Volume 01 January 2009

This Issue

New DigiCert Customers

Fed. Housing Finance Board
The Kroger Company
City of Las Vegas
Penn State University
CarMax
Northrop Grumman
Learn.com, Inc.

DigiCert Expands Support Knowledgebase:

DigiCert has expanded its CSR Creation and Certificate Installation support pages to include a greater variety of new and old server platforms.

Some notable server types that have been added include:

- Cobalt RAQ & XTR
- Nginx
- Novell IChain
- Webstar
- Zeus

DigiCert continues to look for opportunities to provide outstanding support documentation for all available server platforms.

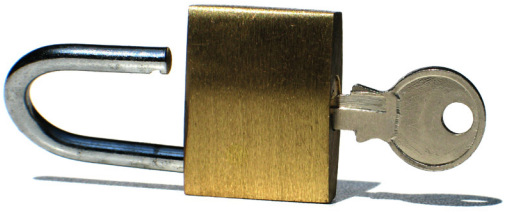
Please let us know if there are other devices that need instructions by sending an email to support@digicert.com.

digicert®
Your Success is Built on Trust™

DigiCert Unaffected by MD5 Vulnerability

On December 30, 2008 a group of security researchers reported that by exploiting a known weakness in the MD5 hashing algorithm, they were able to create a rogue intermediate CA certificate under the "Equifax Secure Global eBusiness CA-1" root certificate, belonging to GeoTrust's RapidSSL brand.

By creating a Rogue Certificate Authority, these researchers were able to issue trusted SSL certificates with any name of their choosing.



Netcraft, an Internet consultancy company founded in 1988, reported the following figures on certificates using the MD5 hashing algorithm:

"Netcraft's December 2008 SSL Survey found 135,000 valid third party certificates using MD5 signatures on public web sites, which is around 14% of the total number of valid SSL certificates in use."

Because all certificates issued by DigiCert use the SHA-1 hashing algorithm, we are happy to reassure all our past, present, and future customers that these findings do not present any reason for them to worry about the integrity of their DigiCert SSL certificates.

The fact that DigiCert uses SHA-1 instead of the outdated MD5, along with various other internal controls, makes the attack by the MD5 researchers impossible on DigiCert's systems.

The recent findings also highlight the problems inherent in the practice of issuing domain validated certificates, which can be issued automatically, with no human element in the verification process. Though frequently the companies that issue these "rapid," "instant," "low assurance," or "automated" certificates tout the speed with which SSL certificates can be issued, these certificates provide no assurance that the certificate belongs to a real company.

To protect our customers, DigiCert issues only organization-validated, high assurance SSL certificates. This, in addition to other security practices, helps to prevent phishing and other abuses.

For more information, call us toll free (Canada or US) at 1-800-896-7973 (International Customers please call us at +1-801-877-2100).

Visit us online at www.digicert.com (24-hour Live Chat service provided).

DigiCert Site Seal

The DigiCert site seal is a recognized symbol of trust and security. This trust mark prominently verifies that your organization's page is secure and can be a powerful force in increasing conversion and visitor assurance.

When a visitor clicks on the seal, a pop up page hosted on digicert.com verifies that the site is secured using DigiCert's services, and that your organization has passed our strong validation standards.

By providing an external, third-party verification of your organization, your site visitors can receive the extra assurance they need to complete their online transactions.

The DigiCert Site Seal is included with every certificate purchase. It can be accessed by logging in to your DigiCert account, clicking on your order number, and selecting "Get Site Seal."

Learn more about DigiCert SSL Services

Choosing the Right SSL Certificate

Which is the best for your needs?

By: Travis Tidball, Director of Customer Relations

SSL certificates play a huge role in not only protecting your organization's sensitive information, but relaying confidence to those that use its services. Your success is built on trust, and after selecting a trusted provider such as DigiCert, which SSL certificate should you choose?

There are four types of SSL certificates that offer a varying level of options depending on your organization's needs: Extended Validation, WildCard Plus, Unified Communications, and SSL Plus.

Instances needing the highest level of assurance (your site visitors need to know that your site is the real deal) such as shopping carts, login pages, or account pages are best served by Extended Validation SSL certificates. These certificates show that your site is secure by enabling the green URL bar in your client's browser window, proving that the site is in fact owned by your organization, and that their information is safely encrypted.

When you need to secure different subdomains such as mail.example.com, staging.example.com, or admin.example.com, you might want to consider WildCard certificates. They can provide the best value by enabling encryption for an unlimited number of subdomains.

You might have a situation that requires you to secure different domain names with a single certificate. For example, Microsoft's Exchange 2007 required a certificate to secure both the internal server name and the external fully qualified domain name. In this case, our Unified Communications certificate is the best choice. It will allow you to secure up to 150 different names (external, internal, and IP addresses) with a single certificate.

The SSL Plus certificate might the best option when you are sure that none of the previously mentioned enhancements are needed.

Of course, all of our SSL certificates come with many standard features. If you're not sure what SSL certificate you need from reading the descriptions, please call or email us and let us help you decide.

Call us toll free (Canada or US) at 1-800-896-7973 (International Customers please call us at +1-801-877-2100).

Visit us online at www.digicert.com (24-hour Live Chat service provided).

Standing Out from the Crowd

What makes DigiCert EV different?

By: Travis Tidball, Director of Customer Relations

The guidelines for issuing an Extended Validation (EV) SSL certificate are defined by the Certificate Authority / Browser Forum (CA/B Forum, http://www.cabforum.org). In order to issue an EV SSL certificate, all Certificate Authority must abide by the same verification requirements.

Although all Certificate Authorities must follow the same procedures for EV, not all Certificate Authorities are equal.

Besides having one of the fastest issuance times and lowest prices for Extended Validation certificates, DigiCert enhances each one with a number of benefits that make them truly unique amidst the similar offerings from other Certificate Authorities.

Each DigiCert Extended Validation certificate includes our "Plus" feature, which allows it to work with or without the www (both example.com and www.example.com).

DigiCert EV certificates come with an unlimited server license, free reissues, and unlimited support via phone, email, or live chat 24 hours each business day.

These features not only make DigiCert stand out from the crowd, but are also what makes us the "Best Value in SSL."

Positive Feedback:

By: Travis Tidball, Director of Customer Relations

It's always a great thing to see the feedback we receive from our customers. DigiCert has had a lot of positive attention from blogs and review sites such as sslshopper.com. We just wanted to take a moment and say thanks to you, our customer.

We work our hardest to provide superior certificate services at an outstanding price. We believe that being a responsible company means standing behind your product as well, which is why DigiCert offers free 24-hour support for the lifetime of our certificates.

Our sales representatives also handle support cases, making a unique combination of individuals that can walk you through ordering to implementation.

For all of those who have taken the time to write about their experiences with DigiCert, we want to express our sincerest thanks and appreciation.

It is because of you that we have continued to grow at an unprecedented rate. We look forward to finding new ways to surprise and astound our customers.

Thanks for choosing DigiCert.

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com