



## AUTHENTICATION GUIDE



# Extended Validation SSL

## Authentication Requirements



Where it all comes together.™

Copyright © 2008 VeriSign, Inc. All rights reserved.

The information in this document belongs to VeriSign. It may not be used, reproduced or disclosed without the written approval of VeriSign.

---

#### DISCLAIMER AND LIMITATION OF LIABILITY

VeriSign, Inc. has made efforts to ensure the accuracy and completeness of the information in this document. However, VeriSign, Inc. makes no warranties of any kind (whether express, implied or statutory) with respect to the information contained herein. VeriSign, Inc. assumes no liability to any party for any loss or damage (whether direct or indirect) caused by any errors, omissions, or statements of any kind contained in this document.

Further, VeriSign, Inc. assumes no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner. VeriSign Inc. reserves the right to make changes to any information herein without further notice.

---

#### TRADEMARKS

VeriSign, the VeriSign logo, VeriSign Trust Network, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Other trademarks and service marks in this document are the property of their respective owners.

---

## Table of Contents

1. Overview of Extended Validation Requirements .....	4
2. Organization Authentication Requirements.....	4
3. Domain Authentication Requirements.....	5
4. Organizational Contact Authentication Requirements.....	5
5. Alternative Authentication Steps .....	6
6. Order Verification Requirements.....	6
7. Acceptance of Agreement.....	6
8. Related Links .....	7

# 1. Overview of Extended Validation Requirements

Extended Validation (EV) SSL Certificates help achieve the highest level of consumer trust through the strictest authentication standards of any SSL certificate. Extended Validation authentication guidelines require VeriSign to obtain and verify multiple pieces of identifying information about EV SSL Certificate applicants.

To ensure your EV SSL Certificate request is processed quickly, review and provide the authentication documents described below.

# 2. Organization Authentication Requirements

The following entities are eligible to receive Extended Validation SSL Certificates provided they are currently registered with and approved by an official registration agency in their jurisdiction. The resulting charter, certificate, license, or equivalent must be verifiable through that registration agency.

- + Government agencies
- + Corporations
- + General partnerships
- + Unincorporated associations
- + Sole proprietorships (except in countries where there are no requirements for proprietors to register, for example, United Kingdom)

**VeriSign must be able to confirm all of the following organizational registration requirements:**

- + Official government agency records must include:
    - + The organization's registration number or the organization's date of registration/incorporation.
    - + The organization's registered address (or the address of the organization's registered agent).
  - + A non-government data source (such as Dun & Bradstreet) must include the organization's place of business address, phone number, and Officer/Director information (as identified in the order).
  - + If the organization has been registered for less than 3 years, VeriSign must verify operational existence through one of the following means:
    - + Through a non-government data source (such as Dun & Bradstreet)
- or -

- + By verifying the organization has an active demand deposit account (such as a checking account) with a regulated financial institution through a through a Lawyer or Accountant's Opinion Letter or directly with the financial institution.

### 3. Domain Authentication Requirements

To qualify for an Extended Validation SSL Certificate, domain registration details must reflect the full organization name as included on the certificate request.

- + The domain must be registered with ICANN or IANA registrar (for CCTLDs).
- + Where domain registration is not updated to reflect the organization name as identified on the certificate, the organization's exclusive right to use the domain name may be verified directly with the registered domain contact.
- + The organization's certificate approver must confirm knowledge of the organization's domain ownership during the verification call.

### 4. Organizational Contact Authentication Requirements

To qualify for an Extended Validation SSL Certificate, the Organizational Contact identified in the certificate request must be employed by the requesting organization and have appropriate authority to obtain and delegate Extended Validation certificate responsibilities.

**Note:** Employment and authorization cannot be verified through the organization's Web site.

**Note:** If the Organizational Contact identified in the certificate request is listed in government records as a corporate officer (such as Secretary, President, CEO, CFO, COO, CIO, CSO, Director, or equivalent), then the Organizational Contact's employment and authorization are deemed approved.

**VeriSign must be able to confirm all of the following Organizational Contact requirements:**

- + Organizational Contact's identity, title, and employment through the Organization's human resources department or an independent source.
- + Organizational Contact is authorized to obtain and approve EV certificates on behalf of the Organization and to delegate this authority to others. This can be verified through one of the following methods:
  - + A Lawyer Opinion or Accountant Opinion Letter
  - + A Corporate Resolution Letter
  - + Directly contacting the CEO, COO, or similar executive at the Organization, including persons named to be in the direct line of management, to confirm the authority of the Organizational Contact. If no public records are available

regarding the CEO, COO, or other executive, VeriSign will contact the Organization's human resources department for contact details.

## 5. Alternative Authentication Steps

If VeriSign is unable to verify any of the required information on your certificate application, we may request that you provide a professional opinion from a lawyer or accountant to verify that information.

## 6. Order Verification Requirements

As part of processing an Extended Validation SSL Certificate, VeriSign must verify the certificate request and all certificate details with the Organizational Contact identified in the certificate request. VeriSign must contact the Organizational Contact using an independently-obtained telephone number for the organization's verified address (not the telephone number provided in the order).

**VeriSign will obtain the telephone number through one of the following methods:**

- + By researching qualified telephone databases to find a telephone number. Ensure your Organization's primary telephone number is listed in a public telephone directory.
- + As provided in a Lawyer Opinion or Accountant Opinion Letter.
- + As confirmed during a site visit conducted by VeriSign.

**During the verification call, VeriSign must verify the following with the Organizational Contact:**

- + The name of the technical contact identified in the certificate request and his or her authority to obtain the Extended Validation certificate on behalf of the Organization.
- + Knowledge of the Organization's ownership and right to use the domain identified in the certificate request.
- + Approval of the Extended Validation SSL Certificate request.
- + Acknowledgement of signature on the Acknowledgement of Agreement

## 7. Acceptance of Agreement

During the verification call, VeriSign will provide the Organizational Contact with a verification code to use when accepting the online EV Acknowledgement of Agreement. VeriSign will also email a direct link to the Agreement.

## 8. Related Links

For additional details on Extended Validation SSL and authentication requirements, go to:

**Extended Validation SSL FAQ**

<http://www.verisign.com/ssl/ssl-information-center/extended-validation-ssl-certificates/index.html>

**Guidelines for Extended Validation Certificates**

<http://www.cabforum.org>

