SECTIGO

Sectigo Reseller Validation Guidelines

The guidelines listed herein are the essential validation procedures for members of Sectigo's Reseller program. All Resellers MUST follow these procedures when verifying certificate details.

These guidelines apply to all certificates requested by a Reseller account and are in conformance with Sectigo's Certificate Practice Statement as amended ("CPS") and the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates. Sectigo may update its CPS and these guidelines, and any amendments must be promptly incorporated into each Resellers validation process. Resellers must check these guidelines often to ensure that their validation procedures match the latest requirements. Updated guidelines are effective upon the earliest of their receipt by the Reseller or by their posting on the Reseller's account. A Reseller failing to follow the validation processes described herein, including any update may have their account privileges suspended or revoked.

Contents

Certificate Validation Overview

The listed validation procedures must be followed for the listed certificate types. Details of each validation step are provided below. Resellers are responsible for knowing what validation is required for each certificate and for performing the appropriate validation based on the certificate desired.

Domain Validated ("DV") Certificates.

Certificate brands: *Sectigo SSL, Essential SSL, PositiveSSL, OptimumSSL, LiteSSL, MDCs*
Before requesting ("DV") certificates, a Reseller must:

1. Require the applicant to execute a Subscriber Agreement governing the use of the certificate and
2. Perform Domain Control Verification (DCV) through Sectigo's servers via one of the following means:
    a. Email sent to WHOIS contact or one of 5 accepted generic administrator type addresses
    b. HTTP CSR Hash method
    c. DNS CNAME CSR Hash method

Details regarding these methods can be found in *Appendix B - DCV - Alternative Mechanisms*

Each Fully Qualified Domain Name (FQDN) listed in an MDC must undergo Domain Control Verification prior to issuance of the MDC.

High Assurance, or Organization Validated ("OV") Certificates

Certificate brands: *InstantSSL, PremiumSSL, EliteSSL, GoldSSL, PlatinumSSL, UCC*
Before requesting high assurance certificates, Resellers must:

1. Require the applicant to execute the applicable Subscriber Agreement prior to requesting the certificate,
2. Perform Domain Control Verification (DCV) through Sectigo's servers via one of the following means:
    a. Email sent to WHOIS contact or one of 5 accepted generic administrator type addresses
    b. HTTP CSR Hash method
    c. DNS CNAME CSR Hash method

Details regarding these methods can be found in *Appendix B - DCV - Alternative Mechanisms*

3. Validate the identity of the applicant.

Each domain listed in a UCC must be validated prior to issuance of the UCC.

Email Certificates

Before requesting an email certificate, Resellers must validate the applicant's access to the email address listed in the certificate by sending the listed email address an activation email.

Custom Client Certificates

Custom client certificates should be validated in a commercially reasonable way depending on the intended use of the certificate. Resellers desiring custom client certificates must work with Sectigo to receive approval on how validation will be performed. The approved validation process established must then be followed prior to requesting the custom client certificates.

Code Signing and Time Stamping Certificates

Code signing and time stamping certificates are only available to Resellers specifically requiring such services. Resellers interested in Code Signing and Time Stamping certificates should contact Sectigo for additional information.

Validation Details

Subscriber Agreement

Each customer must execute a subscriber agreement that governs the use of the certificate. Sectigo's subscriber agreements for its certificates are listed on the Sectigo repository which is located at http://www.Sectigo.com/repository. Subscriber agreements may be executed either electronically or in writing in conformance with local laws. Any customer refusing or failing to execute a subscriber agreement may not be issued a certificate. The posted subscriber agreements are subject to change by Sectigo without notice. Any changes are effective immediately upon their posting to the Sectigo repository.

Resellers may sign the subscriber agreement on behalf of their existing customers if the Reseller has a valid agreement, which has been approved by Sectigo and that grants the Reseller the express authority to 1) apply for, purchase, accept, install, maintain and renew a certificate for the customer's use and 2) bind the customer to the relevant subscriber agreement and procure the customer's compliance with the subscriber agreement. Auditable justification of the Reseller's authority to sign on its customer's behalf must be retained in accordance with the Record Retention and Periodic Audits guidelines below, and be presented to Sectigo upon request.

Domain Validation

Although Resellers tend to have a pre-established or contractual relationship with their customers that allows for the issuance of SSL Certificates, further validation of certificate applicants is required prior to actually providing the certificate. A Sectigo Reseller must use reasonable validation strategies to establish the applicant's ownership or control of the domain name listed in the certificate. Reasonable validation strategies MUST include using Sectigo's DCV system

Identity Validation

Resellers must conform with the requirement for the Verification of Subject Identity Information contained in Section 11.2 of the CA/Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.0:*

Data Source Accuracy

Before relying on a data source to verify Subject Identity Information, the Reseller SHALL evaluate the data source's accuracy and reliability. The Reseller SHALL NOT use a data source to verify Subject Identity Information if the Reseller's evaluation determines that the data source is not reasonably accurate or reliable. All data sources are subject to additional review by Sectigo which shall have final right of determination as to its acceptability.

Reliable Method of Communication

A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Applicant is an Organization

If the Subject Identity Information is to include the name or address of an organization, the Reseller SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The Reseller SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated, which the Reseller has evaluated in accordance with Section C)(1) Data Source Accuracy above;
3. A site visit by the Reseller; or
4. An Attestation Letter.

The Reseller MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the Reseller MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification listed in Appendix A.

*See Appendix A - Accepted Business Documentation for additional examples of acceptable documents by country

Applicant is using a DBA/Tradename:

If the Subject Identity Information is to include a DBA or tradename, the Reseller SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. Documentation or communication provided by a third party source that meets the requirements of Section 11.6;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support that meets the requirements of Section 11.6; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Section 11.6.

Applicant is an Individual:

If an Applicant subject is a natural person, then the Reseller SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

1. The Reseller SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The Reseller SHALL inspect the copy for any indication of alteration or falsification.

2. The Reseller SHALL verify the Applicant's address using a form of identification that meets Section Error! Reference source not found., such as a government ID, utility bill, or bank or credit card statement. The Reseller MAY rely on the same government-issued ID that was used to verify the Applicant's name.

3. The Reseller SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

Upon receipt of the above documentation, the Reseller must verify that the documentation information matches the information provided during the application process.

Code Signing Validation

Prior to requesting a code signing certificate a Reseller MUST:

1. Obtain a properly executed Subscriber Agreement; and

2. Perform Identity Validation as per Section C above; and

3. Perform Domain Validation as per B above, based upon the domain of the email address of the applicant, i.e., applicant email is someone@domain.com. The WHOIS record must show that domain.com is owned by the certificate applicant; and

4. The Reseller MUST call the certificate applicant at a verified phone number. Phone numbers can be verified through reliable third party online databases, or by having the applicant submit a phone bill showing applicant name, address and phone number.

5. Code signing certificates MAY NOT be issued to International Business Corporations or companies incorporated and/or domiciled in Panama, Bolivia or the British Virgin Islands without Sectigo's prior written authorization.

Verify the Authenticity of the Request

For all SSL certificates which are to contain organization information and all Code Signing certificates, the Reseller MUST verify that the Applicant Representative is an employee, or authorized agent of the Applicant Organization. The Reseller must contact the Applicant Organization via a Reliable Method of Communication, such as postal mail, or by telephone call to a phone number which has been verified by a reliable 3rd party. Examples include Dunn & Bradstreet (www.dnb.com), or a verified legal opinion or accountant letter. Phone call should verify that you are reaching the Applicant Organization, verify the authenticity of the certificate request, and verify the contact information of the Applicant Representative. Once the contact information and authority of the Applicant Representative have been verified in this manner, future requests may be verified directly with the Applicant Representative.

Record Retention and Periodic Audits

Resellers must record in detail every action taken to validate an application and to request a Certificate. This includes all information generated or received in connection with the validation of the certificate. These records must be retained for a period of not less than 7 years. Sectigo will perform audits against a randomly selected sample of certificates that a Reseller requests. Resellers are obligated to make their records related to the issuance of certificates open and available to Sectigo in a timely fashion and upon request. If Sectigo determines that a Reseller has failed to follow these guidelines in requesting certificates, Sectigo may suspend or revoke your account, suspend or revoke your certificates, and may charge the Reseller for the cost of the audit.

Trustworthiness and Competence of Validation Staff

Identity and Background Verification

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the Reseller, the Reseller SHALL verify the identity and trustworthiness of such person and keep such documentation as is necessary to confirm to Sectigo, Ltd. that these checks have been made. Evidence of this information will be required at the time of audit by Sectigo, Ltd.

Training and Skill Level

The Reseller SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

The Reseller SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

Validation Specialists engaged in Certificate verification SHALL maintain skill levels consistent with the Reseller's training and performance programs.

The Reseller SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The Reseller SHALL require all Validation Specialists to pass an examination provided by the Reseller on the information verification requirements outlined in these Requirements.

Questions

Should you have any question regarding any application or would like assistance with the validation process, please contact:

partnervalidation@Sectigo.com

Appendix A - Accepted Business Documentation

Accepted Documentation (Country Specific):

Country	Documentation	AKA	Notes
AIA	Articles of Incorporation		
AIA	Certificate of Incorporation		
ARG	Articles of Incorporation/Registration	El reglamento de Constitución de sociedad anónima/Matrícula	A translation of all documentation should be provided, if not already in English
ARG	Business Licence	La Licencia comercial	A translation of all documentation should be provided, if not already in English
AUS	Certificate of Registration of a Company		
AUS	Certificate of Registration of Business Name		
AUS	Certificate of Registration on Change of Name		
AUS	Copy of ASIC Registration		
BEL	Articles of Incorporation/Registration	Les articles d'Incorporation/d'Enregistrement	A translation of all documentation should be provided, if not already in English
BLZ	Certificate of		

	Incorporation		
BLZ	Certificate of Incumbency		
BRA	Copy of the Social Contract	Copia de contrato social	A translation of all documentation should be provided, if not already in English
BRA	National Business Registration Card	Cartao de Cadastro Nacional Da Pessoa Juridica	A translation of all documentation should be provided, if not already in English
CAN	Annual Declaration from the General Inspector of Financial Institutions	Declaration Annuelle de Inspectur general des institutions financieres.	A translation of all documentation should be provided, if not already in English
CAN	Business License		
CAN	Certificate of Incorporation	Certificat de constitution	A translation of all documentation should be provided, if not already in English
CAN	Certificate of Registration		
CAN	Vendor Permit	Permis de vendeur	A translation of all documentation should be provided, if not already in English
CHE	Articles of Incorporation		
CHE	Business License		
CHE	Extract from the Registry of Commerce	Extrait du Journal de la Registre du Commerce	A translation of all documentation should be provided, if not already in English

CZE	Business License	Vypis z obchodniho rejstriku, vedeneho Karjskym obchodnim soudem v Praze	A translation of all documentation should be provided, if not already in English
DEU	Certificate of trade index entry	Handelsregister	A translation of all documentation should be provided, if not already in English
DEU	Copy of Business Certificate	Gewerbeschein	A translation of all documentation should be provided, if not already in English
DEU	District Court Copy of Articles of Incorporation	Amstgericht kopie des Handelsregistereintrag im Handelsregister	A translation of all documentation should be provided, if not already in English
DEU	Official letter from the Federal bureau for finances	Bundesamt fur Finanzen	A translation of all documentation should be provided, if not already in English
DNK	Certificate of Incorporation	Sammenskrevet Resume	A translation of all documentation should be provided, if not already in English
FIN	Extract from the Register of Companies	Ote Kaupparekisterista	A translation of all documentation should be provided, if not already in English
FRA	Business Licence	Registre de Commerce	A translation of all documentation should be provided, if not already in English

FRA	Extracts from the register of commerce and societies.	Extrait du registre du commerce et des societes	A translation of all documentation should be provided, if not already in English
GBR	Articles of Association		
GBR	Articles of Incorporation/Registration		
GBR	Certificate of Incorporation on Change of Name		
GBR	Non Domestic Rating Notice		
GBR	Office of Fair Trading Standard Licence/Renewal		
GBR	VAT Certificate		
GRC	Certificate of Start Up of a Personal Enterprise		A translation of all documentation should be provided, if not already in English
GRC	Extract from the Business Registry of Athens		A translation of all documentation should be provided, if not already in English
IND	Certificate of Commencement of Business		A translation of all documentation should be provided, if not already in English
IND	Certificate of Incorporation		A translation of all documentation should be provided, if not already in English

IRL	Certificate of Incorporation		
IRL	Companies Registration Office certificate of Company Name Registration		
ISL	Certificate of Incorporation from Icelandic Register of Enterprises		A translation of all documentation should be provided, if not already in English
ISR	Custom & VAT Department: Certificate and License for Trading		A translation of all documentation should be provided, if not already in English
ISR	Ministry of Justice: Certification of an Incorporation of Company		A translation of all documentation should be provided, if not already in English
ITA	Proof of Existence of a Company released by the Chamber of Commerce in Italy	Visura Camerale	A translation of all documentation should be provided, if not already in English
JPN	Business Licence		A translation of all documentation should be provided, if not already in English
JPN	Seal Certificate		A translation of all documentation should be provided, if not already in English
MEX	Copy of Entry in the Federal Registration of	Inscripcion en el Registro Federak de Contribuyentes	A translation of all documentation should be provided, if not already in

	Contributors		English
MEX	Company creation bill		A translation of all documentation should be provided, if not already in English
MEX	Mexican business license		A translation of all documentation should be provided, if not already in English
MEX	Mexican IRS card		A translation of all documentation should be provided, if not already in English
MEX	Cheque with company name		A translation of all documentation should be provided, if not already in English
MEX	Back accounts		A translation of all documentation should be provided, if not already in English
MEX	Passport or licence of the legal guardian of the company		A translation of all documentation should be provided, if not already in English
MLT	Certificate of Compliance		
NLD	Articles of Incorporation/Registration	Artikelen van Onderneming/Inschrijving	A translation of all documentation should be provided, if not already in English
NLD	Extract from the Commercial Register of	Kamer Van Koophandel,	A translation of all documentation should be

	the Chamber of Commerce and Industries for Amsterdam	Amsterdam	provided, if not already in English
NOR	Business Registration Certificate	Bronnoysundregistrene	A translation of all documentation should be provided, if not already in English
NZL	Certificate of Incorporation		
PAL	Letter from Chamber of Commerce & Industry		A translation of all documentation should be provided, if not already in English
PHL	Articles of Incorporation/Registration		A translation of all documentation should be provided, if not already in English
POL	Certificate of Registration in the Register of Economic Activities.	Ewidecji Dzialalnoscu Gospodanczej	A translation of all documentation should be provided, if not already in English
POL	Documentation from Department of Treasury	Urzad Skarbowy	A translation of all documentation should be provided, if not already in English
POL	REGON - Certificate of registration in the National Official Register of the Nationalised Industries Units	Krajowy Rejestr Urzedowy Podmiotow Gospodarki Marodowej	A translation of all documentation should be provided, if not already in English
PRI	Business Registration Certificate	Registro de Corp	

PRT	Collective Person Identification Card	Cartão de Identificação De Pessoa Colectiva	A translation of all documentation should be provided, if not already in English
SWE	Article of Incorporation		A translation of all documentation should be provided, if not already in English
SWE	Letter of Incorporation		A translation of all documentation should be provided, if not already in English
SWE	Patent Registration Documentation		A translation of all documentation should be provided, if not already in English
TUR	Certificate of Good Standing from Chamber of Commerce	Ticaret Odasi, Faaliyet Belgesi	A translation of all documentation should be provided, if not already in English
TUR	Company Signatory List	Imza	A translation of all documentation should be provided, if not already in English
TUR	Extract from Companies Gazeteer	Sicil Gazetesi	A translation of all documentation should be provided, if not already in English

TUR	Tax Form	Vergi Levhasi	A translation of all documentation should be provided, if not already in English
TUR	Turkish Id	Turkiye Cumhuriyeti Nufus Cuzdani	A translation of all documentation should be provided, if not already in English
UAE	Professional Licence		A translation of all documentation should be provided, if not already in English
USA	Sales & Use Tax Permit		
USA	Business License/Certificate		
USA	Business Registration Certificate		
USA	Certificate of Acceptance of Appointment by Resident Agent		
USA	Certificate of Assumed Business Name		
USA	Certificate of Authority		
USA	Certificate of Change of Resident Agent and/or Location of Registered Office		
USA	Certificate of Exempt Status		
USA	Certificate of Existence with Status in Good		

	Standing		
USA	Certificate of Formation		
USA	Certificate of Incorporation		
USA	Certificate of Ownership for Unincorporated Business or Profession		
USA	Certificate of Payment of Business Tax		
USA	Certificate of Withholding Identification Number		
USA	Certificate/Articles of Amendment		
USA	Certificate/Articles of Organisation		
USA	Corporate Charter		
USA	Corporation Annual Report		
USA	Corporation Estimated Tax Form		
USA	Declaration of Proprietorship or Partnership Registration		
USA	Employer Identification Number Application		
USA	Fictitious Business Name Statement		
USA	Filing endorsement		

USA	Filing receipt		
USA	General Excise Tax License		
USA	Merchant's Certificate of Registration		
USA	Notary Public Identification Card		
USA	Occupational Tax Certificate/Licence		
USA	Organization Action in Writing of Incorporation		
USA	Privilege License		
USA	Public Records Filing for a New Business Entity		
USA	Restatement and Revision of Partnership Agreement		
USA	Sellers Permit		
USA	Statement of Partnership Agreement		
USA	Trade Name Registration Form		
USA	Trade Name Renewal Form		
USA	Transaction Privilege Tax License		
USA	Zoning Permit		
ZAF	Amended Founding Statement		

ZAF	Certificate of change of name of company	Sertifikaat van verandering van naam van maatskappy	A translation of all documentation should be provided, if not already in English
ZAF	Certificate of Incorporation	Sertifikaat van Inlywing	A translation of all documentation should be provided, if not already in English
ZAF	Founding Statement		

Australia: ABN and CAN

Other accepted business documentation:

- Trading License (Must be further verified directly with the Registration Authority)
- Copy of a utility bill (Acceptable for verification of address, but not existence of the organization)
- A bank statement (They may block out their Bank Account Details) (Acceptable for verification of address, but not existence of the organization)
- DUNs number
- Companies House Number

Appendix B Domain Control Validation

Introduction

All Sectigo server certificates must have DCV (Domain Control Validation) performed on them. DCV is a way to prove some level of control of a registered domain name. DCV can be performed using any one of three methods:

- Email challenge-response
- Creation of a file on the domain's HTTP server
- Creation of a DNS CNAME record for that domain

Email Challenge-Response

This is the default method used for Sectigo certificate orders.

When the order is placed, an email address is selected from a shortlist of acceptable options. An email is sent to that address, containing a unique validation code. The email should be received by someone in control of the domain, where they can follow a link provided in the email and enter the validation code, thus proving domain control.

The list of acceptable email addresses for any given domain is:

- admin@
- administrator@
- hostmaster@
- postmaster@
- webmaster@
- Any email address that appears on the domain's WHOIS record, and is visible to our CA system.

Using via web-interface

The web-interface certificate request process will default to offering email challenge-response DCV. The list of acceptable email addresses will be displayed for selection, based on the common name extracted from the CSR.

Using via API

Once the CSR is received from the customer, the FQDN of the common name (CN) from the CSR must be extracted. The DecodeCSR API can be used, or any other method you have available. The FQDN must then be passed to the GetDCVEmailAddressList API, which will return a complete list ofacceptable email addresses for that FQDN. ONLY email addresses returned from GetDCVEmailAddressList are acceptable. If an email address believed to be on the WHOIS record for the domain is not returned, this means our system was unable to extract it from a WHOIS query, and thus the address cannot be used.

Once a choice is made from the acceptable email address list that address can be passed to the AutoApplySSL API, as the dcvEmailAddress parameter. Once the call is made to AutoApplySSL with this parameter, the DCV email will be sent.

Due to our caching of the WHOIS record result, the API call to AutoApplySSL must be made within 24 hours of the GetDCVEmailAddressList API call.

A call to GetDCVEmailAddressList is not required if the dcvEmailAddress selection is from the 5 ‘default’ email addresses (i.e. not one extracted from the domains WHOIS record).

For multi-domain certificates, please see the information in **Notes** below.

HTTP Based DCV

HTTP based DCV requires that a HTTP server be running on port 80 of the FQDN requested as the commonname of the certificate.

Two hashes of the CSR are generated before submission to Sectigo. A simple text file is created on the HTTP server of the FQDN, with one hash as the filename, and one hash within the text file itself. Additionally a domainname is added to the text file, for expansion with future domain validation mechanisms.

For example:

A CSR is generated with the CN=www.example.com

The DER encoded CSR is hashed using both the MD5 and SHA-1 hashing algorithms.

A text file is created, containing the SHA-1 hash and the domain 'Sectigoca.com' on the next line.

c7fbc2039e400c8ef74129ec7db1842c

Sectigoca.com

The file is then named in the format: <MD5 hash>.txt and placed in the root of the HTTP server, like so:

http://www.example.com/C7FBC2039E400C8EF74129EC7DB1842C.txt

Note: The MD5 hash MUST use all capital letters as above in the naming of the text file.

Once the order is received by Sectigo and the HTTP based DCV is specified, the Sectigo system checks for the presence of the text file, and it's content. If the file is found and the hash values match, domain control is proven.

Using via web-interface

The hash values are calculated and presented via the web-interface during the order process. They are on the same screen as the DCV email-address options.

Both the MDC5 and SHA-1 hash values of the CSR are shown, and must be saved to the file served from your HTTP server as above before continuing with the order.

Using via API

The hashes are generated from the CSR before the order is submitted to Sectigo. The hashes MUST be generated from the DER encoded (i.e. binary) version of the CSR – NOT the base64 PEM encoded version. Variations in the PEM encoding can cause differing hash values, whereas the hashes of the DER encoded version will remain constant.

The file must be created using the UPPERCASE formatting of the MD5 hash, as most HTTP servers are case-sensitive. The Sectigo system will only look for the uppercase hash filename.

The file must be created with a .txt extension.

The SHA-1 hash within the file is case-insensitive.

The Sectigo system will look for the file at both the FQDN provided in the CSR, as well as the 'base' registered domain name. Thus in the above example, the CA system will check for the file at 'www.example.com', and if the file is not found, it will also check 'example.com'.

Note: For DCV on MDC or UCC certificates the Sectigo system will look for the file ONLY on the FQDN, thus if there are multiple sub-domains the text file must be uploaded to each of them.

When the AutoApplySSL call is made, an additional optional parameter must be specified to indicate use of HTTP based DCV. This parameter is called 'dcvMethod' and must be set to the value (uppercase) 'HTTP_CSR_HASH'.

For multi-domain certificates, please see the information in Notes below.

DNS CNAME Based DCV

DNS based DCV requires the creation of a unique CNAME record, pointed back to Sectigo.

Two hashes of the CSR are generated before submission to Sectigo.

A CNAME DNS record is created under the FQDN that the certificate is requested for, in the format:

<MD5 hash>.FQDN CNAME <SHA-1 hash>.Sectigoca.com

For example, a certificate is requested for the FQDN www.example.com. The CSR has the hashes:

MD5: c7fbc2039e400c8ef74129ec7db1842c

SHA-1: 298a056d3e2f3018bda514defb18129dc5af459e

To perform DNS CNAME based DCV, the following DNS CNAME record must be created before submitting the order:

c7fbc2039e400c8ef74129ec7db1842c.www.example.com CNAME

298a056d3e2f3018bda514defb18129dc5af459e.Sectigoca.com

Then the request is submitted to Sectigo, the presence of this CNAME DNS record is checked, and if found, domain control is proven.

Using via web-interface

The hash values are calculated and presented via the web-interface during the order process. They are on the same screen as the DCV email-address options. Both the MDC5 and SHA-1 hash values of the CSR are shown, and must be added to DNS as a CNAME record as the above instructions show before continuing with the order.

Using via API

The hashes are generated from the CSR before the order is submitted to Sectigo. The hashes MUST be generated from the DER-encoded (i.e. binary) version of the CSR – not the base64 PEM encoded version. Variations in the PEM encoding can cause differing hash values, whereas the hashes of the DER encoded version will remain constant.

The DNS CNAME record is then created in the format above.

The Sectigo system will look for the file at both the FQDN provided in the CSR, as well as the 'base' registered domain name. Thus in the above example, the CA system will check for the CNAME record at 'www.example.com',and if the record is not found, it will also check 'example.com'.

Note: For DCV on MDC or UCC certificates the Sectigo system will look for the file ONLY on the FQDN, thus if there are multiple sub-domains the text file must be uploaded to each of them.

When the AutoApplySSL call is made, an additional optional parameter must be specified to indicate use of HTTP based DCV. This parameter is called 'dcvMethod' and must be set to the value (uppercase) 'CNAME_CSR_HASH'.

For multi-domain certificates, please see the information in Notes below.

Notes

All certificate types (single, wildcard, MDC) can be validated with any of the three available DCV mechanisms. Multi-domain certificates can use a combination of any of the mechanisms for all FQDNs in the request.

Re-issuing

Re-issues of the certificates will require re-validation unless the re-issue is within 7 days of the original validation. We now allow the re-issue to not require revalidation of already -validated FQDNs IF the same private key is used to generate the CSR for re-issue. If a new private key is used to generate the CSR, then the order must have DCV re-performed by one of the available methods for all FQDNs in the request before the certificate can be issued. This will also apply to re-issues that facilitate the addition or removal of domains for multi-domain certificates.

Re-sending DCV Emails

DCV emails can be resent from within the web-interface, or via the API 'ResendDCVEmail'.

This will resend the DCV email for single-certificate orders, and for multi-domain certificate orders all outstanding (i.e. unvalidated) FQDNs the emails will be resent.

Multi-domain certificates

Multi-domain certificates (MDCs, UCCs) now require DCV for all orders. Any of the available mechanisms (email, HTTP and DNS CNAME) can be used. The web-based interface for this is provided once the order is placed. Simply login to your account and locate the order.

You will be presented with a screen that allows for selection of any valid email address to validate each FQDN in the certificate. Our system will run WHOIS lookups for all domains to provide the email addresses scraped from those records where possible. You can use the 'Refresh' button to update the data on screen – large numbers of FQDNs in a single certificate will take some time for all WHOIS records to be read. The web interface can also be used to choose the HTTP or DNS CNAME mechanisms for each FQDN.

You can also remove some FQDNs from the certificate if they are unable to be validated, and issue the certificate with only the domains validated to that point.

Multi-domain certificate API Details

The API can be used to request and validate multi-domain certificates via email-based DCV.

The changes to the existing API and processes for ordering are:

- Instead of the 'dcvEmailAddress' parameter, there is now a 'dcvEmailAddresses' (note the plural) parameter.

- This parameter accepts a list of email addresses to use for DCV. There must be one email address per FQDN in the 'domainNames' parameter, and they must be in exactly the same order.

Unlike single certificate orders via the API, our system will not reject orders because of incorrect DCV email addresses. They will be accepted, but no email will be sent. They can then be edited via the webinterface.

It is important to pass only valid email addresses for the DCV email address for each domainName.

Valid email addresses can be obtained by either using one of the default 5 (listed earlier in this document), or by calling the GetDCVEmailAddressList API for that domain.

It is also possible for you to perform and independent WHOIS lookup and send an email you can extract from the output to our API. However, please note that our system can only ‘see’ email addresses on a WHOIS lookup that is from the command-line. Email addresses visible from web-based WHOIS queries, or any that require human challenge-response systems (e.g. CAPTCHAS) will not be usable by our system, and the order will sit awaiting verification until you login and update the DCV email address via the web-interface.

Our system will attempt to send as few emails as possible. Where several FQDNs exist within the same registered domain name, one email will be sent.

The API can also be used to validate domains using the HTTP and DNS CNAME mechanisms. As above, the ‘dcvEmailAddresses’ parameter should be used. For each domain in the ‘domainNames’ parameter, in order, you can specify one of the following:

- A DCV email address as detailed in this document.

- The value ‘HTTPCSRHASH’ – and for this ‘domainName’ the HTTP DCV mechanism will be used.

- The value ‘CNAMECSRHASH’ – and for this ‘domainName’ the DNS CNAME DCV mechanism will be used.

In addition, if you wish to have all the domains validated by one of the alternative (HTTP or DNS CNAME) mechanisms, then simply pass a single value for the 'dcvEmailAddresses' parameter of:

- ALLHTTPCSRHASH, or;

- ALLCNAMECSRHASH

This should be the only value passed for the parameter, and will attempt to verify all domains via the same mechanism.

Multi-Domain Extended Status

The 'CollectSSL' API offers extended status for multi-domain certificates, showing all the requested FQDNs on an order, and the current DCV status of each.

Calling the 'CollectSSL' API with the correct authentication details, order ID and an additional parameter: 'showMDCDomainDetails' with the value 'Y' will provide this information in response to a status query.