# EXTENDED VALIDATION BUILDS TRUST

Online commerce requires trust. Certificate Authorities provide that trust through SSL certificates. EV-SSL (the EV stands for Extended Validation) provides the gold standard for SSL certificates. Merchants must undergo a rigorous process to obtain an EV-SSL certificate, and how browsers display the certificate is different than a normal SSL certificate.

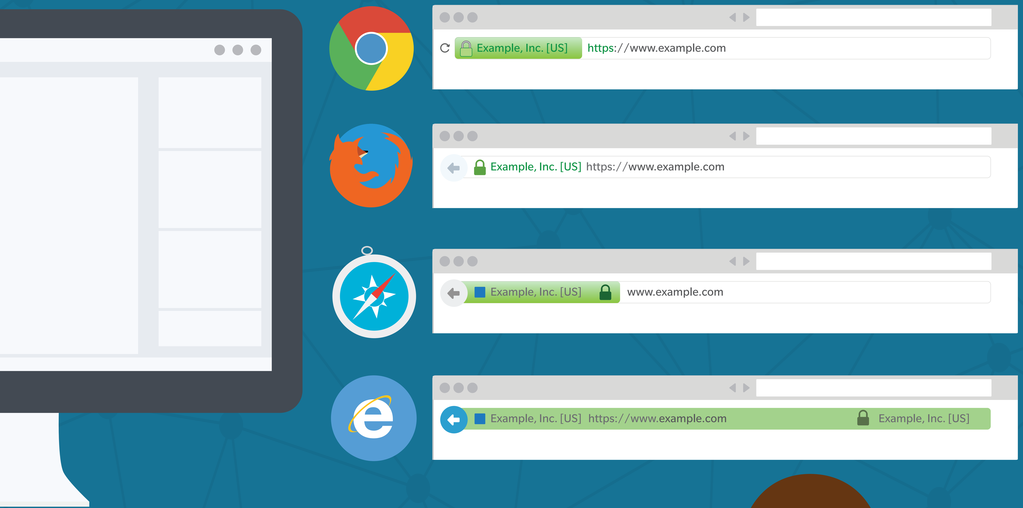
## Here is how EV-SSL works...

### How to apply for an EV Certificate

1. Only certificate authorities (CAs) which pass an independent, qualified audit review may issue EV certificates. CAs must follow rigorous steps before issuing an EV SSL certificate.
2. The authorized CA evaluates the organization applying for the certificate to verify their identity and check that they should receive an EV SSL certificate.
3. The authorized CA confirms the organization's registered legal name, registration number, registered address, physical business address and any assumed business names.
4. The authorized CA verifies the applicant organization's right to use the domain name.
5. The authorized CA substantiates that the applying organization has approved the issuance of an SSL certificate with EV.
6. The authorized CA makes sure the organization applying for an EV certificate is not located in a country on government prohibited lists.
7. Only when everything checks out does the CA issue the EV Certificate.

# WEB BROWSERS DISPLAY TRUST

Look for the color green and the organization name in the website address bar. Each browser has a slightly different way of indicating if a site uses an EV Certificate:




Consumers know the padlock and green bar indicates a trusted connection. Just 2% proceed past "untrusted connection" messages and only 3% would give out credit card information without the padlock icon.*

CA Security COUNCIL

For more information go to

**https://casecurity.org**

*Source: CA Security Council 2015 Consumer Trust Survey
https://casecurity.org/2015-consumer-trust-survey/