December 6, 2010

Independent Studies Examine Far-Reaching Benefits of DNSSEC for Hardware and Software Vendor Communities

Results to Be Presented During Webinars on December 14 and 16

DULLES, VA (Marketwire) - New Forrester Consulting studies, commissioned by VeriSign, Inc. (NASDAQ: VRSN), examine trends in Domain Name System (DNS) security and their impact on hardware and software vendors. Based on an October 2010 survey of enterprise and SMB companies in the US, UK, Germany, Brazil, India and Japan, the studies outline user demand, and hardware and software vendor plans with regards to the incorporation of DNS Security extensions (DNSSEC) into their infrastructures.

The studies feature new research devoted to gauging vendor attitudes toward DNSSEC and the adoption of DNSSEC in the hardware and software communities. DNSSEC is used to authenticate DNS data to help prevent cache poisoning and man-in-the-middle attacks.

VeriSign will host a webinar on Dec.14 to outline key findings from the Forrester study for hardware vendors. Cisco Systems executives Joe Dallatore, Sr. Manager, Security Research and Operations group, and Patrik Fältström, Distinguished Consulting Engineer in the Office of the CTO, will also participate. In addition, VeriSign will host a webinar on Dec.16 to outline key findings from the Forrester study for software vendors.

Following the webinars, white papers will be publicly available at http://www.verisign.com/dnssec.

"The Internet is an increasingly critical infrastructure for our government, economy, society and national security, which is why it's so important that the entire Internet community adopt DNSSEC," said Pat Kane, Assistant General Manager of Naming Services at VeriSign. "If hardware vendors, software companies, ISPs, registries and registrars work collaboratively, it will help to facilitate a smooth, widely effective implementation of DNSSEC."

Among Forrester's key findings:

- A significant number of companies saw substantial customer demand for DNSSEC in the last 12 months
- A high percentage of companies said they already support, or are currently testing support for DNSSEC
- The majority of companies believed support for DNSSEC could be implemented within six months
- Three quarters of the companies indicated a desire to participate in VeriSign's DNSSEC Interoperability Lab

DNSSEC applies digital signatures to DNS data to authenticate the data's origin and verify its integrity as it moves throughout the Internet. The security extensions are designed to protect the DNS from attacks intended to redirect queries to malicious sites by corrupting DNS data stored on recursive servers. The successful implementation of DNSSEC will eliminate a hacker's ability to manipulate DNS data. The resulting digital signatures on that DNS data are validated through a "chain of trust."

VeriSign, in collaboration with the U.S. Department of Commerce and ICANN, deployed DNSSEC in the DNS root zone in July. In addition, the company deployed DNSSEC in the .edu zone in August. VeriSign expects to sign .net by the end of this year and .com by the end of the first quarter of 2011.

About VeriSign
VeriSign, Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, VeriSign enables companies and consumers all over the world to connect online with confidence. Additional news and information about the company is available at www.verisign.com.

Statements in this announcement other than historical data and information constitute forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 as amended and Section 21E of the Securities Exchange Act of 1934 as amended. These statements involve risks and uncertainties that could cause VeriSign's actual results to differ materially from those stated or implied by such forward-looking statements. The potential risks and uncertainties include, among others, the uncertainty of future revenue and profitability and potential fluctuations in quarterly operating results due to such factors as increasing competition, pricing pressure from competing services offered at prices below our prices and changes in marketing practices including those of third-party registrars; the current global economic downturn; challenges to ongoing privatization of

Internet administration; the outcome of legal or other challenges resulting from our activities or the activities of registrars or registrants; new or existing governmental laws and regulations; changes in customer behavior; the inability of VeriSign to successfully develop and market new services; the uncertainty of whether our new services will achieve market acceptance or result in any revenues; system interruptions; security breaches; attacks on the Internet by hackers, viruses, or intentional acts of vandalism; and the uncertainty of whether Project Apollo will achieve its stated objectives. More information about potential factors that could affect the company's business and financial results is included in VeriSign's filings with the Securities and Exchange Commission, including in the Company's Annual Report on Form 10-K for the year ended December 31, 2009, Quarterly Reports on Form 10-Q and Current Reports on Form 8-K. VeriSign undertakes no obligation to update any of the forward-looking statements after the date of this announcement.