorization Domain Name.

Either:

a) a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Certificate Request and SHALL remain valid for no longer than 30 days, or

b) where the Applicant submits certificate requests directly to the CA, a Random Value SHALL be used in this demonstration of control which SHALL be unique to the Applicant and which SHALL remain valid for no longer than the maximum time specified in section 3.3.1, or

c) where the Applicant submits certificate requests other than directly to the CA, e.g. when the Applicant is communicating with the CA through an intermediary party not audited to be in compliance with these guidelines such as a reseller or a web-host, a Request Token SHALL be used in this demonstration of control

[time limited? Whether a Request Token should be required to carry a time stamp?].

New Method: IP Control

8. Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5; or

Definition

Test Certificate: A Certificate which includes data that renders the Certificate unusable for use by an application software vendor or publicly trusted TLS server such as the inclusion of a critical extension that is not recognized by any known application software vendor or a certificate issued under a root certificate not subject to these Requirements.

[Tighter definition needed – critical extension always? Based on pre-certificate definition?]

The Applicant must prove possession of the private key corresponding to the public key in the Test Certificate.

New Method: Test Certificate

9. Confirming the Applicant's control over the requested FQDN by confirming the presence on the FQDN of a Test Certificate (using the same public key) issued by the CA for the purposes of this method and which is accessible by the CA via TLS over an Authorized Port.

[Whether a test certificate should have a specific time limit?]

Open Issue: IETF ACME Spec

IETF is working on Automated Certificate Management Environment specification. It defines several methods. The working group does not have ACME expertise and is looking to someone from the ACME WG to contribute methods to this ballot.