



DNSSEC represents the most significant change in the history of DNS, and must be implemented carefully to avoid causing more harm than good in the form of outages, compatibility issues and other failures. The potential for problems grows as DNSSEC is implemented on larger and larger networks.

Early implementations of DNSSEC in several TLDs and VeriSign's own testbed of a DNSSEC-signed root revealed some issues that DNSSEC implementation can raise. The addition of digital signatures has the potential to substantially increase the size of DNS packets and thus increase Internet traffic. In addition, the success of DNSSEC depends on global adoption, and must be available in the root zone (see sidebar) and top-level zones, such as .com and .net, to encourage and allow widespread adoption. Major development efforts are required at the registry level because every component is affected, including registrar interfaces (EPP), database schemas, business rules, DNS resolution, and monitoring systems. Registrars will need to be DNSSEC aware, by updating their systems to accept and manage DNS key material from their customers, and pass it along to registries. VeriSign is committed to providing registrars with the tools and training required for their DNSSEC deployments. Additionally, ISPs will need to enable DNSSEC on their name servers.

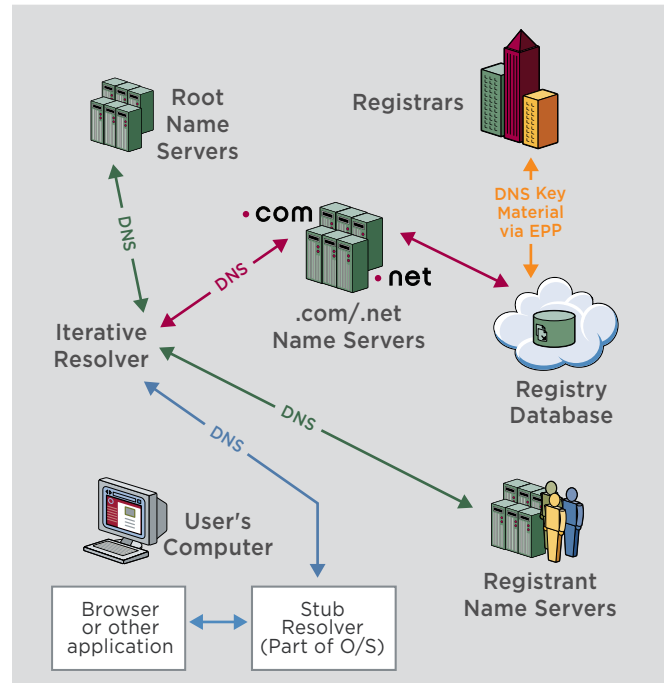
**FULL DNSSEC IMPLEMENTATION STARTS WITH THE ROOT ZONE**

VeriSign, under a cooperative agreement with the U.S. Department of Commerce, and ICANN, as part of its Internet Assigned Numbers Authority (IANA) functions role, are working together to sign the root zone. The U.S. Department of Commerce has developed root zone signing requirements. ICANN will create and manage key-signing keys (KSKs), sign root zone key sets, and publish KSKs to the community. VeriSign will create and manage zone-signing keys (ZSKs) and create, sign, and publish the root zone. While the details of the deployment are not available yet, the three organizations are working together to sign the root zone.

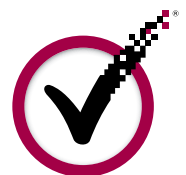
DNS and Internet security are VeriSign's core businesses. VeriSign was a key contributor to the development of DNSSEC and played a leading role in the development of the DNSSEC standards. VeriSign is planning a methodical rollout of DNSSEC across the domain names, starting with the smaller zones and increasing in size, applying lessons learned by observing other DNSSEC deployments, changes in DNS traffic, testing scalability and capacity throughout the deployment schedule of VeriSign operated TLDs. VeriSign anticipates full implementation of DNSSEC to be complete in .net and .com by the first quarter of 2011.

VeriSign's work on DNSSEC is part of our ongoing fortification of and strategic investment in the Internet infrastructure. As a registry, we constantly invest in our network and scalability to keep up with the demands of users and protect against growing threats.

**Systems Impacted by DNSSEC**



Source: VeriSign  
 DNSSEC implementation touches nearly every component of Internet infrastructure, including: the root zone, registries, registrars, ISPs, hosting services, and applications.





## LEARN MORE

To subscribe or to access the archives for the Domain Name Industry Briefs, please go to [www.verisign.com/domainbrief](http://www.verisign.com/domainbrief). Email your comments or questions to [domainbrief@verisign.com](mailto:domainbrief@verisign.com).

## ABOUT VERISIGN

VeriSign, Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, VeriSign helps companies and consumers all over the world engage in communications and commerce with confidence. Additional news and information about the company is available at [www.verisign.com](http://www.verisign.com).

©2009 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. 09/09.

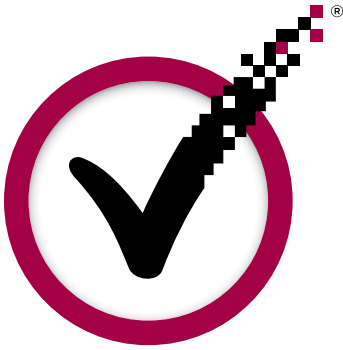
Statements in this announcement other than historical data and information constitute forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. These statements involve risks and uncertainties that could cause VeriSign's 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 and pricing pressure from competing services offered at prices below our prices and market acceptance of our existing services, the inability of VeriSign to successfully develop and market new services, and the uncertainty of whether new services as provided by VeriSign will achieve market acceptance or result in any revenues. 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 presentation.

---

### Zooknic Methodology

For gTLD data cited with Zooknic as a source, the analysis uses a comparison of domain name root zone file changes supplemented with WHOIS data on a statistical sample of domain names which lists the registrar responsible for a particular domain name and the location of the registrant. The data has a margin of error based on the sample size and market size. The ccTLD data is based on analysis of root zone files. For more information, see [www.zooknic.com](http://www.zooknic.com).





# THE DOMAIN NAME INDUSTRY BRIEF

VOLUME 6 - ISSUE 3 - SEPTEMBER 2009

## THE VERISIGN DOMAIN REPORT

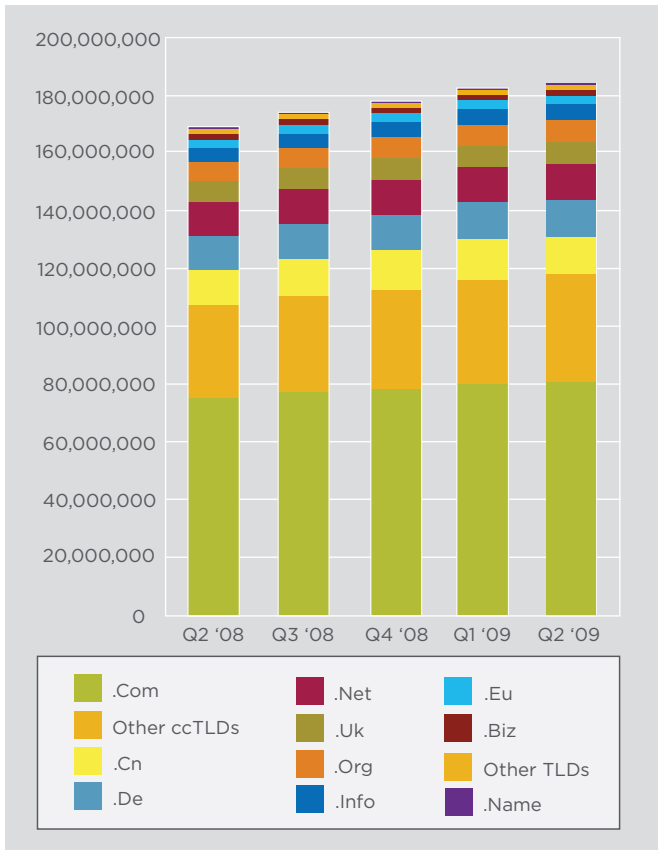
As the global registry operator for .com and .net, VeriSign reviews the state of the domain name industry through a variety of statistical and analytical research. As a leading provider of digital infrastructure for the Internet, VeriSign provides this briefing to highlight to industry analysts, media, and businesses important trends in domain name registration, including key performance indicators, and growth opportunities.



**EXECUTIVE SUMMARY**

At the midpoint of 2009, there was a base of 184 million domain name registrations across all of the Top Level Domain Names (TLDs). This represents a one percent growth over the first quarter of 2009 and a nine percent growth over the same quarter of last year. The base of Country Code Top Level Domain Names (ccTLDs) rose to 74.4 million domain names, a 14 percent increase year over year and a one percent increase quarter over quarter. In terms of total registrations, .com continues to have the highest base followed by .cn (China), .de (Germany) and .net.<sup>1</sup>

**Total Domain Name Registrations**



Source: Zooknic, July 2009; VeriSign, July 2009

**INDUSTRY GROWTH AND COMPOSITION**

Around nine million new domain names were registered across all of the TLDs in the second quarter of 2009. This reflects a reduction in new registrations with a 14 percent decline from the first quarter 2009 and a 15 percent decline from the same quarter in the previous year. As seen in past years, there is seasonality in domain name registrations with the second quarter of the year dropping from the first quarter. In second quarter 2009, the impact of seasonality as well as the overall weak economic conditions impacted the number of new registrations for both gTLD and ccTLD registrations, though the ccTLD decline was much larger.

The composition of the domain name industry and rank order in terms of base size remained consistent with that of first quarter 2009. The largest TLDs in terms of base size were .com, .cn, .de, .net, .org, .uk, .info, .nl (Netherlands), .eu (European Union), and .biz. The size of the base for .cn and .de were nearly equal at the end of the second quarter with .cn just edging out .de.

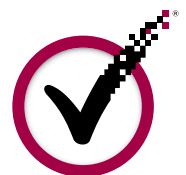
**ccTLD Breakdown**

The second quarter of 2009 ended with 74.4 million ccTLD registrations across all of the ccTLDs, representing a 14 percent increase over the same quarter of 2008 and a one percent increase from the previous quarter. There are more than 240 ccTLD extensions globally, but the top 10 ccTLDs comprise 66 percent of the total number of registrations.

Among the top 25 largest ccTLDs, there was notable growth quarter over quarter among several ccTLDs. Registrations for .ar (Argentina) domain names grew the fastest with an eight percent growth quarter over quarter, which may be related to the opening of IDN registrations at the end of March. Russian Federation (.ru) domain name registrations grew by seven percent, a slightly slower trend than previous quarters but still the second fastest growing among the largest ccTLDs. The Brazilian ccTLD, .br, also saw domain name registrations grow by seven percent over the quarter which was likely due to liberalization of registration requirements for .net.br in April 2009 and .com.br in May 2008. The Chinese ccTLD, .cn, which had been experiencing notable growth, saw the overall base of registrations decline eight percent quarter over quarter.<sup>2</sup>

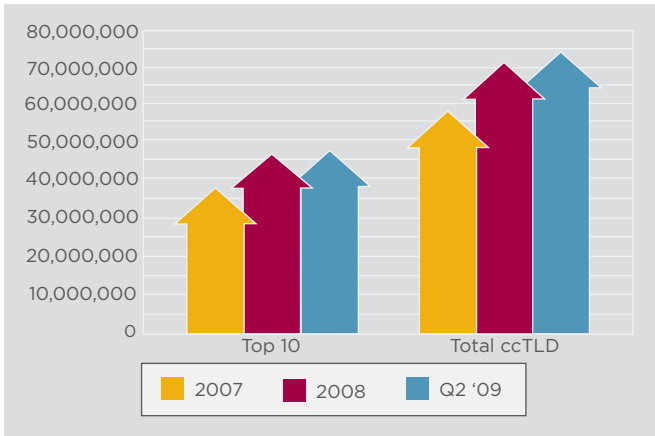
1 The gTLD and ccTLD data cited in this report are estimates as of the time of this report and subject to change as more complete data is received.

2 The .cn Registry (CNNIC) had been running a price promotion with a 1 RMB Yuan (US\$0.14) fee for a one-year .cn domain name registration. The fees changed on March 1, 2009 to 18 RMB Yuan (US\$2.64).





ccTLD Breakdown



Source: Zooknic, July 2009

Only four, .ar, .au (Australia), .br (Brazil), .pl (Poland) of the top 25 largest ccTLDs experienced quarterly growth rates in the second quarter of 2009 that were higher than the growth rates in the first quarter of 2009. Four of the top 25 largest ccTLDs, .ru, .pl, .br, and .fr (France), experienced growth rates year over year in excess of 25 percent.

In terms of the total base of domain name registrations, .cn, .de and .uk were the largest ccTLDs. Year over year, .cn's growth rate was nine percent. Rounding out the top three ccTLDs were .de and .uk, at six percent and 11 percent growth year over year, respectively. Together, the bases of domain name registrations for these three ccTLDs represented 45 percent of all ccTLD domain name registrations.

**TOP CCTLD REGISTRIES BY DOMAIN NAME BASE, SECOND QUARTER 2009**

- |                         |                             |
|-------------------------|-----------------------------|
| 1. .cn (China)          | 6. .ru (Russian Federation) |
| 2. .de (Germany)        | 7. .ar (Argentina)          |
| 3. .uk (United Kingdom) | 8. .br (Brazil)             |
| 4. .nl (Netherlands)    | 9. .it (Italy)              |
| 5. .eu (European Union) | 10. .us (United States)     |

Source: Zooknic, July 2009.

**.COM/.NET DYNAMICS**

VeriSign's average daily Domain Name System (DNS) query load during the second quarter increased from 38 billion to 49 billion per day, resulting in hundreds of millions of Internet users accessing Web sites or sending email. This is a 29 percent increase from the 38 billion queries in first quarter 2009. Managing the increasing traffic on the Internet reflects VeriSign's continued investment in the DNS. VeriSign's continued commitment to its infrastructure has enabled them to maintain a record of 100 percent uptime over the past 11 years, earning VeriSign the reputation of being one of the most reliable and trusted networks in the world.

**The .Com and .Net Base and New Registrations**

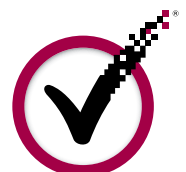
The overall base of .com and .net domain names grew to 93.5 million domain names during the second quarter of 2009. This represents a one percent increase over the first quarter of 2009, a seven percent increase over the same quarter of the previous year, and a 28 percent increase over the second quarter of 2007.<sup>3</sup>

New .com and .net registrations were added at an average of approximately 2.3 million per month in the second quarter of 2009 for a total of seven million new registrations in the quarter. This four percent decline from the previous quarter is in line with normal seasonal fluctuations.

**Renewals**

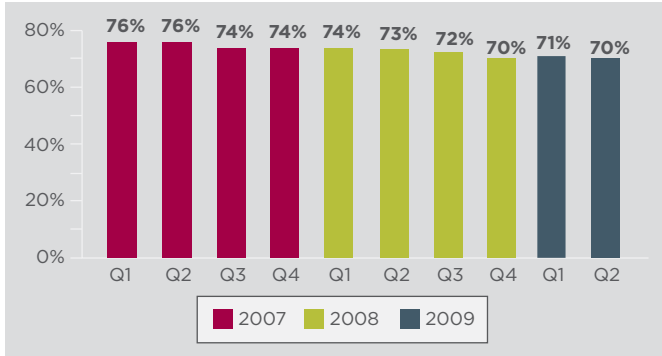
The renewal rate for the second quarter of 2009 was 70 percent which was a slight decrease from the renewal rate in the first quarter of 2009 which was 71 percent. Quarterly renewal rates may deviate a few percentage points in either direction each quarter based upon the composition of the expiring base and the contribution of specific registrars.

<sup>3</sup> For .com and .net domain name registrations, VeriSign reports an adjusted base of active domain name registrations, which reflects deletions that occur within the five-day Add Grace Period beyond the quarter end. This figure may differ from other non-authoritative publicly available sources which do not adjust the base.





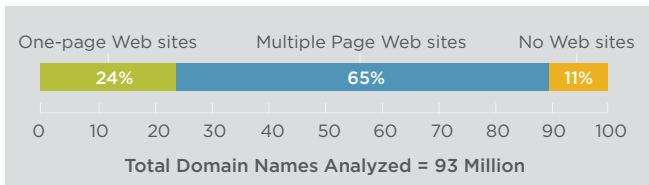
**.Com/.Net Registry Renewal Rates**



Source: VeriSign, August 2009

Whether a domain name resolves to a Web site is a key factor in the renewal rates since domain names that resolve to Web sites are more likely to be renewed. VeriSign estimates that 89 percent of .com and .net domain names resolve to a Web site, meaning that an end-user visiting that domain name would find a Web site. These Web sites can be further described as those having multiple pages or as one-page Web sites. One-page Web sites include under-construction, brochure-ware and parked pages in addition to online advertising revenue generating parked pages.

**.Com/.Net Web Sites**



Source: VeriSign, July 2009

**DNS SECURITY EXTENSIONS (DNSSEC)**

The Domain Name System (DNS) is the addressing system of the Internet. It translates human-friendly domain names into the numerical identifiers (IP addresses) in order to route Internet traffic for applications including email, websites, software updates, virus filters, and VoIP. Because DNS is so important to the functioning of the Internet it must be highly available and highly reliable.

VeriSign has provided 100 percent availability of DNS for the .com and .net zones for over 11 years and has worked to improve the reliability and performance of the Internet infrastructure. Unfortunately DNS is not completely trusted because DNS is vulnerable to “man in the middle” and cache poisoning attacks, which can potentially result in users receiving false messages or being redirected to phishing and phishing sites.

DNS Security Extensions (DNSSEC) offers the potential to strengthen Internet security by authenticating the origin of DNS data and verifying its integrity while moving across the Internet. The Internet Engineering Task Force (IETF) has been working on DNSSEC since 1995, VeriSign has been involved in its development since 2000, and the latest standards for DNSSEC were published in 2005. A reference event that recently brought attention to the implementation of DNSSEC was highlighted by a vulnerability in the DNS protocol that facilitated cache poisoning. This vulnerability can be mitigated by implementing DNSSEC.

DNSSEC introduces security by cryptographically signing DNS data. Users are assured that the data originated from the stated source and that it was not modified as it moved across the Internet. DNSSEC can also prove that a domain name does not exist (a concept called authenticated denial of existence).

The implementation of DNSSEC will fortify DNS data and prevent the compromise of DNS integrity; however, DNSSEC will not provide confidentiality, prevent attacks against name servers, or secure data on Web sites. And it will not solve many of the most common threats to Internet security, such as IP address spoofing or phishing. DNSSEC provides important but incomplete security improvements. Other layers of protection, such as SSL certificates and two-factor authentication, can provide complementary security enhancements to provide an increased level of trust for Internet users.

