Review of Domain Validation Methods

General clean-up comments applicable to many methods

1. We shouldn't need to state that the random number can be used for up to 30 days in each validation method that uses Random Number. We also don’t need to say this each time: CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS. The definition of random number should include this information
    a. I actually had a draft ballot that did some of this, but it didn’t get much support. Would be happy to resurrect it -Tim
2. When we use the defined term Domain Contact, we must be sure that we mean to include all 3 forms of contact and not just Who-is/RDP
3. Including “Notes” in each validation method are non binding and may cause more confusion that they are attempting to address. Recommend removing all “Notes” and including important requirements from the notes elsewhere
4. Be clear and consistent that a user requests the validation of a FQDN, validation is performed on an ADN (most cases) and it’s the ADN that can be reused. Thus if you validated "subdomain.example.com" as the ADN, that only authorizes labels at-or-below subdomain.example.com in the DNS hierarchy, and not for domains with 'fewer' labels.
5. Be clear and consistent on the applicability to support issuance of wildcard domains

Method 1:

1. Better specify requirements to require an exact match - company name + address + jurisdiction + registration number
2. Don’t allow affiliate relationship between Domain Registrant and Applicant (applies to all methods)
3. Require EV (or similar) level validation of authorization (3.2.5)
4. Only use for Org validation

[will be replaced by strong, new methods]

Risk	Mitigation	Discussion

Method 2 - Email, Fax, SMS, or Postal Mail to Domain Contact :

Current BR Text:

> 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 as a Domain Contact.
>
> Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.
>
> The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.
>
> The Random Value SHALL be unique in each email, fax, SMS, or postal mail.
>
> The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.
>
> The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.
>
> Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	Mitigation	Discussion

Recommended Updates

1. Separate freshness value from secret value (applies to multiple methods)
2. DONE: Add RDAP to definitions - done, added to definition of Who-is
3. This method permits sending an email to Domain Contacts, but later it says that the value must be provided by the Domain Name Registrar. Since “Domain Contact’ permits the use of SOA records, is that intentionally not included? If so, then maybe we should change the Domain Contact definition to not include SOA records.
4. Remove “Note” paragraph

Recommended new method

Method 3 - Phone Contact with Domain Contact:

Current BR Text:

> Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.
>
> 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 Registrar as a valid contact method for every Base Domain Name being verified using the phone call.
>
> Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	Mitigation	Discussion
This is more of a limitation than a risk, but using only the Domain Name Registrant’s phone number is overly restrictive.	Change “Domain Name Registrant” to “Domain Contact”	We should allow the phone call to be placed to a Domain Contact (includes the registrant).
It’s not clear how phone transfers should be handled, and this weakness could be	Prohibit transfers except to a specified Domain Contact. The CA must ask to be	Consider not allowing any transfers except to the Domain Contact, otherwise

exploited.	transferred to them by the supplied name. The Name could be a name or the name of a department, but regardless, that “name” has been identified as the Domain Name Contact.	“anyone” could approve the domain.
It’s not clear how voicemail messages can be used (or not) with this method.	If voicemail is reached, allow a Random Value to be left. The Applicant can convey this back to the CA within 30 days to approve the domain	
While the Applicant is asking for a FQDN to be validated, the validation is actually being done for the Authorization Domain Name.	Recommend changing: ...confirming the Applicant's request for validation of the ADN ~~FQDN~~	
Does the “note” provide any value, or should this be deleted .	TBD	
What can be re-used for future requests from this Applicant, FQDN or ADN?		

Recommended Updates

1. The phone call and response should confirm the validation of the Base Domain Name, not the FQDN.
2. There is an inconsistency between Domain Name Registrant and Domain Contact, so we should say the call can be made to a “Domain Contact” vs. “Domain Name Registrant”.
3. Don’t permit phone transfers except to a Domain Contact.
4. If voicemail is reached, allow Random Number to be left. It must be returned to the CA within 30 days.
5. Each phone call MAY confirm control of multiple Authorization Domain Names.
6. Should we remove the note? TBD

Recommended new method

Confirm the Applicant's control over the FQDN by calling the ~~Domain Name Registrant's~~ Domain Contact’s phone number and receiving a confirming response to validate the Authorization Domain Name ~~obtaining a response confirming the Applicant's request for~~

~~validation of the FQDN~~. The CA MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call ~~SHALL be made to a single number and~~ MAY confirm control of multiple ~~FQDNs~~ ADNs, provided that the phone number is identified by the Domain Registrar as a valid contact ~~method~~ phone number for every ~~FQDN~~ ADN being verified ~~using the phone call~~.

In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the Authorization Domain Name being validated. The Domain Contact may return the Random Number to the CA via Phone, Email, Fax, or SMS to approve the request within 30 days of the voicemail.

Method 4 - Constructed Email to Domain Contact :

Current Ballot Text:

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

The Random Value SHALL be unique in each email.

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. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	Mitigation	Discussion
admin@ and administrator@ are not reserved email addresses in RFC2142, so they may not be protected	Update RFC 2142	RFC is 20 years old so it's unlikely it could be updated, and even if it was, it's unlikely that this would ripple down
	Remove them from the BRs	These are often used by Microsoft based servers, so removing them could have an impact on the use of this method.
		Consider not permitting use of this method for Wildcard certificates. Could someone describe the risk?
Email addresses may not be for a Domain Contact	Email addresses should be explicitly provided by a trusted source similar to Method 2. Proposed new method c would allow an email address to be specified through DNS or on a /.wellknown/page..	These email addresses are not provided by the Domain Registrant, nor the DNS admin. Why do we think a response from these email addresses should be trusted? (from Bruce)
Title of "Constructed Email to Domain Contact" may be misleading or incorrect	Recommend changing the title of this method "Method 4 - Constructed Email"	"Domain Contact" is a defined term, and a constructed email address is not a "Domain Contact"

Recommended Updates

- Do we have any recommendations for an updated Method 4?
    - How about ending with "This method IS NOT suitable for validating Wildcard Domain Names" :-)
-

Recommended new method

Method 5 -Domain Authorization Document :

1. Do not resurrect for domain validation; consider for Org validation / EV, but regardless, this does not need to remain in section 3.2.2.4

[Not worth analyzing]

Method 6 - Agreed-Upon Change to Website

Current Ballot Text

Confirming the Applicant's control over the FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Request Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	**Mitigation**	**Discussion**
Underspecified location for random value	Specify the exact locations permissible.	Consider listing the current locations and removing “or another path registered with IANA for the purpose of Domain Validation”
Global redirects can be used to approve certificates without the domain owners knowledge	Forbid following redirects when performing domain validation.	If someone has access to the location of the redirect, then they can approve certificates for all domains being redirected there. Following server side redirects may end up at a CA page where the CA can simply provide the random number for all sites that redirect. Globally placed re-directs are especially concerning.
Unlike DNS, demonstrating control for example.com does not mean you necessarily control www.example.com, so users may be able to obtain certificates for subdomains for which they are not authorized.	Limit validation to the FQDN being included in the certificate and not permit ADN to be used.	Could CAA be used to signal permission to use this method for subdomains? This would be extremely disruptive
For the same reason, the use of this method to support issuance of wildcards is a risk.		
On shared IP address	Consider the use of ALPN which	

environments, the use of SNI can permit certificate issuance for domains on the shared IP address if the Hosting provider does not separate users	notifies CA that the hosting provider has taken steps to separate customers that share IP addresses.	
On shared IP address environments, the use of Host Headers (http) can be abused if the hosting provider does not separate control of the host names between customers	Does anyone have a suggested mitigation? Require CAs to use SNI when doing HTTP validation?	This is the same issue as previously identified in methods 9 and 10?
The use of query strings can be used to ...		What are the risks, can someone describe them? Ryan, can you provide your input here?
May be susceptible to “Cross protocol attacks”		What are the risks, can someone describe them? Ryan, can you provide your input here?
Caching might introduce risk. What are the risks and mitigations for caching results?	Require CAs to use “Cache-Control: no-cache” ? Or do nothing?	What are the risks, can someone describe them? Ryan, can you provide your input here?
HTTP response code is not a 2xx or 3xx	Require success response code for validations	Error status from the Web server indicates that the response should not be trusted

Method 6 Support for Following Redirects

Type	Subtype	Description	Security Properties	Recommendation
Server-side	300 multiple choices	e.g. offer different languages		Allow?
	301 moved permanently	redirects permanently from one URL to another passing		Allow?

		link equity to the redirected page		
	302 found	originally "temporary redirect" in HTTP/1.0 and popularly used for CGI scripts; superseded by 303 and 307 in HTTP/1.1 but preserved for backward compatibility		Allow?
	303 see other	forces a GET request to the new URL even if original request was POST		Allow?
	307 temporary redirect	provides a new URL for the browser to resubmit a GET or POST request		Allow?
	308 permanent redirect	provides a new URL for the browser to resubmit a GET or POST request		Allow?
	HSTS	HSTS header sent in response to an HTTPS request	Should CAs be expected to respect HSTS caching rules and/or obey an HSTS preload list?	Allow?
Client-side	meta refresh	HTML tag		Tim: requires a HTML parser

				inside validation code
	JavaScript	window.location	Would require CA clients to execute scripts on the page.	Tim: requires a JavaScript parser inside validation code

Other considerations:

- What if the URL being redirected to is malformed or uses a scheme like file:// or ftp://
    - Limit to HTTP and HTTPS
- What if the redirect is a downgrade from HTTPS to HTTP? To a different port (e.g. :8080)?
    - Assume redirects between http and https are acceptable
    - Assume that any “Authorized Port” is useable
- What if there are multiple Location headers causing the redirection to be indeterminate?
    - No discussion
- Should CAs be required to comply with Content Security Policy directives such as upgrade-insecure-requests sent from the server?
    - No discussion

Recommended Updates

1. Forbid CAs from following client-side redirects when validating
2. Specify the exact locations
    a. .well-known/pki-validation/
    b. .well-known/acme-challenge/
3. Require that the response be successful
4. Limit of 1 redirect (probably more, ACME supports 10)
5. Limit redirection to ‘http:’ and ‘https:’
6. Should we allow redirects to different ports?
    a. Assume yes, to any Authorized Port

Recommended new method

Confirming the Applicant's control over the FQDN by performing the following:

1.

confirming one of the following under the "/.well-known/pki-validation" or the “.well-known/acme-challenge/” directory, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content is contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file~~ or web page~~, or

2. The presence of the Request Token or Request Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

Processing redirects:

1. The CA MUST NOT follow client-side redirects.
2. Redirects MUST be limited to http and https
3. Redirects MUST to be an Authorized Port (or MUST NOT be to a different port?)
4. CAs MUST NOT follow more than one redirect

The HTTP response must be successful, meaning that no 2xx or 4xx response codes must be accepted

<insert more new check here>

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Method 7 - DNS Change :

Current Ballot Text

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either
1) an Authorization Domain Name; or
2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after
(i) 30 days or
(ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	Mitigation	Discussion
Scope underscore prefix to prevent misuse.	Define the Prefix exactly rather than leave it unspecified. The recommended value is: "_pki-validation"	Since a DNS admin cannot restrict permissions to generic underscore names, they can't restrict certificate issuance. By specifying an exact value, the DNS admin can restrict permissions.
Are there any other Risks we need to discuss?		If none, then we should proceed to ballot this change. ● Do we make this a new Validation Method, or edit this one? ● Effective date will depend on input from those CAs that currently use underscores.

Recommended Updates

1. Mandate the use of "_pki-validation" as the label.

Recommended new method

Change this:

> 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

To this:

> 2) an Authorization Domain Name that is prefixed with the label " _pki-validation".

Method 8 - IP Address :

Current Ballot Text

> Confirming the Applicant's control over the 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.
>
> **Note**: Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

Potential Risks

1. Remove 'any other method'
    a. Agreed, 3.2.2.5 needs to have Any Other Method removed
2. Scope "containing an IP" to just being the authority
3. Obtain contact info from RIR —>validate/contact using 3.2.2.4.2/3
4. ISP can get cert without hijacking
5. Scope of Domain Name in #3
6. 3.2.2.4.8 not reference 3.2.2.5 or specify certain methods in 3.2.2.5
7. Scope validation to FQDN (verify)
8. Consider an opt-in mechanism like .9/.10
9. Should it be possible to get certificates for a.b.c.d.in-addr.arpa?

Risk	Mitigation	Discussion

3.2.2.5 is underspecified and needs to be updated.	See discussion later in this document addressing updates to 3.2.2.5	

Recommended Updates

Recommended new method

Method 9 - Use of a test certificate:

Current Ballot Text

> Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.
>
> Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Potential Risks

Risk	**Mitigation**	**Discussion**
When using SNI to request the certificate, users in shared IP address environments may be able to perform domain	1) Interim: receive confirmation from hosting providers that they have sufficient SNI separation	

validation for the domains of other users on that IP address. Hosting providers that permit shared IP addresses across customers must prevent SNI use between customers	and use IP address whitelisting to enable those customers 2) Final: Use ALPN and only those that have the applicable ALPN in place can use this method	
When SNI is not used when obtaining the Test Certificate, then are the mitigations identified above required.	The use of SNI should be mandatory for this method.	In the scenario where the TLS server is an Apache, etc. instance, not using SNI may mean that an arbitrary (such as the first defined) virtual host's certificate chain will be presented. This means that an attacker who is able to control the certificate configuration for the first virtual host can obtain certificates for ALL domains that resolve to that server's IP address. To mitigate this, I think we should require that SNI be used.

Validation steps

1. When the CA obtains the SSL test certificate, the CA should require server-based opt-in (ALPN)
2. The test certificate must contain the FQDN being validated
3. Consider scoping validation to a single FQDN per validation (one FQDN per test certificate and per domain validation)

Recommended Updates

- Make the use of SNI mandatory
- Make the use of ALPN mandatory

Recommended new method

Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by the CA on the Authorization Domain Name and which is accessible by the CA:

- via TLS
- over an Authorized Port
- using SNI
- using an ALPN challenge with the value of "cabf-tls/1"

If successful, this validation can be used to issue a Certificate with the same Public Key as in the Test Certificate.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Method 10 - TLS Using a Random Number:

Risk	Mitigation	Discussion
If: ● Many users are hosted on the same IP address, and ● Users have the ability to upload certificates for arbitrary names without proving domain control. Then, an attack is possible	Require server-based opt-in (ALPN). See this spec.	Letting the web hoster make such an important "claim" as it relates to domain validation doesn't completely eliminate the risk. All web hosters could simply support ALPN without actually separating users on shared IP addresses. Even thought this helps reduce the risk, there is residual risk.

1. Remove existing methods 9 and 10
2. Require server-based opt-in (ALPN)
3. Describe method in more detail
4. Add Random Value reuse requirements (break out from specific methods)
5. Consider scoping validation to specific FQDN

Method 12:

1. Safely allow non-affiliate relationships via new method, then;
2. Remove Affiliates
3. Add transparency

Method (new): Registrar Challenge Validation (proposed by Peter)

Proposed text:

Confirming the Applicant's control over the request Domain Name by confirming the presence of a Random Value or Request Token in a response from the Domain Name Registrar or Registry received in response to a request containing an Authorization Domain Name."

Note: We may want to be a bit more specific than just ‘in response to a request’

Risk	Mitigation	Discussion

Method a: (tls-alpn replacement for Method 10)

FIXME: add more details and analyze, Roland.

Method b: Using recently issued certificate to reset the domain validation re-use period:

1. When a new certificate is issued, the CA may verify that this certificate is accessible at a FQDN, then the CA may set the current domain validation date to this date/time for each of the FQDNs the CA verifies. The issuance of the certificate must be in compliance with the BRs and this simply updates the domain validation date
2. This method requires the same mitigations as Methods 9 and 10.

Method c: Authorization Email to Domain Contact

Proposed text:

> Confirm the Applicant’s control over the FQDN by sending an email with a random value to an Authorization Email Address. The Authorization Email Address may be provided through
>
> 1. DNS CNAME
> 2. TXT
> 3. CAA record OR
> 4. under a “/.wellknown/pki-validation/ directory
>
> This method will mitigate the issue of not finding email addresses per Method 2 or using unreliable email addresses through Method 4.
>
> This method is explicit as the email address is provided by a by a DNS admin or by a person that controls the website.

[Note: I am not sure about CAA record as I am not sure where the data would be provided. I included CAA record as this was allowed for Method 7.]

Risk	Mitigation	Discussion
Use of DNS CNAME record to store email addresses might not be technically possible	Remove this as an option	Since CNAME records contain Domain Names, it does not seem practical or possible to insert an Email address in this record type.
Since TXT records have no format, it's possible that existing entries could enable issuance without the knowledge of the Domain Admin	The best mitigation is to use a CAA record instead, but if TXT records are to be used, then they need to have a specific, well defined format.	If we must use TXT records over CAA records, then they must have a semantically meaningful format to disambiguate between multiple methods that may wish to allow email addresses in TXT records
CAA records are well suited for signaling domain owners issuance preferences, however not all		

Method d: DNS Domain Validation Website Change

In some cases the Method 6 website change cannot be done on a production website, so another site would be required. This method would allow an alternative Authorization Domain Name to be stated in a DNS TXT or CAA record. This change could be implemented by just updating the definition of Authorization Domain Name to include DNS TXT and CAA record.

This method is explicit as the Authorization Domain Name is provided by a DNS admin.

[Note: I am not sure about CAA record as I am not sure where the data would be provided. I included CAA record as this was allowed for Method 7.]

Method e: Compliant Issuance without Validation

Several of the current methods allow issuance without validating that the Applicant owns or controls anything at all. These methods are popular in the ACME community, as they allow frictionless automatic issuance. However, the security requirements are seriously underspecified, if they can even be made to work.

Example:

1. Applicant reads CA's instructions, and sets WHOIS email to autovalidate@certificatesforeveryone.org

2. Applicant applies for a certificate
3. CA sends random value to autovalidate@certificatesforeveryone.org
4. CA, who controls that address, automatically enters the value on a confirmation website
5. Domain is validated
6. CA issues certificate to Applicant
7. Applicant installs certificate on system
8. Ninety days later, Applicant's system applies for a renewed certificate
9. CA sends random value to autovalidate@certificatesforeveryone.org
10. CA, who controls that address, automatically enters the value on a confirmation website
11. Domain is validated
12. CA issues certificate to Applicant's system
13. Ryan S. Evil applies for a certificate
14. CA sends random value to autovalidate@certificatesforeveryone.org
15. CA, who controls that address, automatically enters the value on a confirmation website
16. Domain is validated
17. CA issues certificate to Ryan S. Evil

A similarly horrible validation method can be constructed with method 6 via CNAMEs.

Method f: Validation methods using the _subdomain

Standardize a well-known subdomain?
Other implications?

Summary

Method	**Freshness or Secret**	**FQDN or ADN**	**Wildcard**	**Possible changes?**
1 Applicant as Domain Contact	N/A	ADN	Yes	Re-define as Method 13
2 Challenge to Domain Contact	Secret	ADN	Yes	
3 Phone call	Secret	ADN	Yes	
4 Constructed email	Secret	ADN	Yes	Discussing moving to FQDN ~~and No wildcard~~
5 DAD	N/A	ADN	Yes	
6 Website change	Freshness	ADN	Yes	Discussing moving to FQDN and No wildcard

7 DNS	Freshness	ADN	Yes	
8 IP address	Freshness	FQDN	No	
9 Test Certificate	Freshness	ADN	Yes	
10 TLS with Random No.	Freshness			
a)				
b)				
c)				
d)				
e)				
f)				

Review of IP Address Validation Methods

Current Ballot Text

For each IP Address listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;
2. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4; or
4. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described.

Note: IP Addresses may be listed in Subscriber Certificates using IPAddress in the subjectAltName extension or in Subordinate CA Certificates via IPAddress in permittedSubtrees within the Name Constraints extension.

Update approach

Break out each supported IP address validation method in a separate section

Add new defined terms:

IP Address Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry such as RIPE, APNIC, ARIN, AfriNIC and LACNIC

IP Address Contact: Contacts listed as the owners or registered contacts for IP addresses received from IP Address Authority.

Replace section 3.2.2.5 in its entirety with the following

3.2.2.5 Authentication for an IP Address

Effective January 31, 2019, all new IP Address validation must be performed in accordance with this section. Effective January 31, 2020, all IP Addresses included in issued certificates must comply with this section.

For each IP Address listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant has ownership or control over the IP Address by:

3.2.2.5.1 Agreed-upon Change for IP Address Validation

Confirming the Applicant's control over the IP address by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate (such as in Section 4.2.1 of these Guidelines).

3.2.2.5.2 Validating the Applicant is the IP Address Owner

The CA SHALL confirm the Applicant’s control over an IP Address by obtaining documentation of IP address assignment to the Applicant directly from an IP Address Authority. A CA MAY NOT use this method unless the CA validates (i) the Applicant's identity under BR Section 3.2.2.1 and (ii) the authority of the Applicant Representative under BR Section 3.2.5.

3.2.2.5.3 Email, Fax, SMS, or Postal Mail to IP Address Contact

Confirming the Applicant's control over the IP Address 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 as an IP Address Contact.

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

The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient shares the same IP Address Contact information for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

3.2.2.5.4 Phone Contact with IP address Contact

Confirming the Applicant's control over the IP address by calling the IP Address Contact's phone number and obtain a confirming response to validate the IP Address.

Each phone call MAY confirm control of multiple IP Addresses provided that the same IP Address Contact phone number is listed for each IP Address being verified and they provide a confirming response for each IP address or IP address range.

In the event that someone other than a IP Address Contact is reached, the CA MAY request to be transferred to the IP Address Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the IP Address(es) being validated. The IP Address Contact may return the Random Number to the CA via Phone, Email, Fax, or SMS to approve the request within 30 days of the voicemail.

3.2.2.5.5 Reverse Address Lookup

The CA SHALL verify the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the Domain Name using a method permitted under Section 3.2.2.4.

3.2.2.5.6 Delegated Control Over a Device

The CA SHALL verify the Applicant’s control over an IP Address by 1) the CA accessing a device located at the requested IP Address, 2) the CA authenticating to the device using credentials provided by the Applicant or created by the CA, and 3) the CA adding a Request Token or Random Value to a file on the device at a location determined by the CA.

Other Topics

Random Number Freshness vs. Secret Value

In some cases we need secret values (email validation) and in other cases we need Freshness. We need to review how they are used and specify additional requirements (for example, maybe secret values should have a shorter usage period than freshness values)

Use of CAA to enable certain Domain Validation Methods or Options

CAA has been identified as a means to help domain owners control or limit validation methods and options. Should we list out the various proposals and discuss how they can be used to reduce risk?

Current usage:

1. Issue - permits issuance of standard and wildcard certificates from the specified CA
2. issueWild - permits issuance of wildcard certificates only from the specified CA

Possible future usage:

1.

ACME TLS-SNI-03

Even thought this RFC is not completed, we should start on defining a new Domain Validation method that would allow this to be used. The current method 10 is underspecified.

Principles for Evaluating Validation Methods

1. Explicit agreement from owner or registrant
2. Control of WHOIS/registrant information
    a. wildcard/subdomain ok
3. Control of DNS
    a. wildcard/subdomain ok
4. Control of the server at the address