01
January
2010

This Issue

digicert®
Your Success is Built on Trust™

Keeping Up With Security Standards

DigiCert Ahead of the Curve

In early January, an international team of computer scientists announced that they had been able to break 768-bit RSA encrypted public keys.

Assuming technological advances continue to progress at their current rate, 1024-bit private keys (those used today by some SSL certificate providers to sign their root certificates) will be able to be cracked in a similar fashion by 2020.

This news represents an impressive feat - a standard desktop computer today would have taken about 1,500 years to achieve similar results - but has been met with little alarm in the security community as a whole.

That is because the news is not unexpected. Responsible Certificate Authorities have already put measures in place to phase out their 1024-bit private key root certificates in exchange for more secure, 2048-bit roots. DigiCert began issuing all multi-year certificates from our 2048-bit root certificate in the beginning of 2009.

As with the recent MD5 vulnerability exploit (the possibility of which was predicted years before anyone was able to actually carry it out), which DigiCert preemptively avoided simply by switching to the more secure SHA-1 algorithm, DigiCert is committed to keeping up with changes in security standards, and always taking the path that will be safest for our clients.

By Bart Mensinger
Senior Manager of Content Optimization

Become a Fan on Facebook

DigiCert is on Facebook! Stay up to date, follow relevant stories, and join the community. Joining the DigiCert fan page is a great way to stay in touch with DigiCert employees and network with others familiar with SSL Certificates and network security.

You can become a fan by clicking on the image to the right or searching for DigiCert's page once logged into your Facebook Account.

Find us on Facebook

Certificate Installation Checker

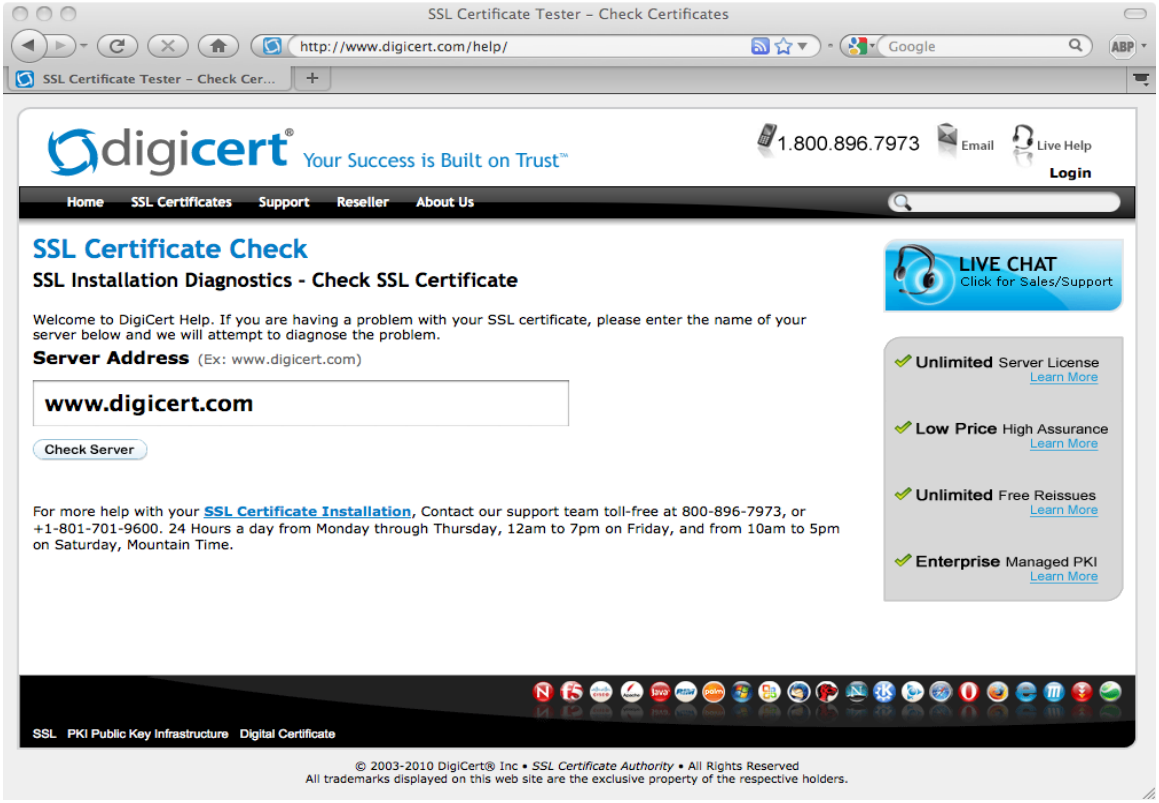
Verify Your Certificate With Ease

By: Travis Tidball, VP of Sales & Marketing

You can test your certificate installation by visiting http://www.digicert.com/help. The certificate checker will verify that:

- Your certificate is properly installed.
- Your certificate does not use MD5 or other weak algorithms.
- The intermediate certificate(s) properly chain your certificate to the trusted root.
- Your certificate has not expired.
- The key associated with your certificate is strong.

The certificate checker works for any publicly available SSL certificate. Just enter the domain name and verify your certificate details!



Details that are properly configured will appear with a green check mark. Areas that are not responding correctly will show a red X and give a brief explanation of the problem.

If you have any questions about your certificate installation (regardless of whether it is a DigiCert certificate), feel free to contact our support team by calling 1-800-896-7973 (international customers please call +1-801-701-9600) or email support@digicert.com. We are happy to help you identify any issues and work to make sure your certificates are operating properly.

Updated Support & Content Pages

By: Travis Tidball, Vice President of Sales & Marketing

DigiCert is always working to expand its support & content pages. Here are some recent additions:

Account Tutorial - Get a quick overview of the DigiCert SSL Certfiicate Account Interface.

DigiCert EV Comparison - How does DigiCert stack up against the competition? Visit the DigiCert EV SSL Comparison site and take a look.

Managed PKI - Are you interested in DigiCert's upcoming Enterprise-grade Managed PKI? Visit this site to read more about it.

Shop by Server - Have questions specific to your certificate type? The Shop by Server section will point you in the right direction and offer helpful tips.

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

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