Volume 01 September 2008

This Issue

New DigiCert Customers

Facebook
BMW
United Parcel Service
Nintendo
Harvard University
Yale University
United Nations

DigiCert completes 2008 WebTrust & WebTrust EV Audits:

DigiCert has met or exceeded all WebTrust requirements, as audited by KPMG LLP, for issuing standard and Extended Validation (EV) certificates based on the standards established by WebTrust for Certification Authorities and the CA/Browser Forum.

DigiCert assisted in establishing the higher standards for EV by working with internet leaders such as Microsoft, Mozilla, and Opera as an active member of the CA/Browser Forum- http://www.cabforum.org/forum.html

Click for more information

digicert®
Your Success is Built on Trust™

What's New

DigiCert unveils new site based on customer feedback

You may have noticed something new when you visited digicert.com recently. DigiCert released a new site design on August 1st based on feedback from customers, employees, test clients, friends, graphic design artists, and many others.

Ultimately, we sought for our new design to improve our levels of service and support by enhancing the overall online experience.

CEO & President Ken Bretschneider said, *"I wanted the new site to reflect our foundation of exceptional value, enhanced customer service, and constant improvement."*

DigiCert's new focus on enhanced user functionality is a result of feedback from our customers. For example, the site's front page now includes a "Shop by…" section, to help customers identify which certificate is best for their unique situations.

We also updated several of our support pages and designed a new set of tools, including our Easy CSR Generators for Exchange 2007 and OpenSSL, as well as our Certificate Testing Tool to verify proper installation of certificates.

Although our objective is to provide a better online experience for our customers, we realize that nothing replaces direct assistance from an experienced live support specialist. DigiCert is committed to having the best support in our industry.

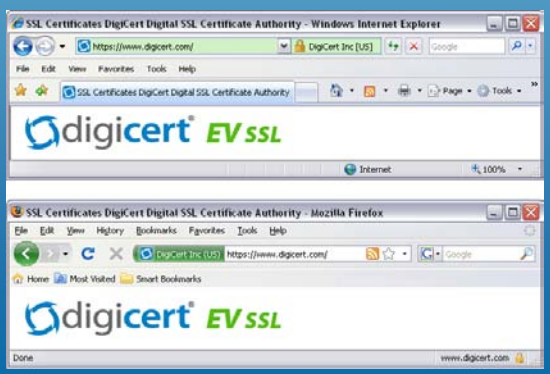
Call us toll free (Canada or US) at 1-800-896-7973 (International Customers please call us at +1-801-877-2100). Visit us online at www.digicert.com (24-hour Live Chat service provided).

Extended Validation Certificates

The new industry standard for SSL authentication

Extended Validation (EV) is the new industry standard for SSL Certificates. EV SSL enables a green URL bar in your client's browser to clearly identify your organization and website as a real and authentic source (currently available in IE7, FireFox 3, and Opera).

EV certificates offer real value by enhancing your end user's trust. Studies show that conversion rates for sites enabled with an EV certificate are significantly higher than those without.



This enhanced trust is backed by unprecedented validation procedures designed to provide the highest assurance to your customers/end-users that you and your website are authentic (the real deal).

EV SSL also provides an effective measure to help reduce phishing fraud by making it more difficult to replicate your online presence.

Learn more about EV Certificates

Industry Issues

The Debian dust has settled – what now?

By Paul Tiemann, CTO

Three months ago in May, users of Debian Linux faced a terrible security flaw. Debian systems had been generating predictable random numbers for the past 20 months. Every SSH key and SSL certificate created since September 2006 would need to be replaced.

All DigiCert certificates can be reissued free of charge for the life of the certificate, and many of our customers proactively replaced their certificates even before we began sending emails. However, in mid-June, it became apparent that some customers were still submitting certificate signing requests (CSRs) with weak keys. We built weak key detection into our ordering systems to reject weak CSRs and alert our customers when a weak key is used.

DigiCert also built weak key detection into its custom Certificate Testing Tool available here: www.digicert.com/help/. If you are not sure whether you have a web site with a vulnerable SSL certificate, our testing tool will tell you.

Since the discovery of this issue, DigiCert has identified any certificates that could have been issued with a weak key. We made an active effort to alert each of our affected customers. We sent out three mass emailings, one each in June, July, and August, and followed up with personal emails and phone calls to customers who were most affected (some had multiple vulnerable certificates.)

"We made an active effort to alert each of our affected customers"

We wish to express appreciation for the prompt response and efforts of those that were affected by the Debian issue.

Because of these proactive measures, we can say with certainty that DigiCert certificates remain strong amidst this troubling situation.

Upcoming Items

New Features Will Make Your Job Easier

Even though we just finished a major site redesign, there are still more exciting updates to look forward to in the coming months. Some of these items include:

- **Quote Generator**
  Automatically generate quotes online! You will no longer need to contact a DigiCert Representative for a quote. Just do it online!
- **New Account Area**
  Advanced Certificate Management Tools! DigiCert is currently developing enhanced management features for your certificates. Stay posted for more updates.
- **Customer Referral Program**
  Earn rewards while saving money for your friends!

These new features are just the start of our continued efforts to be the best value in SSL!

Protecting your Private Key:

By Flavio Martins, Director of Support and Validation

The private key to which your SSL certificate is issued is the lifeline to your secure Web or Mail server. If the key gets into the wrong hands, your server's secure site is vulnerable.

Securing the private key is one of the more important things that you can do to ensure that you have a trusted SSL-enabled site.

The private key is generated when you create your Certificate Signing Request.

Certain server platforms create a password protected private key or keystore. Remember that a strong password is one that is lengthy and utilizes a combination of letters, numbers, and symbols.

You can also ensure security by hardening access to your server. A combination of firewalls, IP address restrictions, client-side certificates, and multiple authentications, is a great way to ensure that access to your server and private key is restricted.

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