

Instalação e uso de certificados SSL: seu guia para o sucesso





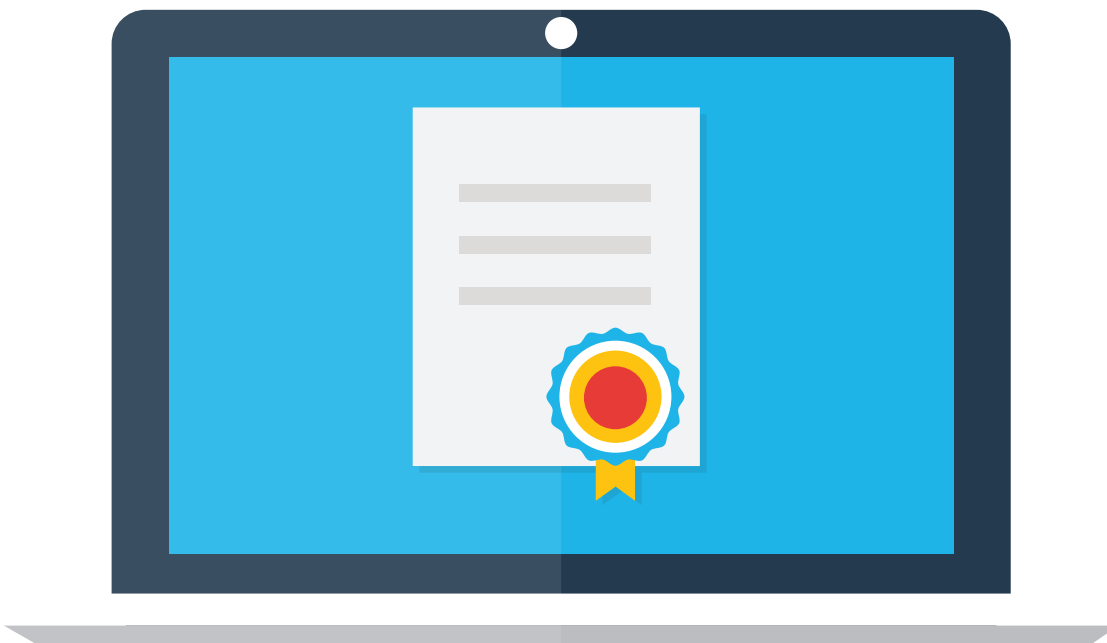
Então você comprou certificados SSL.

Adquirir seu certificado é apenas o primeiro dos vários passos envolvidos na proteção de seu site. Muitas vezes, os certificados não são instalados corretamente, páginas confidenciais permanecem desprotegidas e informações de formulário são publicadas sem criptografia, o que deixa muitos sites vulneráveis a ataques.

É por isso que a Symantec reuniu as dicas a seguir, como uma orientação para que você siga o processo certo desde o início. A finalidade é conduzir você pelos percursos mais difíceis e alertá-lo sobre práticas e procedimentos inadequados que podem enfraquecer o SSL, porque seu certificado SSL é o passaporte para um site mais seguro para você, seus funcionários e seus clientes.

Só existe um jeito de instalar o SSL: o jeito certo!

Como ocorre com várias outras organizações, você reconheceu a necessidade de adquirir um certificado SSL e seguiu adiante com esse importante passo. Agora, você precisa garantir que ele seja instalado corretamente. Se seus clientes não se sentirem totalmente seguros em seu site, eles simplesmente não farão negócios com você.





DICA 1 - Prepare a chave privada e a CSR



Para instalar um certificado digital, primeiro você deve gerar a chave privada e a Solicitação de assinatura de certificado (CSR) a partir dessa chave para o servidor onde o certificado será instalado. Em seguida, você envia a CSR para inscrever-se para um certificado. Veja como fazer isso abaixo.

Se tiver servidores IIS 6 e posteriores ou servidores Redhat Linux, você poderá fazer download de nossa ferramenta [Symantec SSL Assistant](#) e seguir os prompts fáceis de entender. Para ver uma lista de instruções de geração de CSR em outros servidores, consulte [Symantec CSR Generation](#). Para se inscrever em qualquer serviço de Certificados SSL da Symantec, você precisa das seguintes informações:

- O prazo ou período de validade do certificado (1, 2 ou 3 anos)
- O número de servidores que hospedam um único domínio (até 5 servidores)
- A plataforma do servidor
- A organização, unidade organizacional e endereço
- Informações de pagamento e um contato para faturamento
- O nome comum. Esse é o host + nome de domínio, como “www.meudominio.com” ou “webmail.meudominio.com”
- Um endereço de e-mail no qual a Symantec possa entrar em contato para validar as informações
- Uma Solicitação de assinatura de certificado (CSR) gerada a partir do servidor que você precisa proteger

Em seguida, após receber seu certificado, siga as instruções da dica 3.

Se seu servidor não estiver listado ou se precisar de informações adicionais, consulte a documentação de seu servidor ou entre em contato com o fornecedor do servidor. Se não souber qual software seu servidor usa, entre em contato com os administradores de TI.

Durante a inscrição, envie a CSR com o cabeçalho e rodapé:

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

XXXXXXXXXX

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



DICA 2 - Como instalar um certificado SSL – o jeito certo!



Está prestes a instalar um certificado SSL pela primeira vez e se sente um pouco intimidado? Não precisa se preocupar: é muito mais fácil do que você pensa. Vamos dar uma olhada em como instalar um certificado em um servidor com a Symantec.

Todos os servidores seguem a mesma lógica:

Etapa 1 – Salvar o certificado

Siga as instruções do e-mail de confirmação para salvar o certificado SSL em seu desktop a partir do URL fornecido. Com isso, você terá seu certificado e os certificados de CA intermediária de que precisa.

Etapa 2 – Instalar ou mover o certificado para uma pasta de certificados

Etapa 3 – Configurar o certificado no site

Etapa 4 – Referenciar o certificado

[Clique aqui](#) para obter informações detalhadas e instruções passo a passo para cada tipo de servidor.

Para aproveitar seu certificado SSL ao máximo, certifique-se de adicionar o Selo Norton Secured a seu site. Assim seus clientes se sentirão mais seguros quando fizerem transações com você.

Basta copiar e colar as linhas relevantes das páginas do Selo Norton Secured da Symantec para adicionar o selo a seu site. São fornecidas instruções claras no link ao fim desta dica. Também é explicado como testar seu certificado com o Certificate Installation Checker, inserindo-se o domínio quando solicitado.

Agora, seu certificado SSL está instalado e pronto para agir!

Algum problema?

A Symantec tem uma ampla gama de tutoriais em vídeo para diferentes servidores: [Exibir tutoriais](#)

Verifique sua instalação

Basta inserir o URL do servidor a verificar: [Verificar instalação](#)

Gere um selo para seu site

Instruções de instalação do Selo Norton Secured: [Gerar selo](#)

Solução de problemas

Visite o site de Suporte da Symantec: [Acessar suporte](#)



DICA 3 - Proteja suas chaves privadas e escolha as melhores



Chaves públicas e privadas são parte integrante da forma como o SSL funciona. A chave privada é mantida em segredo em seu servidor, sendo usada para criptografar tudo o que está em seu site. A chave pública inserida no certificado é mais uma parte da identidade de seu site, como o nome de seu domínio e os detalhes da organização.

Trate suas chaves privadas como ativos valiosos, compartilhados apenas com o mínimo de funcionários ou colaboradores mais confiáveis. Imagine que você seja o gerente de um banco: você distribuiria as chaves do cofre indiscriminadamente? Não. Veja aqui algumas das dicas mais importantes:

- **Gere chaves privadas em um servidor confiável.** Não designe essa tarefa a terceiros!
- **Proteja as chaves privadas com senha** para evitar qualquer comprometimento quando elas forem armazenadas em sistemas de backup.
- **Renove os certificados todos os anos** – e sempre introduza novas chaves privadas ao mesmo tempo.

O tamanho da chave privada exerce grande influência no “handshake” criptográfico usado para estabelecer conexões seguras. É inseguro usar uma chave curta demais, mas usar uma chave muito longa pode reduzir bastante a velocidade das operações.

A criptografia ECC (Elliptic Curve Cryptography) tem recebido cada vez mais atenção, fornecendo garantias de segurança amplas para tamanhos menores de chave. A Symantec oferece a ECC com tamanhos de chave bem menores do que o número de bits exigido por RSA e DSA, mas é 10.000 vezes mais difícil de quebrar (256 bits para a ECC é a capacidade criptográfica equivalente à RSA de 3072 bits). A ECC oferece segurança mais forte, com sobrecarga de servidor bem mais reduzida, e ajuda a reduzir os ciclos de CPU necessários para operações criptográficas de servidor.

Mais informações sobre a ECC estão disponíveis na página 7.



DICA 4 - Elimine os elos fracos da cadeia



Na maioria das implantações de SSL, é insuficiente usar apenas o certificado de servidor: são necessários três ou mais certificados para estabelecer uma cadeia de confiança completa. Uma cadeia de certificados consiste em todos os certificados necessários para certificar o sujeito identificado pelo certificado final.

Na prática, essa cadeia inclui o certificado da entidade final, os certificados da CA intermediária e o certificado da CA raiz.

O processo de verificação da autenticidade e validade de um certificado recém recebido envolve verificar todos os certificados da CA raiz universalmente confiável, por meio de quaisquer CAs intermediárias, até o certificado recebido – o certificado de entidade final. Um certificado só pode ser confiável se cada certificado de sua cadeia tiver sido emitido e validado adequadamente.

Um problema comum é configurar o certificado de entidade final corretamente mas esquecer de incluir os certificados da CA intermediária. Para verificar se os certificados intermediários estão instalados corretamente, use nosso [verificador de certificados](#).



DICA 5 - RSA, ECC e por que o tamanho da chave importa



A criptografia ECC (Elliptic Curve Cryptography) oferece à sua empresa segurança aprimorada e melhor desempenho do que a criptografia atual.

A ECC, um método de criptografia endossado pela NSA (agência de segurança nacional dos EUA) e aprovado pelo governo americano, cria chaves de criptografia com base na ideia de usar pontos em uma curva elíptica para definir o par de chaves pública/privada. É difícil violar a ECC com os métodos de força bruta normalmente empregados por hackers, e ela oferece uma solução mais rápida que exige menos potência de computação do que a criptografia baseada em RSA.

A RSA é um algoritmo de criptografia e assinatura digital que forma a base da segurança na Internet há quase duas décadas. O uso desse algoritmo ainda é válido, mas o tamanho de chave mínimo aceitável aumentou com o tempo para garantir a proteção contra ataques criptográficos aperfeiçoados. Portanto, com a ECC você obtém melhor desempenho, porque ela exige um tamanho de chave menor e fornece um nível de segurança superior. Por exemplo, uma chave ECC de 256 bits fornece o mesmo nível de proteção que uma chave RSA de 3072 bits. O resultado? Você obtém exatamente a segurança de que precisa, sem sacrificar o desempenho.

Além disso, o tamanho menor da chave ECC significa que certificados menores consomem menos largura de banda. Conforme mais de seus clientes adotam dispositivos menores em suas transações online, a ECC oferece uma experiência de cliente completa melhor.

As raízes ECC da Symantec estão disponíveis nos três principais navegadores desde 2007. Isso significa que os certificados ECC da Symantec funcionarão em sua infraestrutura existente desde que sejam usados navegadores recentes, que podem ser obtidos sem custo adicional.

Saiba mais sobre [ECC e agilidade de algoritmos](#).



DICA 6 - O abrangente Always On SSL



Você deve sempre planejar criptografar todo o seu site com SSL, e a maneira de fazer isso é usar o Always On SSL. Essa é uma medida de segurança econômica para sites que ajuda a proteger toda a experiência do usuário, do início ao fim, tornando mais seguro pesquisar, compartilhar e comprar online.

Empresas realmente preocupadas com a proteção dos clientes e de sua reputação comercial precisam implementar o Always On SSL com certificados SSL de uma autoridade de certificação confiável, como a Symantec. O Always On SSL é fácil de implementar, fornecendo autenticação da identidade do site e criptografando todas as informações compartilhadas entre o site e um usuário (incluindo todos os cookies trocados), protegendo os dados de visualização, modificação ou uso não autorizados.

É importante notar que a Online Trust Alliance está convocando os sites para que adotem o Always On SSL. Ela recomenda: “O Always On SSL é uma medida de segurança prática e comprovada que deve ser implementada em todos os sites onde os usuários compartilhem ou visualizem informações confidenciais”.

Muitos dos sites mais prósperos do mundo reconheceram a sabedoria de implementar o Always On SSL com sucesso, garantindo sua proteção contra “sidejacking” e invasões por meio de ameaças como Firesheep e injeção de código mal-intencionado.

O Always On SSL pode ajudar você a proteger a confiança que os usuários investiram em seu site, garantindo-lhes que você leva a segurança e a privacidade deles a sério e que toma todos os cuidados possíveis para protegê-los online.



DICA 7 - Pinning de chave pública: uma questão de confiança



O pinning de chave pública (mais conhecido como Public Key Pinning Extension for HTTP) foi desenvolvido para fornecer aos operadores de sites a capacidade de restringir as autoridades de certificação que podem emitir certificados para seus servidores.

Basicamente, o pinning de chave pública associa um host à chave pública ou ao certificado esperado. Depois que uma chave pública torna-se conhecida ou é vista para um host, ela fica associada ou “presa” a esse host.

De acordo com o CA Security Council, o pinning de chave pública permite que o proprietário do site declare que seu certificado SSL precisa ter uma ou mais destas características:

- Uma chave pública especificada
- Assinado por uma CA com essa chave pública
- Confiança hierárquica para uma CA com essa chave pública

Se um certificado para o domínio do proprietário do site for emitido por uma CA que não esteja listada (ou seja, sem pinning), um navegador compatível com o pinning de chave pública apresentará um aviso de segurança. Os proprietários de sites também podem fazer o pinning de várias chaves de várias CAs, e todas serão tratadas como válidas pelos navegadores.

O proprietário do site confia que as CAs escolhidas não emitirão um certificado para o domínio do proprietário por engano. Essas CAs normalmente restringem quem pode solicitar a emissão de um certificado para os domínios específicos do proprietário, o que fornece segurança adicional contra a emissão incorreta de certificados para pessoas não autorizadas.

Infelizmente, o CA Security Council afirma que o pinning de chaves públicas que o Google implementou em 2011 não é escalável, já que exige que as chaves públicas de cada domínio sejam adicionadas ao navegador. Uma nova solução escalável de pinning de chaves públicas está sendo documentada por um RFC (Solicitação de comentários) proposto pelo IETF (Internet Engineering Task Force).

Nessa proposta, os pins de chave pública serão definidos por um cabeçalho HTTP do servidor ao navegador. As opções de cabeçalho podem conter um algoritmo de chave SHA-1 e/ou SHA-256, a idade máxima do pin, a existência de suporte para subdomínios e o rigor do pinning, entre outros.



DICA 8 - Espante os interceptadores com o Perfect Forward Secrecy



Você ficaria satisfeito em pensar que um interceptador ocupado em registrar o seu tráfego hoje possa ser capaz de descriptografá-lo no futuro? É claro que não. Apesar disso, essa pode ser a situação da sua organização, embora ela esteja totalmente inconsciente desse perigo.

Pense na criptografia RSA, por exemplo. Ela gera um par de chave pública e privada a fim de criptografar e decodificar mensagens. Porém, o uso contínuo de chaves recuperáveis pode permitir o acesso aos dados criptografados armazenados, caso as chaves sejam comprometidas no futuro. Em muitos casos, um invasor com sua chave privada e o tráfego SSL salvo pode usar a chave privada para descriptografar todas as chaves de sessão negociadas durante handshakes SSL salvos e depois descriptografar todos os dados de sessões salvas usando essas chaves de sessão. É um cenário que não traz muita tranquilidade. No entanto, existe uma maneira melhor: seu nome é Perfect Forward Secrecy.

Quando você usa essa solução, chaves de sessão temporária não recuperáveis são geradas, usadas e descartadas. Além disso, o PFS, quando implementado corretamente com a criptografia ECC (Elliptical Curve – veja a Dica 5), é mais seguro do que algoritmos RSA e tem desempenho melhor.

Usando-se o PFS, não há vínculo entre a chave privada do servidor e cada chave de sessão. Se tanto o cliente como o servidor forem compatíveis com PFS, eles usarão uma variante do protocolo Diffie-Hellman (os nomes de seus criadores), na qual ambos os lados trocam números aleatórios de forma segura e chegam ao mesmo segredo compartilhado. É um algoritmo inteligente que impede um interceptador de originar o mesmo segredo, mesmo se ele puder visualizar todo o tráfego.

Para obter mais detalhes, veja este infográfico da Symantec:
[Visualizar infográfico](#)



DICA 9 - HSTS (HTTP Strict Transport Security): sua rede de segurança



É essencial manter-se ultrasseguro online. E, às vezes, isso significa ir um pouco além – além da segurança padrão – para chegar aonde você quer estar.

Hackers podem utilizar ataques man-in-the-middle, em redes sem fio, como stripping de SSL para interceptar solicitações de navegador para sites HTTPS e enviar as páginas solicitadas por HTTP. Isso significa que a conexão não está mais criptografada, e o hacker pode interceptar informações fornecidas pela vítima no site supostamente seguro. A vítima pode nem perceber a alteração, já que não presta muita atenção à barra de endereço do navegador sempre que navega para uma nova página do site. Os navegadores não têm como saber se um site deve ser fornecido com segurança, e por isso não alertam o visitante quando um site é carregado em uma conexão não criptografada.

O HSTS (HTTP Strict Transport Security) impede que isso aconteça, permitindo que os servidores enviem uma mensagem ao navegador exigindo que essa conexão seja criptografada. Em seguida, os navegadores seguem as instruções da mensagem, de forma que cada página visitada por seu cliente seja criptografada conforme determinado. Isso protege você e seus clientes contra ataques.

Para ativar a proteção HSTS, você define um único cabeçalho de resposta em seus sites. Depois, os navegadores com suporte para HSTS (por exemplo, Chromium, Google Chrome, Firefox, Opera e Safari) seguirão as suas instruções. Após a ativação, o HSTS não permite a comunicação desprotegida com seu site. Para isso, ele converte automaticamente todos os links de texto puro para um formato seguro.

O Internet Explorer ainda não tem suporte para HSTS, mas a Microsoft informou que isso ocorrerá no Internet Explorer 12.

© 2015 Symantec Corporation. Todos os direitos reservados. Symantec, o logotipo da Symantec, o logotipo circular com a marca de verificação e o logotipo do Norton Secured são marcas comerciais ou registradas da Symantec Corporation ou de suas afiliadas nos Estados Unidos e em outros países. Outros nomes podem ser marcas comerciais dos respectivos proprietários.