

**SSL Certificate Application Form**

The purpose of this document is to capture all the necessary data for the issuance of the certificate, so they must be **real** and **correct**, as they will be subjected to the verifications of the specialized teams.

Notice that:

- "Authorization Contact" will be contacted by Entrust to confirm that the organization is authorized to create and manage certificates for the company;
- in the case of EV certificates the Higher Authority role could be contacted by Entrust to confirm all additional roles;
- please provide a complete business landline phone number, including extensions, for contact whenever possible. This will expedite the verification process. Do not provide cell phone numbers.
- please inform designated business roles of the possibility to be contacted by phone and/or e-mail by Entrust to complete verifications.
- Please make sure that the e-mail address for "Authorization Contact " is a direct e-mail address. Generic departmental e-mail addresses cannot be used (e.g. [it@domain.com](mailto:it@domain.com).)

COMPANY INFORMATION				
Applicant Company Name				
Address				
City		Province		ZIP CODE
Nation				
Tax Code		VAT number		
<b>Domains for which certificate is requested (without www)</b>				
Domain name:				
<b>Domain verification method chosen (mark your choice with X)</b>				

DNS

Contact me for explanations

(You will be contacted for clarification about the above two methods.)

Authorization Contact				
Name		Last name		
Company				
Address				
City		Province		ZIP CODE
Corporate role				
Phone		E-mail		
Administrator 1				
Name		Last name		
Company				
Address				
City		Province		ZIP CODE
Corporate role				
Phone		E-mail		
Administrator 2				
Name		Last name		
Company				
Address				
City		Province		ZIP CODE
Corporate role				
Phone		E-mail		



ADDITIONAL INFORMATION NEEDED FOR VERIFICATION EV					
<b>Higher Authority</b>					
Name		Last Name			
Company					
Address					
City		Province		ZIP CODE	
Corporate role					
Phone		E-mail			
<b>Contract Signer</b> (may be the same person who serves as the Authorizing Contact)					
Name		Last Name			
Company					
Address					
City		Province		ZIP CODE	
Corporate role					
Phone		E-mail			

Date \_\_\_\_\_

<b>Signature</b>	
------------------	--

**Note\***

**Roles and Responsibilities**

OV Roles	Additional EV roles
<b>Administrator:</b> Responsible for issuing and managing certificates in the <i>Entrust</i> certificate management portal. Receives portal login credentials to perform functions such as issuing, renewing, and revoking certificates. Administrators will also be responsible for completing the domain verification required to issue certificates.	<b>Higher Authority:</b> This person should be in a corporate role at the manager level or above.  <b>Please note:</b> Higher Authority cannot hold other roles. Higher authority authorizes the other roles (e.g., if the EV contract signer role needs to be updated, Higher Authority will be asked to approve the changes).
<b>Authorization Contact:</b> Reference for account authorizations, (such as adding new administrators). Will be contacted annually by <i>Entrust</i> to confirm any changes to company information. May be filled by an IT manager.	<b>Contract Signer:</b> This person accepts the EV service contract at the time of enrollment. He/she must also confirm the new administrators.  This can be the same person who performs the Authorization Contact role.
<b>Notes on OV verification operations</b> Upon creation of the Entrust Certificate Management platform, the company/organization will have its identity verified by the Entrust verification team. The authorizing contact will receive a verification phone call. This phone call has to be made to a verified phone number, belonging to the organization. This is made to ensure that the authorizing contact is connected to the organization listed on the certificate.	<b>Notes on EV (Extended Validation) Verification Operations.</b> As EV verification offers a higher level of reliability, additional approvals are required to ensure that certificates are requested and managed by trusted roles within the organization.

**INFO and ASSISTANCE**

For any clarifications or requests for assistance, please see the dedicated area on the Namirial support site: [assistenza.namirial.it](https://www.namirial.it/assistenza).