



Confidence in a connected world.  **Symantec**

CUSTOMER SUCCESS

Directorz Co. Ltd.

Boosting SSL Security While Cutting CPU Use by 46 Percent with Symantec Solutions

Most businesses would love to face the challenge that Directorz, a Tokyo-based web hosting company, needed to solve. Two of its web properties have surged in popularity, raising the CPU burden on its web hosting servers. To see if performance could be streamlined, Directorz tested Symantec premium SSL certificates, which include a new ECC encryption algorithm that provides stronger security and faster performance than the current industry-standard RSA algorithm. The results include a 46 percent lower CPU burden and a 7 percent reduction in response time, enabling more total simultaneous connections to a single site.

Must have trust

The Internet depends on trust. Users want to be confident they are interacting with a trusted website, and that information they share will be secure.

An SSL certificate provides this trust. It is issued by a Certification Authority (CA) only after the CA authenticates the identity of the organization requesting it. An SSL certificate on a web server gives users third-party validation of the site owner's identity, and it interacts with the user's browser to indicate when a web session is being encrypted. This gives the user the assurance that shared data is protected.

Kei Kato knows the value of this trust. When he founded a web hosting company called Directorz in Tokyo in 2007, he wanted SSL certificates to authenticate his servers. He also wanted to sell SSL certificates to his clients, so that they could build trust with their own users for websites and extranets that they hosted at Directorz.

Mr. Kato has been in the web hosting industry since 1999, and from the beginning he was familiar with Symantec SSL certificates. They were called VeriSign certificates at that time, before Symantec acquired the VeriSign authentication business, and they were the first SSL certificates in the industry. "They are the most widely recognized certificates in the world," Mr. Kato says.

ORGANIZATION PROFILE

Website: directorz.co.jp
Industry: Information Technology
Founded: 2007
Headquarters: Tokyo, Japan
Employees: 12
Offering: web and email hosting and website security to companies in technology, and other industries

SYMANTEC SOLUTION

Website Security

STRATEGIC IT TRENDS

Threat Landscape

Why Symantec?

- Best-known SSL protection builds user trust
- EV SSL technology makes a green tab or address bar and further enhances trust
- New ECC encryption algorithm reduces CPU usage for faster performance
- Choice of encryption algorithms in one certificate boosts flexibility

Enhancing trust even further

Mr. Kato chose Symantec SSL certificates when he started Directorz in 2007, and in 2009, he began using Symantec™ Secure Site Pro with EV SSL Certificates. These include a technology that triggers a green strip or tab in the address bar in browsers. As a result, users have an easy and reliable way to verify site identity and security.

"The Symantec EV SSL Certificates cost more than SSL certificates from Symantec's competition," says Mr. Kato. "But at Directorz, we have many clients who know the value of the EV green bar and the Norton Seal because they win increased trust from users. Those clients pay more for the EV SSL certificates because they are worth it."

Popularity can be a problem

In 2010, Mr. Kato and his technology team launched two particularly successful projects at Directorz. One is a site known as Kmonos (kmonos.jp), which contains useful data about 3,600 companies listed on Japan's stock exchange. The site is used by university students, job seekers, and others who want to research the companies, and it is achieving about 1.3 million page views per month. The site also raises awareness of Directorz as a hosting provider and potential place to work.

Another fast-growing project is Co-akuma (<https://co-akuma.directorz.jp/blog/>), a blog on the Directorz site that features tips for beginning engineers on a range of technologies. The blog was intended for internal training at Directorz, but a celebrity in Japan commented in public interviews about how friendly and clear the explanations and drawings are, and now the blog gets 300,000 page views a month. Its contents have been turned into a popular book.

Must have speed

The growing audience for both sites presented a challenge: The web server at Directorz was getting overburdened, and users typically don't come back if pages don't load quickly. "Kmonos in particular gets a lot of concentrated traffic whenever a job hunting season is started, and the site would labor

SOLUTIONS AT A GLANCE

Key Challenges

- Authenticate websites and servers to build trust
- Minimize CPU usage for encrypted sessions
- Enable encryption algorithm flexibility to accommodate changes over time

Symantec Products

- Symantec™ Secure Site Pro with EV SSL certificates

Technology Environment

- Server platform: Intel Xeon 2Core Server, CPU 2GB, Apache Web Server
- Web server software: Apache and Nginx

BUSINESS RESULTS AND TECHNICAL BENEFITS

- 46% less CPU burden on Apache web server
- 7% reduction in response time
- 10,000-fold increase in difficulty to crack ECC keys vs. comparable-size RSA keys

under the weight of huge numbers of SSL connections at the same time," says Mr. Kato. To gain processing speed, Mr. Kato and his team decided to test a Symantec SSL certificate with Elliptic Curve Cryptography (ECC).

The encryption algorithms in ECC are based on elliptic curves over finite fields. They provide stronger security and faster performance than RSA-based algorithms, which are the current encryption norm.

As an example, a 256-bit ECC key provides the same level of security as a 3072-bit RSA key. Yet compared to a 2048-bit RSA key, which is a new encryption standard recommended by the U.S. government, ECC-256 keys are 10,000 times harder to crack.* And because ECC keys have a shorter key length, they process faster.

"In our testing, the Symantec ECC-based SSL certificate reduced the CPU burden on the web server by 46 percent compared with an RSA-based SSL certificate, and shortened response time by 7 percent."

Kei Kato

President
Directorz Co. Ltd.

Cutting CPU use by 46 percent

Mr. Kato and his team validated the faster performance. “In our testing, the Symantec ECC-based SSL certificate reduced the CPU burden on the Apache web server by 46 percent compared with an RSA-based SSL certificate, and shortened response time by 7 percent,” says Mr. Kato. “Many of our clients will be interested in ECC, especially those who are concerned about using SSL because of its effect on CPU utilization.” ECC will also allow Directorz to avoid purchasing extra servers. “We’re saving around US\$3,600-6,000 per year by avoiding these investments” Mr. Kato adds.

The ECC algorithm can enable more total simultaneous connections to a single site, which is important in an era when tablets, smartphones, and other mobile devices are driving more traffic onto the web, Mr. Kato observes.

Before deploying ECC, it’s necessary that a business upgrade to the latest versions of web server hosting software, Mr. Kato notes. That’s why it’s useful, he says, that a Symantec premium SSL certificate enables any of algorithms to be used. Symantec provide certificate includes options of ECC as well as RSA and DSA (Digital Signature Algorithm) algorithms, at no extra cost. By providing three options in one certificate, organizations can easily test to determine how to optimize certificate performance for their specific security ecosystem.

“Many of our clients will be interested in ECC, especially those who are concerned about using SSL because of its effect on CPU utilization.”

Kei Kato

President
Directorz Co. Ltd.

* Symantec Official Blog. Introducing Algorithm Agility: ECC and DSA. Symantec.com. Accessed June 14, 2013