Redmond

THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

Certificates Help Ensure Data Security on the Ever-Changing Internet

There's no substitute for caution when it comes to data security, but SSL certificates and other tools can help organizations prevent data breaches.

1105 MEDIA

Not all SSL certificates are the same.

We have the Internet's most trusted mark.

Symantec™ Website Security Solutions include industry-leading SSL, certificate management, vulnerability assessment and malware scanning, Express Renewal, and 24x7 support. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe to search, to browse, and to buy. With 100 percent uptime since 2004, military-grade data centers, and industry-leading SSL, Symantec is the leading provider of website security for your business. Call (866) 893-6565 or visit www.symantec.com/ssl-certificates to learn more about Symantec Website Security Solutions.

Confidence in a connected world. Symantec™

Certificates Help Ensure Data Security on the Ever-Changing Internet

BY DEREK SCHAULAND

The Internet is a place where almost any business can be conducted: sales transactions, retail and shopping, banking, and many other things (including email and social media). With all of the recent data breaches putting consumer information at risk, including a large and very public breach at Target, security has become a top priority for many organizations. With more and more companies taking transactions online to increase sales and potentially reduce the need for data entry professionals to keep up with new demand, keeping information secure and being extremely

confident that your company will be less likely to experience a breach is paramount. Sure, there is no way to guarantee 100 percent that an organization will never experience a data breach (unless no online transactions happen and/or there is little to no data storage), but being reasonably sure certainly helps.

One way to improve security for online transactions is to rely on certificates of all kinds to ensure that customer data is kept safe. Providing additional security through certificates and extended validation will give consumers peace of mind when visiting many organizations' Internet sites. Without additional security, the data breaches will surely continue and, as the attacks become more sophisticated, they will become much harder to stop.

One way to improve security for online transactions is to rely on certificates of all kinds to ensure that customer data is kept safe.

What can IT do to protect information sent across the Internet?

Much of the security that is needed to keep information safe online is simply the result of diligence on the part of the consumer or Internet user. SSL certificates are helpful and will help keep your information safe when shopping online, but being aware of your online surroundings and keeping your system patched on all fronts will help, too. Ensure that all of the computers you use have active antivirus solutions as well as anti-malware software to prevent infections or applications from running on your systems that may be looking to capture your information. These applications can be devastating if they are not detected and diligently monitored.

Many times, when a data breach occurs, the online transactions and information exchanges are considered to be at fault because of the possibilities of infection or other problems on the incoming machines. However, as technology grows and evolves, being available on so many devices, it becomes more likely that technologies looking to capture this information may be found on point-of-sale devices and terminals, even in those companies within brick- and-mortar stores.

What is an SSL certificate and how does it protect information?

An SSL certificate is a file used to create a secure connection between a server and a client. Typical places SSL certificates are used are on webservers where e-commerce transactions happen and

on e-mail servers. Using them provides assurance to the client that the connection to this site can be trusted. When a web browser comes across a site that is using SSL security, it requests the identity of the web server. The server provides this identification with a copy of the SSL certificate. The browser checks its certificate store to see if this certificate is trusted; if so, a message is returned to the web server. In response, the server sends a signed acknowledgement to the browser to begin the SSL encrypted session.

The steps needed to ensure the security of the session mentioned above happen very quickly and are most likely unnoticeable to the browsing user.

Using SSL Certificates provides assurance to the client that the connection to this site can be trusted.

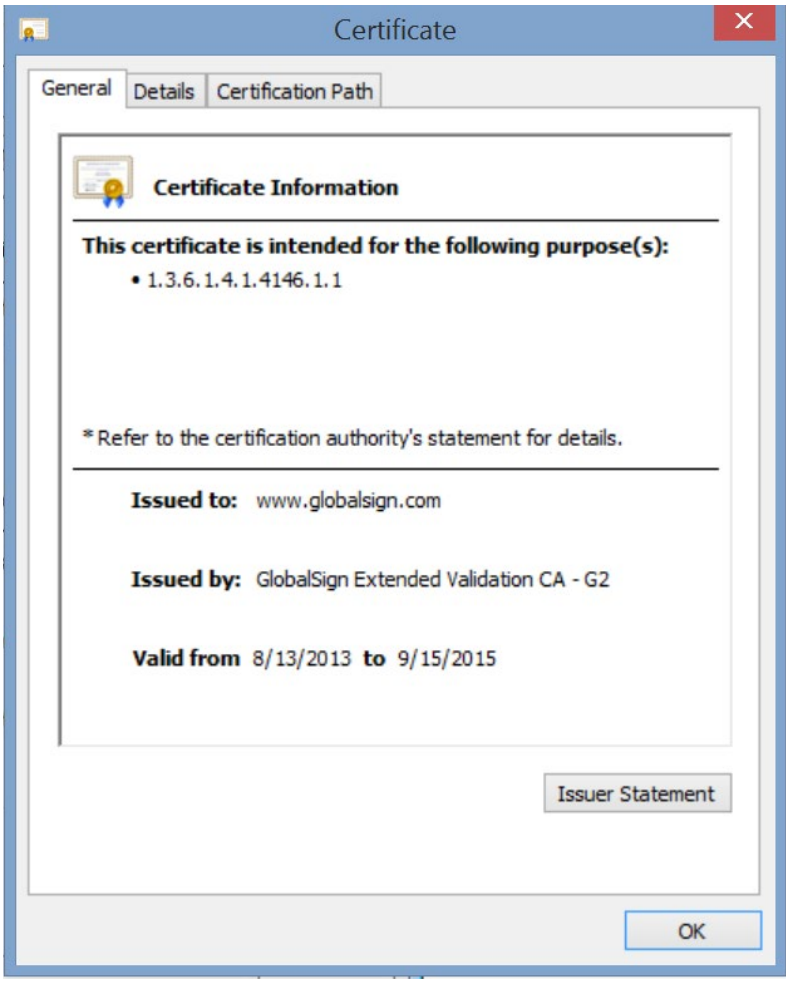

Figure A: *Reviewing Certificate Details*

What does an SSL certificate cost?

The cost of an SSL certificate varies by vendor and by the number of years the certificate is purchased for; on average, the cost of an extended validation SSL certificate is just a bit less than twice the cost of a standard SSL certificate. Generally, the functionality of the certificates is the same regardless of vendor. It might be wise to consider several vendors and several years of certificates for each purchase. Multiple-year purchases can bring the annual cost down considerably. Check with your certificate vendor if you have one, or with your security or your anti-virus provider.

SSL and Extended Validation

Extended validation is an enhanced (or more secure) standard of certificate.

Extended validation is an enhanced (or more secure) standard of certificate. The process for obtaining and verifying the identity of a server just to get one of these certificates is much more rigorous than with traditional SSL certificates. Extended validation helps companies further boost their patrons' confidence. Extended validation's criteria are defined by the CA/Browser Forum, a voluntary collection of software and Internet security vendors as well as other technology organizations. It is much more rigorous than identification validation for standard SSL certificates.

EV support first appeared in Internet Explorer 7, Mozilla Firefox 3, and other browsers that have been around for quite some time. All modern versions of major browsers as well as their mobile counterparts are EV compatible. In addition, all web servers that support SSL v3 support EV certificates.

For example, when a shopping site is using an extended validation certificate, the address bar will be green, as shown in **Figure B**.

Other benefits of EV include:

- Higher levels of encryption than standard SSL certificates
- Multiple encryption algorithm support
- Image displaying that a website has been secured with an EV SSL certificate
- Display of organization's name in address bar to affirm identity

Figure B: *EV certified website with a green address bar*

Depending on the provider of the EV SSL certificate, other features or different variations of those mentioned above may be available. While generally an EV certificate is an x.509 certificate, as is a standard SSL certificate, the EV certificate policies field contains a different object identifier for each SSL provider.

Remember that, like any root certificate, some browsers may not recognize all EV certificates.

Merchants should ensure their sites are using certificates to help keep customers coming back.

How does this prevent data breaches like those recently in the news?

Certificates, both SSL and EV SSL, can be helpful in preventing data breaches by keeping customer data safe when it gets transmitted to sites, but they are not the only piece of the puzzle. Being vigilant about your information online also helps ensure the security of information passed to sites on the Internet. Merchants should ensure their sites are using certificates to help keep customers coming back. They should also take it upon themselves to educate their customers (both potential and existing) and make as much information as possible about security and how data is handled available. This will help keep good faith among site visitors and customers alike and help spread overall understanding of SSL security. Additionally, transparency about the security a site is implementing can speak volumes about how customer data is being protected and managed.

Are there any shortcomings when using certificates?

More and more sites are implementing certificates to ensure visitors that their information will be safe. Certificate vendors are working with both merchants and technology firms to make sure that the latest in security is available, helping to ensure that their clients are as safe as they can be. Remember, though, being diligent when visiting merchants or other sites is the best security. Being aware of a site's use of certificates before providing any information can make sure your data stays safe.

Should I be considering certificates for other things?

While the widest reach for certificates is likely in the SSL/online merchant space, there are plenty of other places that use certificates

to validate identity. For programmers, code signing certificates can be used to ensure that software or files created have not been tampered with. Some organizations use certificates to verify the identity of users logging into a website, application, or computer system. Many times, when an organization provides a badge for its employees, the badge contains a smart card featuring a certificate to provide access to corporate resources and even buildings. All of these certificate types help keep information secure for organizations, their employees, and the consumers they serve.

Internet security is extremely important and should be considered anytime information is exchanged online. As in many other cases where you might provide personal information, extreme care should be taken when passing your information between sites on the Internet.

Certificates are only part of the solution when it comes to information security.

The certificate is only part of the solution for secure data

Certificates are only part of the solution when it comes to information security. Being careless with the specific information I share on the Internet is a different problem entirely. Remember that even connections to sites that make information available publicly (Facebook or Twitter, for example) can be secured by certificates. This does not mean the information being transacted is not publicly visible once sent by its owner. In that case, the certificate encryption definitely benefits the site rather than the user. R

Derek Schauland has worked in technology for 15 years in everything from a help desk role to Windows systems administration. He has also worked as a freelance writer for the past 10 years. He can be reached at derek@derekschauland.com.