Website Security Solutions | Symantec

AUTHENTICATION GUIDE

TABLE OF CONTENTS

Introduction 3
Certificate Types 4
Authentication Matrix 5
U.S. Government Denied Lists 6
Organization Authentication 7-8
- Jurisdiction
- Proof of Right with examples

Domain Authentication 9-10
- "WHOIS"
- Domain Requirements
- Alternative Methods of Approval

Organizational Unit Review/ Confirmation of Operational Existence 11
Address Verification 12
Third Party Telephone Number 13-14
Contact Requirements 15
EV Employment Confirmation & Authority 16
Verification Call/Acknowledgement Agreement 17-18
Domain Validated Certificates 19
Symantec Safe Site 20
Professional Opinion Letter 21
Best Practices 22
Partner Resources 23
Contact Information 24

INTRODUCTION

At Symantec, we are relentless in driving innovation and technology that protects the world's information in today's ever-changing threat landscape. As a part of driving innovation, authentication is a crucial part of our portfolio.

Symantec has driven and adopted the Certification Authority and Browser Forum Baseline Requirements to further strengthen the security around SSL operations and authentication processes for greater protection and trust in online transactions. The CA/B Forum Baseline Requirements, which help minimize risk and increase user confidence and trust, raise all CAs to a higher level of standards and authentication security.

Our established authentication and verification procedures help merchants grow their online businesses, inspiring trust and confidence in consumers by verifying and reducing the risk of fraud. These procedures are a result of years of operating trusted infrastructure for the Internet and having authenticated over half a million businesses.

As a valued authorized partner in the Website Security Partner Program, your understanding of our Authentication practices is essential to partner business continuity and sales success. Symantec Website Security Solutions has created this guide to help you appreciate the power and trustworthiness of this process, as well as help you navigate the Authentication process.

Individuals and businesses initiate authentication by providing information to Symantec as part of the online enrollment process. Depending on the certificate type being ordered, Symantec may verify that:

- The organization and organizational contact personnel are not listed on any of the U.S. Government denied entity lists: Denied Countries List, Denied Persons List, Denied Entities List, US Treasury Department List, or are subject to embargoes, sanctions or other restrictions.
- The organization has Government-issued credentials such as articles of incorporation or a business license that allow it to conduct business.
- The organization owns the domain name for which the certificate is issued OR has obtained legal right to use that domain name from the owner of the domain.
- The organization's contact personnel can be verified via a third-party phone number as an employee of the organization that is ordering the certificate.
- The organization is operating at a verified physical address.
- Symantec also carefully reviews any order information that has been flagged as being inconsistent with the order.

This comprehensive guide will provide detailed information involved from enrollment to issuance, in a handy easy to read manner.

CERTIFICATE TYPES

The Symantec Website Security Partner Program gives you access to the most recognized security solutions. This partner program includes industry leading premium and value brand website security and SSL products.

This guide will break down the product offerings available in the Website Security Partner Program into 5 different categories, each outlined below:

1. **Domain-Validated (DV)** SSL Certificates provide encryption with domain-only authentication, and validate the requestor is affiliated with use of the domain.

   Domain-Validated SSL Products offered:
   - Thawte SSL123
   - GeoTrust QuickSSL Premium
   - RapidSSL

2. **Organization-Validated (OV)** SSL Certificates provide full business authentication, along with verifying business identity and domain ownership.

   Organization-Validated SSL Products offered:
   - Symantec Secure Site
   - Symantec Secure Site Pro
   - Symantec Secure Site Wildcard
   - GeoTrust True Business ID
   - GeoTrust True Business ID Wildcard
   - Thawte SSL Web Server
   - Thawte SGC SuperCert
   - Thawte Wildcard SSL

3. **Extended Validation (EV)** SSL certificates utilize a more stringent level of authentication in providing the industry's highest level of assurance available today.

   Extended Validation products offered:
   - Symantec Secure Site with EV
   - Symantec Secure Site Pro with EV
   - Thawte SSL Web Server with EV
   - GeoTrust True Business ID with EV

4. **Code Signing** IDs provide full business authentication. The ID generates a digital signature that provides authentication of the code source and assurance of code integrity.

   Code Signing products offered:
   - Symantec Code Signing for Organizations
   - Thawte Code Signing for Organizations
   - Symantec Code Signing for Individuals
   - Thawte Code Signing for Individuals

5. **Symantec Safe Site** verifies identity and confirms the site has passed a daily malware scan by displaying the Norton Secured Seal. Symantec Safe Site does not provide SSL encryption.

   Symantec Safe Site products offered:
   - Symantec Safe Site for Organizations
   - Symantec Safe Site for Individuals

Our partner program includes industry leading premium and value brand website security and SSL products.

AUTHENTICATION PRODUCT MATRIX

The level of authentication varies by certificate category and product type. We have created a comprehensive guide to help you better understand what is involved in the validation of each certificate. The Authentication Product Matrix below will plot the course through the journey of Authentication, while the detailed instructions of each of these steps can be found throughout this guide.

	Product Name	U.S. Government Denied Lists	Organization Authentication	Domain Authentication	Organizational Unit Review	Verification of Operational Existence	Verification of Business Address	Confirmation of 3rd Party Telephone #	EV Contact Employment & Authority Confirmation	Verification of Contact	Acknowledgement Agreement
Domain Valida-tion*	Thawte SSL123	•		•	•						
	GeoTrust QuickSSL Premium	•		•	•						
	RapidSSL	•		•	•						
Organization Validation	Symantec Secure Site	•	•	•	•			•		•	
	Symantec Secure Site Pro	•	•	•	•			•		•	
	Symantec Secure Site Wildcard	•	•	•	•			•		•	
	GeoTrust True Business ID	•	•	•	•			•		•	
	GeoTrust True Business ID Wildcard	•	•	•	•			•		•	
	Thawte SSL Web Server	•	•	•	•			•		•	
	Thawte SGC SuperCert	•	•	•	•			•		•	
	Thawte Wildcard SSL	•	•	•	•			•		•	
Extended Validation	Symantec Secure Site with EV	•	•	•	•	•	•	•	•	•	•
	Symantec Secure Site Pro with EV	•	•	•	•	•	•	•	•	•	•
	Thawte SSL Web Server with EV	•	•	•	•	•	•	•	•	•	•
	GeoTrust True Business ID with EV	•	•	•	•	•	•	•	•	•	•
Code Signing	Symantec Code Signing for Organizations	•	•		•			•		•	
	Thawte Code Signing for Organizations	•	•		•			•		•	
	Symantec Code Signing for Individuals	•			•			•		•	
	Thawte Code Signing for Individuals	•			•			•		•	
Safe Site*	Symantec Safe Site for Organizations	•	•	•	•		•	•		•	
	Symantec Safe Site for Individuals			•	•		•	•		•	

*These products have specialized authentication practices. Use Table of Contents to see specific sections to reference for further information.

U.S. GOVERNMENT DENIED LISTS

The U.S. Government publishes and maintains the following Government Denied Lists. These lists include global organizations and individuals that Symantec is prohibited from doing business with. Symantec will not issue a certificate to an Organization if that Organization or any contact person listed on the order appears on any of these lists, some of which include:

- US Department of Commerce' Bureau of Industry and Security Denied Persons List:
  These are violators of the Export Administration Regulations. The list of Denied Persons contains information on the names and addresses of firms and individuals denied access to U.S. goods in addition to the reason(s) for the denial action.

- US Department of Commerce' Bureau of Industry and Security Denied Entities List:
  These persons, countries, or organizations have been determined by the US government to present an unacceptable risk of diversion to developing weapons of mass destruction or the missiles used to deliver those weapons.

- US Treasury Department List of Specially Designated Nationals and Blocked Persons:
  These are Specially Designated Nationals and other persons whose property is blocked by the US government, to assist the public in complying with the various sanction programs administered by OFAC (Office of Foreign Assets Control).

Symantec also ensures that its customers are not from a Denied Country that the U.S. Government forbids U.S. companies and their non-U.S. locations from selling certain products to.

These countries may change at any time, but currently include:

- Cuba
- Iran
- Syria
- Sudan
- North Korea

ORGANIZATION AUTHENTICATION

As part of Symantec's Authentication process we will validate the Organization name entered during the enrollment, as it will appear on the SSL Certificate. The Organization requesting a certificate must be an active entity, confirmed by the government authority responsible for registering businesses within the specific jurisdiction (Locality, State, Country) referenced in the certificate request.

An exact match between the enrolled Organization name and confirmed name is required. We cannot accept any misspellings, unregistered acronyms, or abbreviations in the Organization name.

Important Note: Extended Validation certificates require an exact match between the enrolled Organization and confirmed name, including Corporate Identifiers (e.g., Inc, Corp, LLC, Ltd, Pty Ltd, etc.)

Symantec has access to an extensive number of government resources globally. In most cases, Symantec can find a Proof of Right document on file in one of the many government or private databases that we have access to.

Examples of "government authority" resources include:

- California Secretary of State (for US Corporations filed in the State of California, US)
- City of Chicago, IL (Chicago Business Licenses)
- National Credit Union Administration (United States Federal Credit Unions)
- UK Companies House
- Kamer van Koophandel (KVK) (Companies Registered in The Netherlands)
- New Zealand Companies Office
- State Administration for Industry & Commerce of the People's Republic of China

However if a particular resource is not available or we cannot validate your organization within the available resources, we may request a current, Government Issued Business Credential, often called a "Proof of Right" (POR). Proof of Right is a document that gives a company or organization the right to do business in that name. If a Proof of Right document is required for your organization, we will contact the organizational contact on the enrollment and request a copy of an acceptable Proof of Right document.

Examples of acceptable documents include but are not limited to:

- Articles of Incorporation / Certificate of Formation
- Business / Vendor / Reseller / Merchant License
- Charter Documents / Partnership Papers
- Registration of Trade or Assumed Name / Doing Business As / Fictitious Name Statement
- Registro Mercantil

Once an acceptable Proof of Right document is received from the customer, we must then verbally validate it with the issuing authority. If we can't confirm the validity of the document with the issuing authority we may use a third party to verify the organization's existence.

Please note that anytime documentation is required for an order, it may delay the issuing time of that certificate. Certificates cannot be issued until all proper documentation is in order and has been verified with the issuing agency. For this reason, timely submission of documentation is essential.

ORGANIZATION AUTHENTICATION

As indicated on the previous page, the items which are being verified with the "government authority" resources are:

1. The Organization Name in the enrollment – Must be an exact match to the business registration
2. The Jurisdiction – Country, State & City (where applicable) must match the enrollment
3. The Organization Status – Must state active or equivalent, any inactive/revoked or equivalent organizations cannot obtain an SSL certificate and must update their status.

Organization: Symantec (UK) Limited
Country: GB
State: Berkshire
Locality (city): Reading

Organization: Symantec Corporation
Country: US
State: California
Locality (city): Mountain View

Organization: Symantec (UK) Limited
Country: US
State: California
Locality (city): Mountain View

Organization: SYMC LTD
Country: GB
State: Berkshire
Locality (city): Reading

DOMAIN AUTHENTICATION

In order for Symantec to validate your website domain name(s), we require that we either find proof that you own the domain name(s) you are trying to secure, or that you have a legal right to use that domain name. For the former, we check online databases that list the legal owner of every domain name we secure. A "WHOIS" report is a service provided by most domain registrars which provides information on ownership (Registrant) of the domain as well as contact information.

Depending on your domain extension(s), Symantec will use various "WHOIS" search databases to determine the domain registrant (owner).

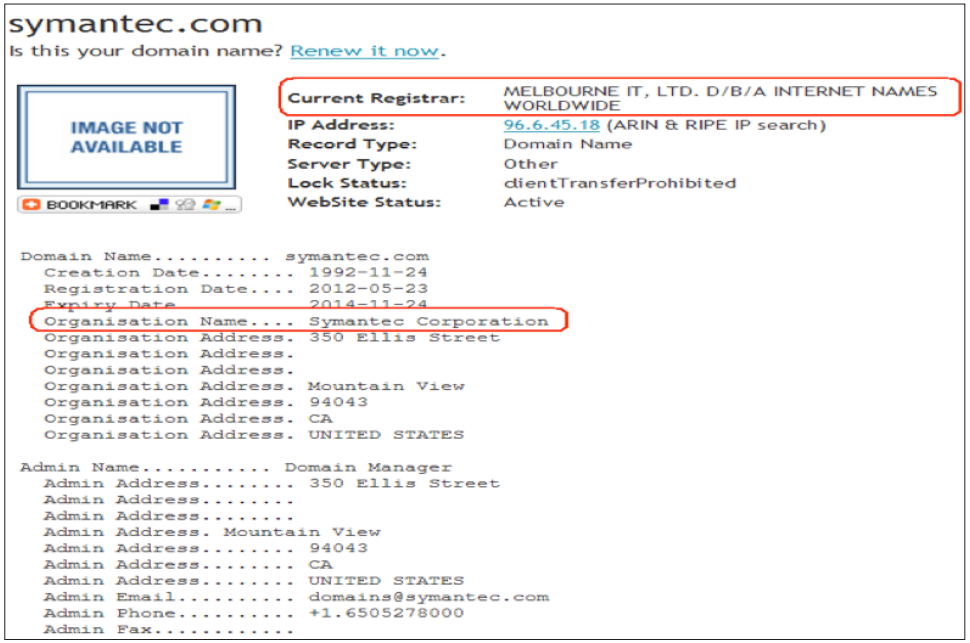
Important Note: "Intranet" common names (not containing a fully-qualified domain name) are no longer allowed per industry guidelines (CA Browser Forum).

We must also verify the domain(s) listed within the certificate enrollment are registered with a domain Registrar who is accredited by either:

- ICANN (Internet Corporation for Assigned Names and Numbers): For non-country code top level domains (.com, .net, .org, .biz, etc.) and International country code top-level domain extensions (.de, .uk, .au, .cn, etc.)
- IANA (Internet Assigned Numbers Authority): For International country code top-level domain extensions (.de, .uk, .au, .cn, etc.)

For example to find the owner of the domain Symantec.com

1. We may use a "WHOIS" search
2. Enter the domain in question (e.g. Symantec.com) and review Search results
3. The domain registrant (owner) is Symantec Corporation



DOMAIN AUTHENTICATION

What happens if the domain is not registered to the organization appearing on the certificate enrollment?

- If the registrant (owner) of the domain(s) enrolled in the order does not match the legal Organization name (as verified during Organization Authentication) we may request an update to the Registrant information with the domain registrar to show the full legal Organization Name.

- If any domain is "Privately Registered", meaning the true identity of the Registrant is not made public, we will request the identity be made available at least briefly so ownership may be validated.

Alternatively, we may approve the domain if:

- The domain is registered to a verified Parent/Subsidiary, or legally linked organization.

- Authorization is given by the domain administrator (listed in the "WHOIS" report) that the Organization has exclusive control of the domain. This can be done by either:
  - Verbal confirmation – we will call the telephone number listed in the "WHOIS"
  - Written confirmation – we will e-mail the administrator listed in the "WHOIS" (replies must be received from the same e-mail address it was sent to); or we may send the request to the following "pre-approved" aliases at your domain
    - admin@
    - administrator@
    - webmaster@
    - hostmaster@
    - postmaster@

Example: Enrollment for www.symantec.com, we can send to admin@symantec.com

- A "Professional Opinion Letter" is submitted, signed and attested to by a licensed attorney or Certified Public Accountant in the same country as the Organization. (See POL section)

- The customer can complete Practical Demonstration of domain control. This is done by the customer temporarily publishing a security code (provided by our Authentication Representatives) on their website.
  - Our Authentication Representatives must be able to reach the Organizational Contact using a verified third party telephone number under the Organization name.
  - If the Organizational or Technical Contact is unable to complete practical demonstration directly, they may conference in an employee within the Organization who is able to fulfill practical demonstration requirements. How ever, the Organizational or Technical Contact must remain on the line.
  - Once our Authentication Representative confirms security code and domain control, the code can be removed from the website.

If no WHOIS is available for a given top-level Domain (e.g. .zm domains), the Registrant must be confirmed directly with the Registrar IANA lists as responsible for that top-level domain.

ORGANIZATIONAL UNIT/ CONFIRMATION OF OPERATIONAL EXISTENCE

As part of the CA/Browser Forum Baseline Requirements for SSL Certificates, the Organizational Unit entered in the Certificate Signing Request (CSR) during the enrollment must be validated.

The Organizational Unit field must NOT contain any of the following:

- Unverified Legal Names (e.g., “Corp”, “Ltd.”, etc.)
- Unverified Trading Names (e.g., “Trading as”)
- Unverified Trade Marks (e.g., “(tm)”)
- Unverified Persons Names (Marc Smith)
- Domain Names & IP Addresses

The Organizational Unit may still contain

- Department names
- Server names (as long as it is not a domain name)
- General words and phrases

You may leave the Organizational Unit field blank, or enter information from the allowable items listed above.

Any information entered in the Organizational Unit field must be verified. If we are unable to verify the information and it falls under the “not allowed” section, our Authentication Representatives must update/remove from the CSR section before the certificate can be issued.

Certification Authority and Browser Forum Extended Validation guidelines stipulate organizations requesting Extended Validation must first have their Operational Existence confirmed.

Symantec must verify that the enrolling Organization has the ability to engage in business. The Operational Existence requirement is satisfied if the Organization has been registered and in existence for over 3 years, confirmed by the resource used during Organization Authentication.

If the organization is registered for less than 3 years, we can confirm Operational Existence by:

- Utilizing a valid Dun & Bradstreet report
- Verifying the Organization has a demand deposit account (such as a checking account) via one of the following:
  - Document from a regulated financial institution verifying that the Applicant has an active, current, Demand Deposit Account with the Institution. This document/information **must** be verbally confirmed directly with the financial institution, via a third party telephone number before we can accept it.
  - A Professional Opinion Letter.

ADDRESS VERIFICATION

Based on product type, Symantec may verify the address listed on a certificate enrollment. Verified information and requirements vary by product type; however any and all discrepancies must be corrected prior to certificate issuance.

Safe Site (only)
This step is required for products which display an address in the Certificate Seal.

The Organization's physical address must be confirmed via one of the third party sources below:

- Any government-based resource used for Organization Authentication
- Any Symantec approved third party telephone number database
- Valid Dun and Bradstreet report
- "WHOIS" report
- Verbal confirmation via the Verification call

If the address cannot be verified through one of the resources above we will request **ONE** of the following documents containing the Organization Name and address:

- Bank or Insurance Statement
- Utility Bill
- Telephone Bill

Extended Validation
The address in the enrollment must be a physical address and not a P.O. Box address, and must be a verified valid business address for the Organization or its verified Parent/Subsidiary.

- Parent/Subsidiary must be within the same country as country of Jurisdiction
- Subsidiaries are required to be majority owned

This address can be verified through ONE of the following sources:

- Government agency resource used during Organization Authentication
- A valid Dun & Bradstreet report
- Global Authentication and Verification Report
- A Professional Opinion Letter

If the address does not match, the Organizational Contact may be asked to provide an alternate, verifiable address for the Organization. The order must be updated to reflect the verified address.

CONFIRMATION OF THIRD PARTY TELEPHONE NUMBER

Symantec should be able to contact the customer's organization, and confirm that the Organizational Contact is a full time employee of the Organization Name in the enrollment. To begin this process our Authentication team will try to obtain an independently verified (third party) telephone number for the organization.

Confirmation that Technical Contact is a full time employee is allowed for organization-Validated (OV) SSL Certificate enrollments.

Organization Validated & Safe Site (only)
The telephone number must be listed under the Organization name (or verified Registered Trade name, or Legally Linked organization) in the country on the certificate request.

It must be obtained through a Symantec approved third party resource, such as:

- Approved online directory (Yellow Pages)
- Directory assistance
- Government resource used to authenticate the Organization
- Dun & Bradstreet Report

If we are unsuccessful in obtaining a valid third party telephone number for the organization, we will e-mail the Organizational Contact with the following alternate options:

- A "Professional Opinion Letter for SSL", signed and attested to by a licensed attorney or Certified Public Accountant in the same country as the Organization may be used to provide a qualified telephone number
- A Telephone Bill under the organization name, including the billing address and telephone number being billed
  - Symantec must then verbally confirm the information with the issuing telephone company, using a third party telephone number for the telephone company.
- Certified Utility Bill, Financial Institution Statement, Lease Agreement, or Telephone Bill under the organization name, which contain the billing address and telephone number being billed.
  - These documents must be certified and attested to by one of the following professionals in the customers jurisdiction.
    - Notary Public
    - Government Officials
    - Attorneys Licensed to Practice Law
    - Certified Public Accountant

The professional completing the letter will be verified (with the registered Bar Association/Board of Accountancy/Notary Public/Government Agency) in the appropriate jurisdiction. If we are unable to verify the professional we cannot accept a letter signed by that individual.

Note: We cannot accept the invoices from: Virtual PBX companies, Virtual Office/call forwarding Services, Voice over IP (VOIP) services that do not list telephone numbers on the invoices

our Authentication team will try to obtain an independently verified (third party) telephone number for the organization.

CONFIRMATION OF THIRD PARTY TELEPHONE NUMBER

Safe Site & Code Signing for Organizations (only)
The Safe Site & Code Signing for Organizations procedure for obtaining a third party telephone number is the same as an Organization Validated Certificate, however there is one additional alternative option:

- A Notary Letter signed by the Organizational Contact and notarized.
  - This letter must be notarized by a Public Notary or equivalent in the country of the Applicant's Jurisdiction or any jurisdiction where the Applicant maintains a confirmed office or physical facility.
  - The Notary Public or equivalent must include their certification information, as we will verify their active status.

An acceptable Notary Letter will take place of the final verification call.

Code Signing for Individuals
For validation, an ID form will be sent to the applicant requesting a copy of their valid passport and a confirmation of their telephone number.

If a passport is not available, two valid forms of ID will be accepted:

- Government-issued ID containing full name and a photo:
  - Drivers License
  - National or State ID Card
  - Military ID Card

- Secondary ID, containing full name:
  - Medical Card
  - Employee Badge
  - Utility Bill
  - Social Security Card
  - Proof of Age Card
  - Student ID Card

The ID Form must be notarized by a Public Notary or equivalent in the country of the Applicant's Jurisdiction or any jurisdiction where the Applicant maintains a confirmed office or physical facility.

Extended Validation
To obtain/confirm a telephone number for an Extended Validation order, the telephone number must be listed under the Organization name (or verified Registered Trade name, or Legally Linked organization) and must include the entire verified business address.

It must be obtained through a Symantec approved third party resource, such as:

- Approved online directory (Yellow Pages)
- Directory assistance
- Government resource used to authenticate the Organization
- Dun & Bradstreet Report

If we are unsuccessful in obtaining a valid third party telephone number for the organization, we will e-mail the Organizational Contact with the following alternate option:

- A "Professional Opinion Letter for EV", signed and attested to by a licensed attorney or Certified Public Accountant in the same country as the Organization may be used to provide a qualified telephone number.

CONTACT REQUIREMENTS

Symantec verifies the contact information listed on a certificate enrollment. Verified information and requirements varies by product type and brand, however any and all discrepancies must be corrected prior to certificate issuance.

Please ensure your customers are aware of the certificate enrollment and respond to all contact attempts within a timely manner, failure to do so may result in delayed certificate issuance.

	Contact Requirements	Organization Validated	Code Signing	Domain Validated	Extended Validation	Symantec Safe site
General Rules (All Contacts)	Free e-mail address allowed? (e.g. yahoo, gmail, hotmail, etc.)	Y (not preferred)	N	Y	N	Y
	Mismatch between personal e-mail address and contact name allowed? (i.e. Jill Smith John_doe@email.com	N	N	N	N	N
	Is a PO Box allowed in the address field?	Y	Y	Y	N	Y
Organizational Contact	Must Organizational Contact be an employee of enrolling organization?	Y	Y	Y	Y	Y
	Can Organizational Contact be listed as a job title or alias? (i.e. Network Admin, IT Dept)	Y	N	Y	N	N
Technical Contact	Must Technical Contact be an employee of enrolling organization?	N	Y	N	N	N
	Can Organizational Contact be listed as a job title or alias? (i.e. Network Admin, IT Dept)	Y	N	Y	N	Y

Important Note: Billing Contact details are pre-populated based off the Partner Center account, and do not require further Authentication.

EV ORGANIZATIONAL CONTACT EMPLOYMENT & AUTHORITY

With Extended Validation Certificates, Symantec must be able to contact your Organization, and confirm that the Organizational Contact applying for the certificate is an employee of the Organization listed in the order. This person must also have the "Authority" to purchase the certificate on behalf of the organization.

Organizational Contact Employment Confirmation
The Organizational Contact employment can be confirmed several ways:

- If the Organizational Contact is listed as an officer or executive of the organization in:
  - The Business Registration used during Organization Authentication
  - A valid Dun & Bradstreet report
  - The Global Authentication and Verification Report
- Confirmation with the Organization's Human Resources department
  - Symantec will contact using the third party telephone number (see "Confirmation of Third Party Telephone Number")
- Professional Opinion Letter

Organizational Contact Authority Confirmation
"Authority" indicates that the Organizational Contact is authorized to purchase the EV certificate on behalf of the Organization. Authority can be determined several ways:

- Authority is confirmed if the Organizational Contact is listed as an officer or executive of the organization in:
  - The Business Registration used during Organization Authentication
  - A valid Dun & Bradstreet report
  - The Global Authentication and Verification Report
- Authority of the Organizational Contact is confirmed if the Organizational Contact's job title is confirmed by Human Resources as someone with 'deemed authority'
  - Deemed Authority is someone with title of Director or higher (VP, Officer, CEO, CIO, etc.)
- Authority is also confirmed via a signed Acknowledgement Agreement.

If the Organizational contact is not someone with 'deemed authority', confirmation of Authority can be confirmed with someone with 'deemed authority', or the individual Human Resources confirms as the Organizational Contact's direct manager.

VERIFICATION CALL/ACKNOWLEDGEMENT AGREEMENT

The final step in the validation process is the Verification Call or e-mail. Symantec uses the previously obtained third party telephone number to reach the Organizational Contact or Technical Contact (if employed directly with the organization) and verify the enrollment details. In some cases we can issue the certificate without speaking directly with the Organizational or Technical Contact, while in others direct contact is required.

For Organization Validated certificates, additional options are available when the Organizational or Technical Contacts are not readily available to receive the Verification Call (requires web access):

- Online Verification
- Verification with an automated attendant

Online Verification is only possible when the contact's e-mail address is confirmed or a personal voicemail is reached and a message can be left with instructions. E-mail addresses are confirmed by using either Proof of Right documentation or directly with an individual at the previously obtained third party telephone number obtained for the organization.

Verification with an automated attendant is currently available for certificate orders from AU, CA, GB, HK, NZ, SG and US. Plans are currently in place to expand automated Verification to new countries and updates will be provided when this occurs.

Automated Verification begins with an e-mail to the Organizational Contact who must initiate the process and is successful after 4 simple steps. This process requires that the contact is available to receive two calls - first to a telephone number entered during Step 2 and second to the previously obtained third party telephone number.

Please reference the matrix below to understand acceptable methods of verification by product/category type.

Product Category/ Name	Verification Call with Organizational Contact	Verification Call with Technical Contact	Verification by confirmed e-mail	Personal Voicemail Confirmation	Verification Not Required
Domain Validation	• **				•
Organization Validated	•	• *	• *		
Extended Validation	•				
Code Signing for Organizations	•				
Code Signing for Individuals	•				
Safe Site for Organizations	•			•	
Safe Site Individuals					•

*Can only be used if employment and contact information have been confirmed

**Required for Major Corporations, Financial Institutions and Well-known Trademarks

After completing an enrollment, the Organizational Contact in the certificate enrollment must complete an Extended Validation Subscriber Agreement (also known as the "Acknowledgement Agreement"). This can be done online, or by signing the form and returning to us via fax or e-mail.

ACKNOWLEDGEMENT AGREEMENT

Acknowledgement Agreement Form
The Organizational Contact in the certificate enrollment will receive a copy of the Acknowledgement Agreement form via e-mail.

The Acknowledgement Agreement form has two separate sections; one required and one optional.

Required Content:

Order Number: <Order Number>

I, <Organizational Contact>, have read and confirm my acceptance, on behalf of <Organization Name>, of the Symantec SSL Certificate Subscriber Agreement version 6.0, which includes all Extended Validation terms and conditions, a copy of which is available at https://www.symantec.com/about/profile/policies/repository.jsp?tab=Tab2#stn-cps
In requesting this Extended Validation Certificate and accepting this agreement on behalf of my Organization, I confirm that <Organization Name> (Applicant) is entering into a legally binding and enforceable Subscriber Agreement that imposes extensive obligations on Applicant. I understand and acknowledge that an EV Certificate serves as a form of digital identity for Applicant and that the loss or misuse of this identity can result in great harm to the Applicant. By signing this Subscriber Agreement, I hereby represent that I have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the company's website, and that Applicant is responsible for all uses of its EV Certificate. By signing this Agreement on behalf of Applicant, I further represent that I (i) am acting as an authorized representative of Applicant. (ii) am expressly authorized by Applicant to sign Subscriber Agreements and approve EV Certificate requests on Applicant's behalf, and (iii) have confirmed Applicant's exclusive right to use the domain(s) to be included in EV Certificates.

Full name of organizational contact: <Organizational Contact>
Signature: _____
Title:_____
Date:_____
Place of signing (e.g. City, State): _____

The form must be completed with the correct **"variable fields"** (Organizational Contact and Organization) which match the enrollment, and the remainder of the form cannot be altered in any way.

Important Note: It is imperative the Acknowledgement Agreement be signed by the Organizational Contact only, otherwise it is void and we cannot accept it.

Optional Content:

Other organizational contact information (optional)

To assist with order processing, we recommend that you provide Symantec with the additional contact information below. We recommend that you also advise these people that they will be contacted by Symantec to verify certain details about your order for an Extended Validation certificate.

Human Resources contact. Symantec may contact this person to verify your employment and job title.

Name _____
Telephone_____ Ext _____

The Human Resources Contact will be contacted to complete employee verification. To avoid delays, it is recommended the Human Resource contact is informed of our intent to reach them.

A new Acknowledgement Agreement form is not required for each enrollment if the Organizational Contact and Technical Contact remain the same.

Online Acknowledgement Agreement
All of three SSL brands in the Symantec Website Security Partner Program which offer Extended Validation Certificates also have an online method of completing the Acknowledgement Agreement. During the final verification of the order, online Acknowledgement can be completed in the following steps:

1. A Symantec Authentication Representative will provide a personalized link via e-mail to the verified e-mail address of the Organizational Contact (e-mail must be verified by the contact directly during final verification or through Human Resources).

2. Symantec Authentication Representative will also provide a security code to the Organizational Contact verbally over the phone.

3. Organizational Contact then clicks the link and reviews the agreement. The process is complete upon acceptance of terms, and successful submission of previously provided security code.

A new Acknowledgement Agreement form is not required for each enrollment if the Organization and Technical Contacts remain the same.

DOMAIN VALIDATED CERTIFICATES

Domain-Validated (DV) SSL Certificates provide encryption with domain-only authentication. These certificates do not include authentication of business identity, but provide validation the requestor is affiliated with use of the domain before we can accept it.

Authentication of Domain-Validated products consists of confirming that the Domain Name listed in the Certificate Request is registered, and that the Domain Approver has control over the Domain.

Upon enrollment within the Partner Center, an Approval Request e-mail (also referred to as the "Approver E-mail") is sent to the e-mail selected during the enrollment process.[1] The e-mail options provided during the enrollment process include:

- Any e-mail address listed in the public domain registration record ("WHOIS" report), or
- Any one of the pre determined e-mail aliases below (often used by domain administrators) combined with the domain from the certificate enrollment.
  - admin@
  - administrator@
  - hostmaster@
  - webmaster@
  - postmaster@

Example: If the certificate Common Name is www.abc.com, a valid approver e-mail address would be 'admin@abc.com'

Once the "Approver E-mail" is received, the recipient must click on the link provided to approve or reject the request. This process confirms the approver is affiliated with the domain owner.

As a Website Security Partner, you have the ability to resend the "Approver E-mail", or change the Approver e-mail address (to one of the allowable aliases listed above) within your Partner Center. Please reference our Knowledgebase Solutions for specific instructions.

Important Note: If a Domain Validated certificate request is for a major corporation, well-known trademark, or ANY financial institution, the Organizational Contact MUST be an employee of the company. In addition, Symantec must complete a verification call with the Organizational Contact, using a third-party telephone number.

(e.g. an order for www.visa.com must have an employee of Visa listed as the Organizational Contact and a full verification will be completed with that contact)

[1]There are two alternatives to the Approval Request e-mail process available to Partners with API enabled.*

File authentication – using this method, the domain approval step is driven by the verification of a Symantec defined content update to the website being secured by the certificate. Required content details are provided in the response to the certificate order request placed via the API only.

DNS authentication – using this method, the domain approval step is driven by the verification of a Symantec defined update to the DNS record of the domain being secured by the certificate. Required DNS update details are provided in the response to the certificate order request placed via the API only.

For more information on File authentication of DNS authentication please contact your Channel Account Manager.

**Footnote detail developed and updated by Product Management; all other information in Authentication Guide developed and managed by Customer Authentication Services.*

SYMANTEC SAFE SITE

Symantec Safe Site shows the world that Symantec has confirmed your identity and your site has passed a daily malware scan by displaying the Norton Secured Seal. Symantec Safe Site can be purchased for Organizations or Individuals, however it does not provide SSL encryption.

Symantec Safe Site for Organizations
The Authentication steps to reference for the Symantec Safe Site for Organizations can be found in the Authentication Product Matrix. The Authentication steps to reference include:

- Government Denied Lists
- Organization Authentication
- Domain Authentication
- Organizational Unit Review
- Verification of Business Address
- Confirmation of Third Party Telephone Number
- Verification of Contact

Symantec Safe Site for Individuals
Symantec Safe Site orders under Individual names will go through an automated validation process with Equifax at the time of enrollment. The applicant will be asked a series of questions to validate his or her identity. If the applicant passes validation the order will advance to the Domain Authentication step.

If the applicant fails validation, the Individual will need to complete and return a **Notarized Confirmation (Individuals)** form which is kept on file and valid for 25 months.

- The form must include a photocopy of a government issued photo identification, which must be issued in the same country listed on the enrollment.
- If the identification does not include an address, it must be hand written on the form.

Note: Self Proprietors in Austria, Germany, France, and Switzerland do not need to complete the Notarized Confirmation (Individuals) form if valid Business Registration documentation is provided

Once the individual validation is complete the order then goes through Domain Authentication. For Symantec Safe Site for Individuals, the Registrant (domain owner) **must** match the Individual name on the enrollment when viewing a "WHOIS" report.

Important Note: If the domain is registered to anyone other than the individual enrolling for the certificate the domain registration must be updated, there are no alternative methods of approving domain for this type of order.

PROFESSIONAL OPINION LETTERS

If we are unable to confirm any of the validation steps of the order, the Professional Opinion Letter (POL) may be requested.

The Professional Opinion Letter verifies certificate and Organization details via one document. It can be requested to confirm one or more of the following items:

- Authenticity of POR documents – documents must accompany POL (OV only)
- Employment & Authority of the Organizational Contact (EV only)
- Organization's Business Address & Telephone Number
- Organization's exclusive right to use the Domain
- Organization's Operational Existence (via confirmation of an active Demand Deposit account) (EV only)

A Professional Opinion Letter does not replace the Verification Call

Professional Opinion Letter Requirements

Professional Opinion Letter must be completed by:

- **Attorney** (solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or any jurisdiction where the Applicant maintains a confirmed office or physical facility. (EV & OV)

OR

- **Certified Public Accountant** (chartered accountant, or equivalent) licensed to practice accounting in the country of Applicant's Jurisdiction of Incorporation or any jurisdiction where Applicant maintains an office or physical facility. (EV & OV)

OR

- **Qualified Government Officials** (based on country regulations) in the country of Applicant's Jurisdiction of Incorporation or any jurisdiction where Applicant maintains an office or physical facility. (OV only)
  - These may include Clerks, Bailiffs, Registrars, Judges, Justices of the Peace and Police Officers.
  - Notaries Publics (outside of the US and Canada) who are a Government Official or Legal Professional can sometimes sign the POL.

The professional completing the letter will be verified with the registered Bar Association or Board of Accountancy in the appropriate jurisdiction. If we are unable to verify the professional we cannot accept a letter signed by that individual.

Important Note: EV orders require all information in the Professional Opinion Letter be confirmed directly with the Attorney or Certified Accountant. They will be contacted using the contact details filed with the registered Bar Association or Board of Accountancy in the appropriate jurisdiction. Please ensure this person is aware of our intent to contact them to verify the information.

BEST PRACTICES

Our goal is to get your order to you as quickly as possible, while strictly adhering to the Authentication requirements. Symantec may not issue out a certificate which has not yet passed all validation steps, doing so may jeopardize the integrity of the certificate.

- To expedite the issuance of your order please ensure
  - The enrollment is placed under the legal Organization name and jurisdiction
  - The Organization is active and in good standing
  - The domain is registered to the legal Organization name on the enrollment (or Individual where applicable)
  - The Organizational Contact is a permanent employee of the enrolling Organization (where applicable)

- Notifications or request for information are sent to the Organizational and/or Technical contacts on the order. Please ensure your customers are aware of the certificate enrollment, and they respond to our requests in a timely manner. Failure to do so may result in delayed certificate issuance.

- As a Partner, if you are not a contact on the order, you may reference the order status and posted comments in the Partner Center or API (quick search).

Extended Validation

- If an Organization would like to list its 'trading as' or 'doing business as' name in the certificate, it can only appear in the 'Organization Name field' under the following conditions:
  - The trading name must be verified with the appropriate government agency as being valid and belonging to the organization.
  - The name must appear in conjunction with the verified Organization name (incorporated name)
    Example: Alphabet Soup (ABC Inc)
    Trade Name: Alphabet Soup
    Organization Name: ABC Inc.
  - If the full Organization name plus Trading name exceeds our 64 character limit, then only the Organization name may be used.

Code Signing

- Since both the Organizational and Technical Contacts of a Code Signing order must be from the enrolling organization, a Partner may not list themselves on these types of certificate enrollments.

- The Code Signing certificate must be downloaded into the same web browser from which the CSR was generated.

PARTNER RESOURCES

Beyond this Partner Authentication Guide, we have other support tools and resources for partners that will quickly enable partners to more effectively work their business. Log in today.

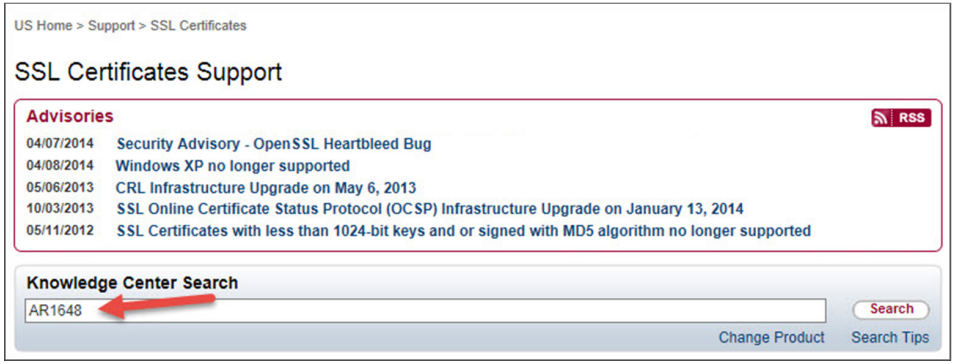
- **Partner Center:**
  Symantec: https://products.websecurity.symantec.com/geocenter/reseller/logon.do
  Thawte: https://products.thawte.com/geocenter/reseller/logon.do
  GeoTrust: https://products.geotrust.com/geocenter/reseller/logon.do
  RapidSSL: https://products.geotrust.com/geocenter/reseller/logon.do

- **PartnerNet:** https://partnernet.symantec.com/Partnercontent/Login.jsp
  Created exclusively for our partner community, PartnerNet provides you with everything you'll need to help you develop new business opportunities and meet the growing needs of your customers.

  Resources available on Partner Center or Partner Net:
  - Authentication Video
  - Webcast Trainings by product category:
    - Domain Validated (DV)
    - Organization Validated (OV)
    - Extended Validation (EV)
    - Code Signing
    - Symantec Safe Site

- **Road to Profitability R2P:** www.roadtoprofitability.com
  Take a trip through our Website Security Partner Program. Each stop along the way has valuable information to help you become more profitable today—and on the road ahead.

Additional Resources:
Symantec Knowledgebase: https://products.websecurity.symantec.com/geocenter/reseller/logon.do
Thawte Knowledgebase: https://products.thawte.com/geocenter/reseller/logon.do
GeoTrust Knowledgebase: https://products.geotrust.com/geocenter/reseller/logon.do
To view a list of Partner Center FAQs search AR1648 within the Knowledgebase.



CONTACT INFORMATION

Visit our website
http://go.symantec.com/wspp

To speak with Partner Support
866-893-6565 (option 7) or 650-426-3347 (option 7)
e-mail: partnersupport@symantec.com
(U.S., Canada, and Latin America)
e-mail: emeapartnersupport@symantec.com
(Europe and Africa)
e-mail: apacpartnersupport@symantec.com
(Asia, Australia, and New Zealand)

To speak with the Partner Sales Team within the U.S.
Go to go.symantec.com/wspp to chat with a sales person
866-893-6565 (option 6) or 650-426-3347 (option 6)
e-mail: channel-partners@symantec.com

To speak with the Partner Sales Team outside the U.S.
Go to go.symantec.com/wspp to chat with a sales person
+49 69380789081 (Germany)
+33 157324268 (France)
+44 2034505486 (UK)
+27 21 819 2800 (South Africa)
For other specific country offices and contact numbers, please visit our website.

About Symantec
Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com.

Symantec Worldwide Corporate Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec Worlwide Corporate Heaquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com