

Installation and usage of SSL certificates:

Your guide to getting it right





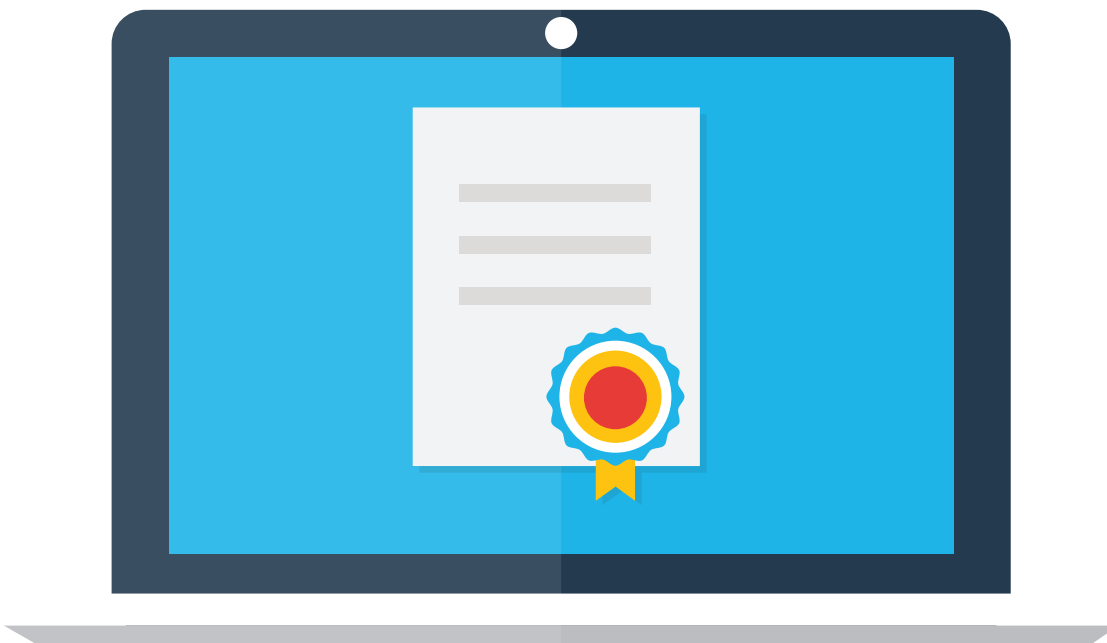
So, you've bought your SSL Certificate(s).

Buying your certificate is only the first of many steps involved in securing your website. All too often, certificates are not properly installed, sensitive pages are left insecure, and form information posted unencrypted, leaving many websites vulnerable to attack.

That is why Symantec has put together the following tips, as your guidance to getting the process absolutely right from the outset. Steering you through the more stormy waters, warning you off the more turbulent practices and procedures that can undermine SSL, because your SSL Certificate is the passport to a safer, more secure site for you, your people and your customers.

Only one way to install SSL – and that's properly!

Like many other organisations, you've recognised the need to purchase an SSL Certificate and taken that all important step. Now you need to make sure it is properly installed. If your customers don't feel completely safe on your site, they simply will not do business with you.





TIP 1 - Preparing the Private Key and CSR



To install a digital certificate, you must first generate the private key and the Certificate Signing Request (CSR) from that private key, for the server where the certificate will be installed. Then submit the CSR to enrol for a certificate. Here's how.

If you have IIS 6 and above servers or Redhat Linux servers you can download our tool – [Symantec SSL Assistant](#) – and follow the user-friendly prompts. For a list of CSR generation instructions on other servers, have a look at: [Symantec CSR Generation](#). To enrol for any of Symantec's SSL Certificate services, you will need the following information:

- The term or validity period of the certificate, 1, 2 or 3 years
- The number of servers hosting a single domain (up to 5 servers)
- The server platform
- The organisation, organisational unit, address
- Payment information and a contact for invoicing
- The common name. This is the host + domain name, such as 'www.mydomain.com' or 'webmail.mydomain.com'
- An email address where Symantec can reach you to validate the information
- A Certificate Signing Request (CSR) generated from the server you need to secure

Then, once you get your certificate, follow the instructions in tip 3.

If your server is not listed or you need additional information, refer to your server documentation or contact your server vendor. If you do not know what software your server uses, contact your IT administrators.

During enrolment, submit the CSR with the header and footer:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



TIP 2 - How to install an SSL Certificate – the Right Way!



About to install an SSL Certificate for the first time and finding the idea a bit intimidating? You needn't worry. It's much easier than you might think. Let's have a look at installing a Certificate on a server, with Symantec.

All servers follow the same logic:

Step 1 – Saving the Certificate

Follow the instructions in your confirmation email to save the SSL Certificate to your desktop from the URL provided. That will give you both your Certificate and the intermediate CA Certificates you need.

Step 2 – Install or move to a Certificate folder

Step 3 – Configure the Certificate on the website

Step 4 – Reference the Certificate

[Click here](#) for detailed information and step by step instructions for each server type.

To get the most out of your SSL Certificate, be sure to add the Norton Secured Seal to your website. That will make your customers feel more secure when transacting with you.

Just copy and paste the relevant lines from Symantec's Norton Secured Seal pages to add the seal on your website – clear instructions will be found in the link at the end of this tip. This will also explain how you can test your Certificate with the Certificate Installation Checker by entering your domain when prompted.

Now your SSL Certificate is installed – and ready to roll!

Having problems?

Symantec has a range of tutorial videos for different servers: [View Tutorials](#)

Check Your Installation

Just enter the URL of the server you want to check: [Check Installation](#)

Generate Your Site Seal

Norton Secured Seal Installation Instructions: [Generate Seal](#)

Troubleshooting

Visit Symantec Support site: [Access Support](#)



TIP 3 - Protect Your Private Keys – and Opt for the Best



Public and private keys are an integral part of how SSL works.

The private key is kept secret on your server and is used to encrypt everything on the website. The public key placed inside the certificate is yet another part of your website's identity, such as your domain name and organisation details.

Treat your private keys as priceless assets, shared only amongst the minimum number of most trusted associates or employees. Imagine that you are a bank manager: would you hand out the keys to the vault indiscriminately? No. So here are some best practice tips:

- **Generate private keys on a trusted server.** Do not hand this task over to a third party!
- **Password-protect the private keys** to prevent any compromise when they are stored in backup systems.
- **Renew certificates every year** – and always introduce new private keys at the same time.

The size of the private key exerts a great deal of influence on the cryptographic 'handshake' used to establish secure connections. Using a key that is too short is insecure, but using a key that's too long can seriously slow down operations.

Elliptic Curve Cryptography (ECC) is gaining increasing attention, providing strong security assurances at smaller key lengths. Symantec offers ECC with key sizes at a fraction of the number of bits that RSA and DSA require, yet is over 10,000 times harder to crack (256-bits for ECC is the equivalent cryptographic strength of 3072-bits RSA). ECC offers stronger security with much reduced server overhead and will help to reduce CPU cycles required for server cryptographic operations.

More information on ECC is available on Page 7.



TIP 4 - Eliminate Any Weak Leaks in the Chain



In most SSL deployments, the server certificate alone is insufficient: three or more certificates are needed to establish a complete chain of trust. A certificate chain consists of all the certificates needed to certify the subject identified by the end certificate.

In practice this chain includes the end entity certificate, the intermediate CA certificates and the root CA certificate.

The process of verifying the authenticity and validity of a newly received certificate involves checking all of the certificates from the universally trusted Root CA, through any intermediate CAs, down to the certificate just received – the ‘end entity certificate’. A certificate can only be trusted if each certificate in that certificate’s chain has been properly issued and validated.

A common problem is configuring the end entity certificate correctly, but forgetting to include the intermediate CA certificates. To check if the intermediates are installed properly use our [certificate checker](#).



TIP 5 - RSA, ECC and Why Key Length is Important



Elliptic Curve Cryptography (ECC) offers your business enhanced security and better performance than current encryption.

A US government-approved and National Security Agency-endorsed encryption method, ECC creates encryption keys based on the idea of using points on an elliptic curve to define the public/private key pair. It is difficult to break using the brute force methods often employed by hackers and offers a faster solution with less computing power than RSA-based encryption.

RSA is an encryption and digital signature algorithm that has been the basis for security on the internet for nearly two decades. It is still a valid algorithm to use, but the acceptable minimum key size has increased with time to ensure protection from improved cryptographic attacks. Thus, with ECC, you get better performance, because it requires a shorter key length and provides a superior level of security. For instance, a 256-bit ECC key provides the same level of protection as a 3072-bit RSA key. The result? You get precisely the security you need without sacrificing performance.

Moreover, ECC's smaller key length means smaller certificates that consume less bandwidth. As more of your customers move to smaller devices for their online transactions, ECC offers a better all-round customer experience.

Symantec's ECC roots have been available in the top three browsers since 2007, so Symantec's ECC certificates will work in your existing infrastructure, as long as modern browsers are used, and they are available at no additional cost.

Learn more about [ECC and Algorithm Agility](#).



TIP 6 - All-embracing 'Always On SSL'



You should always look to encrypt your whole website with SSL – and the way to do that is to use Always On SSL. This is a cost-effective security measure for websites that helps protect the entire user experience from start to finish, making it safer to search, share and shop online.

Companies that are truly serious about protecting their customers and their business reputation will implement Always On SSL with SSL certificates from a trusted Certificate Authority, such as Symantec. Always On SSL is easy to implement, delivering authentication of the identity of the website and encrypting all information shared between the website and a user (including any cookies exchanged), protecting the data from unauthorised viewing, tampering or use.

Significantly, the Online Trust Alliance is calling for websites to adopt Always On SSL. It advises “Always On SSL is a proven, practical security measure that should be implemented on all websites where users share or view sensitive information”.

Many of the world’s most successful websites have recognised the wisdom of successfully implementing Always On SSL, protecting themselves against sidejacking and hacking through threats such as Firesheep and malicious code injection.

Always On SSL can help you protect the trust that users have invested in your website, giving users the assurance of knowing that you take their security and privacy seriously – and that you are taking every possible step to protect them online.



TIP 7 - Public Key Pinning: a Matter of Trust



Public key pinning (more properly known as the Public Key Pinning Extension for HTTP) is designed to give website operators the means to restrict which certificate authorities can issue certificates for their servers.

Basically, public key pinning associates a host with their expected certificate or public key. Once a public key is known or seen for a host, the public key is associated or 'pinned' to that host.

According to the CA Security Council, public key pinning allows the website owner to make a statement that its SSL certificate must have one or more of the following:

- A specified public key
- Signed by a CA with this public key
- Hierarchical-trust to a CA with this public key

If a certificate for the website owner's domain is issued by a CA that is not listed (ie, not pinned), then a browser that supports public key pinning will provide a trust dialogue warning. Website owners can also pin multiple keys from multiple CAs and all will be treated as valid by the browsers.

The website owner trusts that the chosen CAs will not mistakenly issue a certificate for the owner's domain. These CAs often restrict who can request the issuance of a certificate for the owner's specific domains, which provides additional security against certificates being wrongly issued to an unauthorised party.

Unfortunately, the CA Security Council states that the public key pinning that Google implemented in 2011 is not scalable as it requires the public keys for each domain to be added to the browser. A new, scalable public key pinning solution is being documented through a proposed IETF RFC (Internet Engineering Task Force Request for Comments).

In this proposal, the public key pins will be defined through an HTTP header from the server to the browser. The header options may contain a SHA-1 and/or SHA-256 key algorithm, maximum age of pin, whether it supports sub-domains and the strictness of the pinning, for example.



TIP 8 - Drive off the Eavesdroppers with Perfect Forward Secrecy



Would you be happy to think that an eavesdropper who was busy recording traffic – your traffic – here and now might be able to decrypt that in the future? No, of course not. And yet that could be the situation your organisation finds itself, albeit totally unaware of this danger.

Take RSA, for example. It generates a public and private key to encrypt and decode messages. Yet the continued use of recoverable keys could make stored encrypted data accessible, if keys are compromised in the future. In many cases, an attacker with your private key and saved SSL traffic can use the private key to decrypt all session keys negotiated during saved SSL handshakes, and then decrypt all saved session data using those session keys. It's a scenario that doesn't make for sleep-filled nights. But there's a better way – and it's called 'Perfect Forward Secrecy'.

When you use this solution, unrecoverable temporary session keys are generated, used and discarded. Moreover, PFS, when implemented correctly with Elliptical Curve Cryptography (ECC – see Tip 5), is more secure than RSA algorithms and performs better.

Using PFS, there is no link between the server's private key and each session key. If both client and server support PFS, they use a variant of a protocol named Diffie-Hellman (after its inventors), in which both sides securely exchange random numbers and arrive at the same shared secret. It's a clever algorithm that prevents an eavesdropper from deriving the same secret, even if the eavesdropper can view all the traffic.

For more details, see this Symantec Infographic:
[View Infographic](#)



TIP 9 - HTTP Strict Transport Security: your safety net



Staying ultra-safe online is vital. And sometimes that means ‘going the extra mile’ – beyond standard security – to get to where you want to be.

Hackers can make use of man-in-the-middle attacks, over wireless networks, such as SSL stripping to intercept browser requests to HTTPS sites and serve back requested pages over HTTP. This means that the connection is no longer encrypted and the hacker can intercept information that the victim enters into the supposedly secure website. The victim may never notice the change as they aren’t paying close attention to the browser address bar every time they navigate to a new page on a website. Browsers have no way of knowing that a website should be delivered securely, so will not alert you when a website is loaded via an unencrypted connection.

HTTP Strict Transport Security (HSTS) prevents this from happening by allowing servers to send a message to the browser demanding that any such connection must be encrypted. The browsers then acts on that message, so every web page that your customer visits will be encrypted as intended. Safeguarding you and your customers from attack.

To activate HSTS protection, you set a single response header in your websites. After that, browsers that support HSTS (Chromium, Google Chrome, Firefox, Opera, Safari for example) will respect your instructions. After activation, HSTS does not allow insecure communication with your website. It achieves this by automatically converting all plain-text links to secure ones.

Internet Explorer does not yet support HSTS, but Microsoft has stated that it will do so in Internet Explorer 12.

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Circle Logo and the Norton Secured Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.