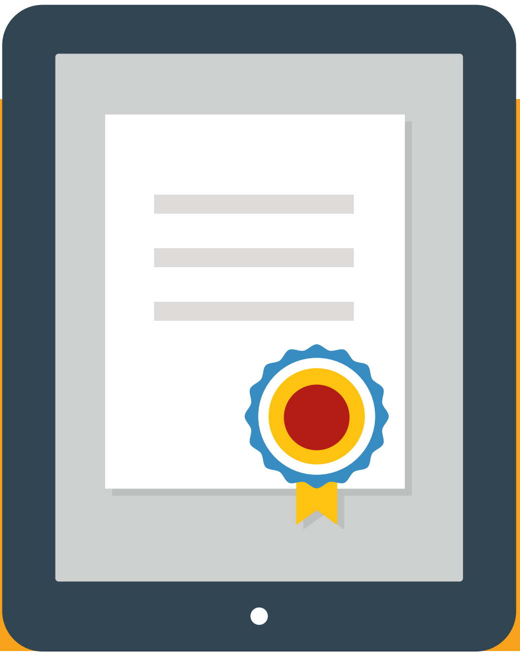
Symantec. | Website Security Solutions

Not all Certificate Authorities are created equal



Vigilance today will keep your website safe tomorrow

There have been a string of successful attacks oncertificate authorities (CAs) this year, and the threat to CAs will certainly not abate. On the contrary, hackers have been raising their game steadily and thetechniques used to exploit networks grow ever more sophisticated.

As one of the world's leading certificate authorities, we at Symantec take the responsibility for securing the transit of data on the Internet as a serious obligation to our customers.

We believe that it's critical that a CA's top business priority be placed on:

- **The continual hardening of the infrastructure** that protects the cryptographic keys
- **Securing the authentication process** that validates identity.

Rigorous and diligent upkeep of the security infrastructure surrounding a CA must be seen as a crucial ingredient to the success of a CA's customers and the web consumer community at large.

For businesses considering a choice of CA, it is important to remember that your choice does in fact matter. Not all Secure Sockets Layer (SSL) certificates are issued with equal diligence and businesses should consider the level and **rigour of authentication and security** that goes into the SSL certificates in which you place the trust of your brand and your customers. Although price certainly plays a significant role in the purchasing process, as the multiple CA breaches this year have reminded us, we suggest **price should be but one of many factors in selecting a CA.**

VeriSign Authentication Services (now part of Symantec) has a proud history as a CA, having never been breached. To ensure the security of your website, and therefore the security of your business and customers, we implement the following stringent procedures to ensure the security of all our SSL certificates:

- **Diligent security** to protect our cryptographic keys
  - Specifically designed hardened facilities to defend against attack
  - Hardware-based cryptographic signature systems
  - Regular third-party audits
  - Thorough network security and antimalware defence
- **Daily penetration testing** to ensure there are no network vulnerabilities, and subsequent remediation of any findings
- **Enforcement of dual control** for Organisation Validation (OV) and Extended Validation (EV) certificate issuance
- **Use of authentication and registration best practices** to identify ownership
- **Documented employee background investigations** to protect against insider threat
- **A secure CA environment** with dual access control, biometrics based security, 24/7 facilities and hardware monitoring in place on site

- **Separation of duties for product developers** working in authentication and verification
- **Strong passwords** at a systems and infrastructure level
  - 90-day refresh
  - No repeats
  - Provision and de-provision of passwords

For consumers, it is important to know that SSL remains the most effective method of secure web data transmission. It is equally critical to remain aware of who is behind the security of the website you are doing business with. Are they reputable? Do they have a proven track record for issuance of certificates? Do they have a robust infrastructure in place to prevent attacks? To further protect yourself online, know what to look for:

- **Updated browser software** to obtain the latest set of valid root keys
- **Watch for the green address bar** provided by EV SSL for extra protection
- **Look out for a recognised trust mark** such as the Norton Secured seal with the check-mark
- **Make sure that you can see the 's' in "https"** in the URL to indicate a secure environment.
- **Watch for the padlock** to verify who has signed the SSL certificate, and ensure that you recognise the Certificate Authority listed.

It is important for the online community to understand that there is nothing inherently broken with SSL, it is really just about CAs and businesses doing the right thing to ensure that customer information remains secure. CAs that follow established best practices for securing private keys; along with vigilant enforcement of stringent authentication practices are critical components in keeping the Internet a safe environment for all.

More Information

Visit our website

www.symantec.co.uk/seal

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec (UK) Limited
Website Security Solutions
350 Brook Drive, GreenPark,
Reading Berkshire RG2 6UH, UK
www.symantec.com