# DigiCert's SSL Certificates Not Affected by MD5 Collision Attacks

LINDON, Utah, March 3 /PRNewswire/ -- Internet security researchers announced recently that they were able to forge digital certificates signed using the MD5 hashing algorithm. They were able to exploit known flaws in the algorithm in order to create the fake certificates, which could then be used to launch nearly undetectable phishing attacks. Studies show that this security breach could affect approximately 14% of SSL certificates on the Internet.

DigiCert is the leading Certificate Authority (CA) in value and quality of service and an issuer of various kinds of certificates, including Unified Communications, WildCard and Extended Validation (EV) Certificates. Because all of DigiCert's SSL certificates are signed using the SHA-1 algorithm, which is considered to be a cryptographically stronger algorithm than MD5, SSL certificates issued by DigiCert are unaffected by this recently discovered security exploit.

SSL certificates are special computer files that facilitate the encrypted transmission of sensitive information such as credit card details, user names and passwords, and health records. Normally when a website's address begins with https://, it means the information transmitted between the user and the web site will be encrypted using the Secure Sockets Layer (SSL) protocol. The SSL certificate facilitates this unique behavior in browser software and is usually indicated by a padlock symbol or "lock" icon in the frame or "chrome" of the browser. (The lock must appear in the chrome, and not merely somewhere on the page itself.) If the SSL certificate is also an Extended Validation (EV) certificate, it may also be indicated by a green address bar highlighting the web address at the top of the browser.

DigiCert customers and visitors to web sites secured with DigiCert SSL certificates can rest assured that their data is safe during transmission. DigiCert also strongly authenticates organizations who request SSL Certificates. DigiCert checks to see that the company requesting the certificate is a validly formed entity and that the person requesting the certificate is authorized by the organization to receive the certificate. Only after extensive checking on the validity of the entity and the authority of the certificate requester does DigiCert issue an SSL certificate using the SHA-1 algorithm. Even more extensive steps are taken prior to issuing an EV certificate, which provides the green address bar -- a sign of enhanced trust. EV requirements prohibit the use of the MD5 algorithm.

DigiCert issues various kinds of certificates, including Unified Communications, WildCard and Extended Validation Certificates. DigiCert offers a 30-day trial period for all SSL certificate products and provides a full 100% money-back guarantee. All products are backed by DigiCert's industry-leading personalized support service, including step-by-step certificate setup and installation and ongoing support. DigiCert is a WebTrust-Certified Certificate Authority, a member of the CA/Browser Forum, the W3C Consortium, and the Authentication and Online Trust Alliance.

For more information, visit www.digicert.com.

*About DigiCert, Inc.*

*DigiCert, Inc. is a leading provider of enterprise-grade, high-assurance, 256-bit SSL Certificates trusted by many national and state governments, educational and medical institutions, and Fortune 500 companies around the world. DigiCert's commitment to innovation and value provides clients with peace of mind backed by a 100% money-back guarantee and live 24-hour phone, chat and email support, along with intuitive GUI certificate management. Located in Lindon, Utah, DigiCert is a WebTrust Certified Certificate Authority, a member of the CA/Browser Forum, the W3C Consortium, and the Authentication and Online Trust Alliance.*