Everything a business manager needs to know about SSL certificates

By Andy Churley

Andy is Director of Product Innovation at CentralNic Group and has more than 20 years experience in the IT Security Industry.

Summary

Almost every time you visit a website, log in to something or buy anything online you are using a SSL (Secure Socket Layer) certificate to protect your sensitive information. All businesses that operate websites should have at least one SSL certificate.

Google (and other browser and search engine providers) now mark websites without an SSL certificate as ‘not secure’ or downgrade their position in search results, causing website traffic to non-SSL sites to drop off a cliff.

Management of SSL certificates are often consigned to the realm of the IT department and are generally poorly understood by business owners. However, SSL certificates provide two non-technical elements that are vital to any business transaction: Trust and Privacy. A basic understanding of what they do and why they are important is a must for business people.

Business owners should:

- check that all their websites have a SSL certificate deployed;
- determine what level and type of certificate should be used;
- ensure that all websites are using the right certificate.

The short article below explains everything that a business person needs to know about SSL certificates.

If you don’t have time to read the entire article – just contact Bonnie Wittenburg (bwittenburg@key-systems.net) for a free, enterprise wide portfolio audit to provide an up-to-date snapshot of your SSL health.
Everything a business manager needs to know about SSL certificates

Every time you log-in to your online bank account, every time you buy something on Amazon and nowadays, almost every time you visit a website – you are accessing an SSL Certificate and securing the information that you send to it, and that it sends to you.

For individual internet users, SSL encryption is something that happens invisibly but for online brands, retail websites and large companies SSL encryption is the foundation stone to their online security, customer confidence and website revenue. It is therefore surprising that many brands have no SSL management policy nor even a single group that maintains them.

Domain names and SSL certificates

Domain names (web addresses) and SSL certificates are inextricably linked and share a number of the same properties:

1) **They are numerous**: most businesses will have more than one domain name (many will have thousands) and more than one SSL certificate

2) **They expire**: many medium to large businesses with sizable portfolios could be faced with renewing several domain names a day

3) **They are linked to websites**: domain names point the way to a website and SSL certificates are usually secure communications between a website and a web visitor

The impact of loss

When looking at the importance of any business asset, one measure commonly used is the impact on the business should that asset no longer be available.

Both domain names and SSL certificates are business critical online assets. If a domain name expires, its website is no longer accessible on the internet and the ability to trade online will be lost. If an SSL certificate expires, its website will cease to be trusted by search engines and all visitors will receive a warning that the site is not secure – online revenues will plummet.

Most online retailers can tell you, down to the nearest cent, how much any outage has cost them in sales revenue terms; the long-term reputational cost of a security breach or particularly a data loss incident is more difficult to measure but is widely acknowledged to be potentially crippling for any business, no matter how big it is.

Domain names (web addresses) are increasingly being recognised as business-critical strategic IP assets and placed under the care of a single group or department (normally the legal or marketing departments). These groups recognise the strategic value of a domain name rather than simply counting its financial cost and also recognise the value of their overall domain portfolio, not only from its revenue generating potential but also from a brand protection point of view.

It is far less common for organisations to manage their SSL certificates centrally and they are typically managed by IT departments because, unlike domain names, SSL certificates have to be installed on computer hardware to function.

It’s all about security, right?

Most web users think that SSL Certificates are the things that provide the security during e-commerce transactions – and they would be right. But SSL certificates do so much more.

The main objective for any organisation using SSL Certificates is to ensure two key things:

1) **Secrecy**: making sure any communication between a web visitor and the website owners over the internet is secure and free from interception or tampering (security) using ‘man in the middle attacks’

2) **Legitimacy**: demonstrate clear proof to any web visitor that their website actually belongs to them (validation)
How secure is SSL encryption?

In short, it’s nigh on impossible to succeed in a brute force attack against SSL encryption.

To give you an idea… we often use the metaphor of “trying to find a needle in a haystack”. It’s a great metaphor as we can all see how difficult and time consuming that would be.

Let’s enlarge that metaphor slightly to say it’s like ‘trying to find one atom in the entire universe’. If you could imagine everything in the known universe…, you would be looking at around $10^{82}$ atoms (that’s 10 with 82 zeros after it). That’s a very big number!

In order to factor (crack) an encrypted message using 1024bit encryption, an attacker would need to try more than $10^{305}$ different prime numbers. That’s more like ‘trying to find one atom in a universe of universes’.

To make matters even more difficult for an attacker, nowadays almost all browsers use 2048bit encryption as standard, which is 4.3 billion times harder to factor than a simple 1024bit key.

The four types of SSL certificate

While there three validation levels of SSL certificates there are four common types of SSL certificate. It is important from a security and an operational point of view to use the right SSL certificates for your intended internet infrastructure and business practices.

1. **Single domain SSL certificates** allow the website owner to secure one fully qualified domain name on a single certificate. This type of certificate is often favoured by SMBs; which only have one main website.

2. **Wildcard SSL certificates** permit website owners to secure a single domain name and any sub-domains e.g. `www.domain.name`, `investor.domain.name`, `login.domain.name`. Any subsequent sub-domains that are added are automatically secured with a wildcard certificate.

3. **Subject Alternative Names (SAN) Certificates** (sometimes called multi-domain certificates) enable website owners to secure multiple domain names under a single certificate. However, website owners must specify which domain names are to be covered by a SAN certificate.

4. **Unified Communications (UC) Certificate** is a certificate that was designed to protect Microsoft communications installations such as Exchange and Office. UC certificates support the Microsoft Exchange Autodiscover service and allow environment owners to specify up multiple domains on a single certificate.

The three levels of SSL certificate.

With validation it’s all about trust. For e-commerce to work properly, anyone buying anything online needs to be able to trust that they have a strong likelihood of receiving the item that they have ordered. When a customer visits a website to buy something from it they must be confident that the website they are visiting is actually the website they intended to visit. SSL certificates provide 3 levels of provable validation:

- **Domain Validated (DV) certificates** are verified using only the domain name. For example, the certificate issuer can validate the domain name by sending an email with a confirmation link to an email address, which uses the domain to be protected.

- **Organisation Validated (OV) certificates** step up the validation process where the certificate issuer will verify the business and the business address of the applicant.

- **Extended Validation (EV) certificates** provide the maximum level of assurance and require the most validation. The certificate issuer verifies such things as legal existence and identity, current bank accounts, physical existence, domain ownership and identify a known individual requesting the certificate.

_Domain names are increasingly being recognised as business-critical strategic IP assets and placed under the care of a single group or department_
SSL certificates provide the necessary compliance with Google’s and other web browsers’ stringent search rules and protect your most important assets – your website visitors.

Categorise the prime function: of each website. Does the site sell products and services? Does it offer downloads? Does it have an area for visitor registration e.g. to sign up to receive news and information?

Create a policy: to determine what level and type of SSL certificate is required for each category of website function.

Check all of your websites: to ensure that each of them has the correct SSL certificate for its function, that it has been implemented correctly and that it has not expired.

Companies should also seriously consider:

1) Standardising on one brand of SSL certificate, in order to simplify certificate management and reduce the risk of unnoticed certificate expiry.

2) Selecting a certificate management portal, which reduces issuance delays and helps ensure the portfolio is optimised and up-to-date.

3) Locating a single entity (inside the organisation or an outsource partner) with the responsibility for managing the company’s SSL certificate portfolio.

About the Author

Andy has been in the field of IT Security and online brand protection for over 20 years and has worked for some of the leading firms in the industry including nCipher, Actividentity (now HID), NetNames and CentralNic.

About BrandShelter

BrandShelter manages SSL certificates on behalf of some of the largest companies on the planet. It has some of the world’s best corporate portfolio management platforms, which greatly reduces the risk of expired SSL certificates and boasts some of the world’s leading experts in portfolio management. BrandShelter offers a free, enterprise wide portfolio audit to provide an up-to-date snapshot of your SSL health.

To find out more, contact:

Bonnie Wittenburg
Executive Vice President
Key-Systems USA, Inc.,
885 Harrison St. SE, Leesburg, VA 20175

Tel.: +1 703 297 8151
Fax.: +1 201 596 1433
Email: bwittenburg@key-systems.net

Web: www.key-systems.net
www.RRPproxy.net
www.domaindiscount24.com
www.BrandShelter.com