Volume 01 December 2008

This Issue

New DigiCert Customers

Amazon.com
Costco
America Online
Deloitte & Touche
Johns Hopkins University
NASA
U.S. Department of State

DigiCert Joins ACE:

DigiCert recently joined as a contributing member of the ACCESS Connect Ecosystem (ACE) program.

ACCESS is a global provider of advanced software technologies to the mobile and beyond-PC markets.

With research and engineering centers throughout the world and a progressive company culture that emphasizes and nurtures innovation and creativity, ACCESS delivers unique solutions that bring vlaue to its customers and partners and which hel make life easier, more productive, and more enjoyable.

ACE
ACCESS Connect Ecosystem

http://www.access-company.com

digicert®
Your Success is Built on Trust™

Making the Switch: EV SSL Certificates

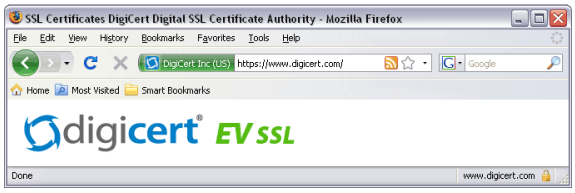
"High Powered Websites Adopt EV: Who's Next?"

Extended Validation SSL certificates, often called EV for short, have been gaining popularity as the new standard for SSL certificates. Introduced in early 2007, Extended Validation was developed by the Certificate Authority (CA) / Browser Forum as a means for combatting online fraud.

Once implemented, these certificates allow the browser to report that the site is not only secure, but that the identity of the online source is verified as well.

As a founding member of the CA/Browser forum, DigiCert has the unique opportunity to help EV SSL certificates take form and grow. To date, EV is now supported by the following browsers:

- Internet Explorer 6 (SP2)+
- FireFox 3+
- Opera 9.5+
- Safari 3.2+
- Chrome 1+



With the most recent additions of Apple's Safari and Google's Chrome, EV certificates are currently supported by all major browsers.

The enhanced focus on security via encryption and identity assurance makes EV certificates an excellent choice for Ecommerce, login pages, and high security situations. Studies show that EV certificates lead to higher conversion rates and increased user trust.

These factors may be reasons that led major sites to make the switch to EV certificates. You may notice a new certificate on Facebook https://www.facebook.com and the Authentication and Online Trust Alliance https://www.aotalliance.org.

DigiCert is driven to provide the best value for Extended Validation SSL certificates. Including an unlimited server license, free lifetime reissues, and free industry-leading support, DigiCert certificates are flexible and compatible with virtually all browsers and devices.

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.

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

PCI Compliance: SSL Requirements

By: Travis Tidball, Director of Customer Relations

Website owners interested in conducting online transactions with Credit or Debit Cards may well be familiar with the PCI (Payment Card Industry) Compliance standard. This standard helps organizations prevent credit card fraud and other security concerns when processing card payment transactions. Although many steps are involved, obtaining a proper SSL certificate is an important part. PCI Standards require the following items:

"Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks.

- Verify that strong encryption is used during data transmission.
- For SSL implementations
  - Verify that the server supports the latest patched versions.
  - Verify that HTTPS appears as part of the browser universal Record Locator (URL)
  - Verify that no cardholder data is required when HTTPS does not appear in the URL.
- Select a sample of transactions as they are received and observe transactions as the occur to verify that cardholder data is encrypted during transit.
- Verify that only trusted SSL/TLS keys/certificates are accepted
- Verify that the proper encryption strength is implemented for the encryption methodology in use."

The full requirements can be found at https://www.pcisecuritystandards.org. As a High Assurance Certificate Authority, all DigiCert SSL certificates meet the requirements for full PCI compliance.

Industry Issues

IRS to require EV for all e-file sites

By: Travis Tidball, Director of Customer Relations

The Internal Revenue Service has issued draft 2 of a requirement for all e-file tax sites to use Extended Validation SSL Certificates beginning January 1st, 2009.

The draft includes the following statement:

"This requirement applies to Authorized IRS e-file Providers participating in Online Filing of individual income tax returns that collect taxpayer information via the Internet. These Providers shall possess a valid and current Extended Validation Secure Socket Layer (SSL) certificate using SSL 3.0 / TLS 1.0 or later, and minimum 1024-bit RSA / 128-bit AES."

The requirement applies to all sites that allow you to file your taxes directly through their site.

Although no formal statement has been made, many speculate this has been implemented to help prevent online tax scams and phishing attacks which have plagued previous tax seasons.

http://www.irs.gov/efile/article/0,,id=186487,00.html

New DigiCert Keytool Command Generator:

By: Travis Tidball, Director of Customer Relations

DigiCert has implemented a new Keytool Command Generator, designed to make the Certificate Signing Request generation process on Tomcat and other Java based applications much simpler.

By going to https://www.digicert.com/easy-csr/keytool.htm, you can access this tool. It will allow you to enter the certificate details (including Common Name, Organization Name, Key Size, etc.).

Once you enter the information and press the "generate" button, the tool will create a full command that only needs to be copied and pasted into keytool. This will create the keystore and accompanying CSR.

Other command generator can be found for OpenSSL https://www.digicert.com/easy-csr/openssl.htm and Exchange 2007 https://www.digicert.com/easy-csr/exchange2007.htm.

DigiCert is often looking for new tools and methods to make SSL certificates easier to work with. Please feel free to write us or give us a call if you have any other tools you would like prepared to make your certificate process easier.

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