# News Release

**FOR IMMEDIATE RELEASE**
**CONTACT:**

Judy Kaneko
Symantec Corp.
(408) 203-0014
Judy_Kaneko@symantec.com

Mike Bradshaw
Connect Public Relations
(801) 373-7888
mikeb@connectpr.com

**Symantec's Website Security Solutions Advance the Future of Trust and Protection on the Internet**

*New SSL Algorithms and Web Security Products Prepare Enterprises for the Hyper-Connected Internet and New Encryption Requirements*

**MOUNTAIN VIEW, Calif. – February 13, 2013–** Symantec Corp. (Nasdaq: SYMC) unveiled new updates to its Website Security Solutions portfolio with innovative and comprehensive capabilities to meet the increasing security and performance needs for connected businesses. The WSS strategy focuses on protecting companies, meeting compliance requirements, improving performance and reducing infrastructure costs. The end result is to deliver trusted shopping, trusted advertising and trusted applications for businesses and their customers. The company also announced the first available multi-algorithm SSL certificates with new ECC and DSA options. These offerings will help organizations protect their web eco-systems and strengthen the foundation of trust online.

Read more detailed blog post: Algorithm Agility ECC & DSA Blog

"As companies execute their web strategies, they face increased complexities in protecting their business in a world of Internet-connected things," said Fran Rosch, Vice President Identity and Authentication Services, Symantec. "Website Security Solutions can solve their unique challenges with first-to-market solutions, ECC- and DSA-powered certificates, to secure and accelerate their business."

Click to Tweet: New SSL Algorithms and Web Security Products Prepare Enterprises for the Hyper-Connected Internet: http://bit.ly/V5FNtu

To stay ahead of new and sophisticated cyber threats, the National Institute of Standards and Technology (NIST) recommends all websites to migrate from RSA 1024-bit to 2048-bit certificates by January 1, 2014. Symantec began transitioning customers to its RSA 2048-bit SSL certificates last year. With today's announcement, the company broadens its SSL portfolio with new security algorithms to address this requirement with increased protection and performance.

**ECC Algorithms Faster and Stronger**

Symantec is the first CA to offer commercially available SSL certificates using **Elliptic Curve Cryptography** (ECC) and **Digital Signature Algorithm** (DSA). ECC is currently scheduled to be available in Symantec™ Managed PKI for SSL first half of 2013. Based on internal testing[1], ECC advancements deliver the following advantages:

- Greater security as Symantec ECC will be 10,000 times harder to break than an RSA 2048-bit key based on industry computation methods. Symantec 256-bit ECC certificates offer the equivalent security of a 3072-bit RSA certificate.

- Improved server performance during peak loads with the ability to process more requests per second with lower CPU utilization, which becomes more important as mobile and tablet adoption place increasing demands on web infrastructure.

- Improved server-to-desktop performance and response time. Internal testing showed a server with an RSA certificate handled 450 requests per second with an average response time of 150 milliseconds to the desktop clients. The server with an ECC certificate under the same conditions netted an average response of just 75 milliseconds.

ECC delivers higher scalability to handle the demands of online interactions across billions of connected endpoints, enabling organizations to make greater gains in their online information sharing, cloud services and global ecommerce initiatives. For end users, improved computational performance and enhanced infrastructure utilization increase their overall productivity for a more favorable experience.

**Industry-leading Companies Partner with Symantec to Accelerate ECC Adoption**

Symantec has partnered with industry-leading web hosting companies, service providers and browsers to integrate ECC into their IT environments, including Akamai, Citrix, F5, Google, HID Global, Juniper Networks, Opera and Red Hat.

"The future is going to necessitate increasingly higher security cryptography and Akamai sees ECC as a technology that will allow cloud platforms to scale to meet those security demands without the crippling complexity of today's common algorithms," explained Stephen Ludin, chief architect, Akamai Technologies. "It is a significant step forward to better protect our data online in this hyper-connected world. As the Certificate Authority ecosystem for ECC gets ready, we will be building support into the Akamai Intelligent Platform."

"Juniper's SSL VPN solution, #1 in the world market, supports both ECC and DSA algorithms for added security and flexibility. The Junos Pulse SSL VPN client and gateway software are both FIPS compliant," said

[1] Preliminary testing results conducted by Symantec research and development, January 2013

Michael Callahan, VP of product marketing, Juniper Networks. "We are fully committed to and continue to invest in standards-based security solutions, including the strictest of NIST Suite B standards for our customers, across federal, enterprise and service provider markets."

"F5 helps customers seamlessly combine industry-leading traffic management with security and access solutions, including VPN and SSL encryption capabilities," said Jason Needham, VP of Product Management and Product Marketing, F5 Networks. "One of the primary goals is to give organizations more choice and flexibility in deploying technologies to suit their business needs. F5 is proud to team up with leaders like Symantec to help enterprises and service providers enhance web and mobile security while scaling to better support cloud and BYOD initiatives."

**DSA Algorithm Meets U. S. Government Security Requirements**

Symantec adds another algorithm to its portfolio by introducing **Digital Signature Algorithm** (DSA), an additional 2048-bit encryption technology, which is now available in Symantec Managed PKI for SSL solution. DSA delivers the high security and performance to comply with U.S. government standards and allow market access. ECC and DSA are approved by the U.S. government and endorsed by the National Security Agency to meet their protection and compliance requirements.

**Recover Costs and Eliminate Expensive Downtime with Powerful New SSL Management Services**

The difficulties and complexities, in tracking SSL certificates and staying compliant, increase in tandem with the diversity of networks in large enterprises. A recent Symantec SSL global customer survey[2] of companies using more than 2,000 SSL certificates, reported an average loss of $222,000 last year due to unexpected certificate expiration, rogue certificates, misconfigured certificates, and in some instances lost millions of dollars due to downtime of critical business systems.

Symantec updates its **Certificate Intelligence Center** cloud service with new management and automation capabilities to manage the certificate lifecycle, from installations, renewals and upgrades to revocation. Other key features include a comprehensive view of a customer's entire SSL portfolio with integrated monitoring, reporting and rating functions. Automation capability is currently scheduled to be available first half of 2013.

**Safe Delivery of Trusted Applications**

[2] Symantec SSL Management Global Customer Survey, February 2013

**Symantec Secure App Service** delivers an industry first in offering a hosted code-signing service for companies and app stores to secure their third-party or company-owned applications. This new cloud-based service assures users the application they are using is trusted and authenticated and has not been maliciously tampered with. For the app developer, the Secure App Service provides full audit and reporting capabilities to track activity for better control and protection. Available today with a SOAP API for integration within the enterprise environment, Secure App Service is scheduled to be available this summer with a full management GUI.

**Website Security Solutions Tackle Increased Malvertising Attacks**

The increase in malvertisements or malicious ads threatens online businesses and ad networks serving up online ads. According to a recent survey of ad publishers[3], more than 50 percent have experienced at least one malvertising incident in the last twelve months and about 90 percent rate malvertising protection as very important.

Symantec's **AdVantage** is the company's first advertising and media service to protect web businesses and brand reputations. The secure cloud-based service delivers real-time monitoring, notification and detailed forensics of malvertisement incidents. Ad networks and publishers get immediate insights through visual tracing and comprehensive incident reporting to quickly remediate issues and reduce risk in display advertising.

**Partner Quotes on ECC Adoption**

"Citrix recognizes that ECC encryption represents the future of SSL encryption," said Steve Shah, Sr. Director, Citrix. "This shift in the cryptographic infrastructure is clearly a next generation approach to the security ecosystem, allowing for better scalability in cloud computing and the supporting infrastructure. Once the certification authority infrastructure is in place, the trend will be clear to follow for networking product groups to make remote datacenters more accessible quickly, even allowing for increasing key sizes and increasing security needs."

"We believe in constantly furthering web security, which is why Chrome supports Elliptic Curve Digital Signature Algorithm (ECDSA) on all modern operating systems," said Adam Langley, software engineer at Google.

"HID Global specializes in security access solutions for the cloud, data and the door, with a comprehensive portfolio incorporating both physical and logical access solutions," said Julian Lovelock, VP of Product Marketing at HID Global. "We're very supportive of the new DSA and ECC algorithm options emerging in the marketplace, and we strongly feel that where the NIST Suite B has drawn up the future of security algorithms, the industry will follow."

"At Opera we are committed to both high quality and security, and we welcome the adoption of new and improved security standards on the web. Elliptic Curve Cryptography provides significant improvements over earlier algorithm standards, and we are delighted to see Symantec support it. Opera's Presto engine added support for ECC in version 395." Source: Security Manager at Opera

[3] Symantec AdVantage Malvertising Survey, September 2012

"Red Hat and Symantec have long collaborated to bring compelling, secure solutions to our customers," said Bryan Che, Sr. Director Product Management, Red Hat Cloud Business Unit. "We continue to be interested in providing the advantages of increased security and computational efficiency that elliptical curve cryptography (ECC) offers for key management and digital signature, and have been an active participant with Symantec in Project Beacon. Currently, our Red Hat Certificate System supports ECC public-key cryptographic systems and continues to enhance its web browser and operating system ECC support."

**AdVantage Customer Quote**

"As a leading digital media network in South East Asia, our business depends on protecting our customers, and network of over 10,000 websites, from increasing threats and malvertisements," said Eng Tat, Head of Technology Development, Innity. "Symantec AdVantage provides critical security against the malicious advertisements that can ruin display advertising, damage brand reputation and ultimately, hurt eCommerce businesses."

**Resources**

- Website Security Solutions and Algorithm Agility Press Kit
- SlideShare Presentation: Website Security Solutions
- FAQ: ECC and DSA Certificates Website Security Solutions
- Website Security Solutions
- Symantec Managed PKI for SSL
- Data Sheet: Symantec SSL Certification with the ECC Algorithm
- Data Sheet: Symantec SSL Certificates with the DSA Algorithm
- Algorithm Agility with RSA, ECC and DSA White Paper
- Educational Resources: www.staysecureonline.com
- Symantec Certificate Intelligence Center
- Symantec Secure App Service
- Symantec AdVantage
- Website Security Solutions Partner Program
- SSL Firsts video
- Why Symantec and SSL Overview Video
- Website Security Solutions Blog
- Algorithm Agility ECC & DSA Blog

**Connect with Symantec**

- Follow Symantec on Twitter
- Join Symantec on Facebook
- View Symantec's SlideShare Channel
- Subscribe to Symantec News RSS Feed
- Visit Symantec Connect Business Community

**About Symantec**

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

###

**NOTE TO EDITORS:** If you would like additional information on Symantec Corporation and its products, please visit the Symantec News Room at http://www.symantec.com/news. All prices noted are in U.S. dollars and are valid only in the United States.



FORWARD-LOOKING STATEMENTS: Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and are subject to change. Any future release of the product or planned modifications to product capability, functionality, or feature are subject to ongoing evaluation by Symantec, and may or may not be implemented and should not be considered firm commitments by Symantec and should not be relied upon in making purchasing decisions.