



Whitepaper

Why strong Validation processes for SSL are essential for the preservation of trust in the Internet economy

Weak validation processes undermine the value of SSL as a trust enabling technology

Introduction

Today, online commerce is worth an estimated US\$1 trillion and continues to grow at a substantial rate. One of the key success factors for e-commerce has been the implementation of highly available security technology into browsers and web servers – in particular SSL. SSL ([Secure Sockets Layer](#)) is the transaction security protocol used by hundreds of thousands of websites to protect online commerce.

The widespread use of SSL has invariably encouraged online commerce and helped it rise to its current levels. As a result our Internet economy has come to depend on SSL as a security and trust infrastructure, but what does the little yellow padlock really mean to the user? More than some SSL Providers would have you believe...

Since the SSL protocol was released by Netscape as a security technology in 1996 consumers have been educated to look for the SSL padlock before passing any critical details over the Internet. Technically, the SSL protocol provides an encrypted link between two parties, however in the eyes of the consumer, seeing the SSL padlock in their browser means much more:

- That they have a secure (encrypted) link with the website
- That the website displaying the padlock is a valid and legitimate organization or an accountable legal entity

As well as ensuring that their details remain secure during a transaction, consumers also care whether the website they are dealing with is legitimate. In order to solve the critical issue of identity assurance as well as information security on the Internet, the efforts of SSL Providers (Certification Authorities), consumer magazines and industry bodies have rightly resulted in the SSL padlock becoming synonymous with trust and integrity – factors consumers associate with being legitimate.

This paper examines how we use SSL commercially and how good validation processes play a critical part in the preservation of a trusted e-commerce infrastructure.

What is SSL?

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remains private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

Who can issue SSL Certificates?

SSL Certificates can be issued by anybody using freely available software such as Open SSL or Microsoft's Certificate Services manager. Such SSL Certificates are known as "self-signed" Certificates. However, self-signed SSL Certificates are not inherently trusted by customer's browsers and whilst they can still be used for encryption they will cause browsers to display "warning messages" – informing the user that the Certificate has not been issued by an entity the user has chosen to trust.

Such warnings are undesirable for commercial sites – they will drive away customers. In order to avoid such warnings the SSL Certificate must be issued by a "trusted certifying authority" - trusted third party Certification Authorities that utilize their trusted position to make available "trusted" SSL Certificates.



Warning message IE users will see from a self-signed SSL Certificate

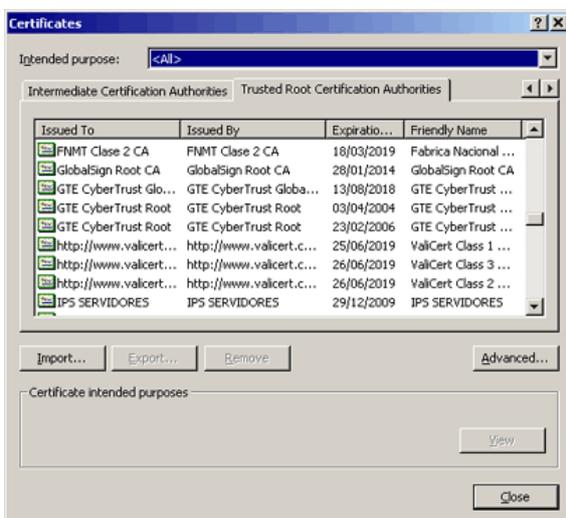


Warning message Netscape users will see from a self-signed SSL Certificate

What is a Certification Authority?

Browsers and Operating Systems come with a preinstalled list of trusted Certification Authorities, known as the Trusted Root CA store. As Microsoft and Netscape provide the major operating systems and browsers, they have elected whether to include the Certification Authority into the Trusted Root CA store, thereby giving trusted status.

Microsoft and Netscape determine which organizations are Certification Authorities.



The Microsoft trusted root CA store



The Netscape trusted root CA store

SSL certificates issued by trusted Certification Authorities do not display a warning and establish a secure link between website and browser transparently. In such circumstances, the padlock signifies the user has an encrypted link with a company who has been issued a [trusted SSL Certificate](#) from a trusted Certificate Authority.

Microsoft and Netscape have therefore determined the role of the Certification Authority – to use their trusted status to “pass trust” to websites whom ordinarily would not be trusted by a customer.

The key issue must now be addressed – before passing such trust, how does the CA know the website can be trusted?

What does a Certification Authority do before issuing a trusted SSL Certificate?

The SSL protocol did not originally include the provision of a validated business identity within the SSL Certificate. Yet both Microsoft and Netscape (and other browser vendors) have a policy of only issuing SSL Certificates to validated entities so consumers now expect such website identity assurances. Market education through the consumer press and industry bodies has also added to people's perception of the SSL padlock as indicating a secure and authentic site.

As a result of their "trusted" status, Certification Authorities have a responsibility to ensure they only ever issue SSL Certificates to legitimate companies. This may only be achieved by employing stringent validation processes to ensure issuance practices only allow the SSL Certificate to be issued to a legitimate company. After all, anyone relying on the presence of an SSL Certificate will do so not just for the encryption factor, but also to indicate the legitimacy of the site.

Whether they realize it or not, consumers dictate that Certification Authorities have a duty to perform satisfactory validation for all SSL Certificate applicants. If validation is weak, consumer confidence in SSL Certificates will be undermined. Gartner has recently examined the consequences of weak validation in their report "Secure Sockets – sometimes isn't", and concluded that consumer web-based commerce could be dramatically inhibited.

All SSL Certificates are not equal!

The value of SSL is protected by the strength of a standard two-point validation process:

- Step 1: Verify that the applicant owns, or has legal right to use, the domain name featured in the application.
- Step 2: Verify that the applicant is a legitimate and legally accountable entity

The compromise of either step endangers the message of trust and legitimacy provided to the end consumer. Companies such as GeoTrust, through its QuickSSL and FreeSSL products, and IPSCA, the Spanish SSL Provider, perform only the first stage of the two-step validation process (as employed by all other SSL Providers) by only verifying that the applicant owns the domain name provided during Certificate application. This validation step relies on the use of Domain Name Registrar details to validate ownership of a domain name and then a challenge email is sent to the listed administrator of the domain name. If the challenge is met with a successful reply, the Certificate will be issued.

Anybody who has purchased a domain name knows that when completing the ownership details, any company, organization or person can be the named owner – these records are not validated! So by relying solely on such records, potentially untrustworthy information is being trusted. Bizarrely, GeoTrust even refer to this cut-down domain-control authentication process as being stronger than traditional two step validation – which includes both the domain name ownership validation step and the added step of business legitimacy verification.

To protect themselves, GeoTrust insert the term "Organization Not Validated" into the issued Certificate. This term is visible to all customers visiting the website using the issued SSL Certificate. Whilst the term no doubt protects GeoTrust from any potential legal recourse, it also means that a website's customer gains little comfort in the trustworthiness of the site – after all as far as the customer is concerned the Organization has NOT been validated!

Trusted Certificates VS Browser Recognized Certificates

We have established that: The role of the Certification Authority is to pass trust.

We have established that: Validation = Trust / No Validation = No Trust

A Certification Authority that does not conduct sufficient two-step validation is simply issuing an SSL Certificate that is designed to bypass the browser warning message – a browser recognized certificate, but not a trusted certificate. Remember that Microsoft and Netscape included the warning message in their browsers in order to alert the user of the un-trusted status of an SSL Certificate.

Bypassing the warning message = Selling the encrypted link without telling the customer it is an encryption only link

If a website is only interested in providing encryption to its visitors it can do so by using a free self-signed Certificate – there is no need to pay a Certification Authority for a trusted SSL Certificate.

The “not trusted” warning message will even let the customer know that whilst the website can provide encryption, it does not provide trust.

Without sufficient validation processes, SSL Certificates are simply encryption certificates that bypass the browser warning message. In other words they are not trusted certificates in the true sense of the word, they are simply browser recognized certificates.

Certification Authorities are trusted by browsers for a reason – to provide trusted certificates. Conducting only weak validation undermines why a Certificate Authority must be a trusted entity and begs the question of why companies should pay for an untrustworthy certificate that consumers, through no fault of their own, inadvertently trust?

In their white papers on SSL, GeoTrust strongly publicize that SSL is NOT for trust and only for encryption and consequently use the argument to justify their lack of business legitimacy validation. However, if SSL is for encryption only why is there a need to display “Organization Not Validated” in their SSL Certificates?

The presence of this warning message is effectively admitting that the consumer, e.g. the party relying on the SSL Certificate, does not inherently know that the SSL Certificate is for encryption only and should not be relied on for business legitimacy. In other words, the consumer must be told that the SSL Certificate does not provide the trust they believed it ordinarily would have.

By displaying the “Organization Not Validated” message, GeoTrust is trying to remove the current association of business legitimacy with SSL. As this message is embedded into the Certificate, where only expert users will be able to find it, consumers are in danger of inherently misinterpreting the intended usage of such Certificates.

The commercial dangers of weak validation

Companies using weakly validated Certificates risk losing the trust of customers who rely on such Certificates when they discover the Certificate stands for “encryption” only. Without the assurance that the company behind the site is legitimate, the customer will go elsewhere to conduct their business. Can a company really afford to lose customers simply because of their choice of SSL provider?

Only by choosing a strongly validated SSL Certificate from a provider who performs two-step validation processes can the user expectations of SSL be realised, and ultimately preserved. Consumers have long associated SSL with more than just encryption. Yet, by removing sufficient validation, the Certificate Authority is not fulfilling its responsibilities to deliver the trust in a “trusted certificate”.

In an environment where trust goes hand in hand with commercial success, removing validation from the very products used to provide such trust is not only dangerous but also poses a long term threat to the Internet economy.

SSL Providers retailing non-validated Certificates will often attempt to sell a “Trust” only product. The downside to this exercise is that websites are forced to purchase both an SSL Certificate and a Trust product just to gain both encryption and trust functionality, whereas a fully validated SSL Certificate can already provide both.

Comodo, like Verisign, Thawte, Baltimore and Entrust, is serious about the validation employed in SSL Certificate applications. If you wish to maintain the trust of your customers, we strongly believe that you should be serious about validation too.

Comodo Instant SSL – the only low cost fully validated SSL Certificate

In May 2002 Comodo launched InstantSSL, the only low cost fully validated SSL Certificates. Prior to the launch of InstantSSL, GeoTrust offered the industry’s cheapest SSL certificates through the QuickSSL brand (the low price being attributed to the due absence of strong validation processes). However, InstantSSL certificates are less than half the price of GeoTrust QuickSSL certificates, issued quickly, and unlike GeoTrust QuickSSL and IP-SCA certificates, InstantSSL certificates are fully validated.

What an SSL Certificate should tell the site’s visitors

Comodo is at the forefront of providing fully qualified SSL Certificates. Digital Signature legislation is catching up to how digital certificates are used commercially and appreciates that applications such as SSL mean much more in commercial terms than just encryption. The EU Directive on Digital Signatures is considered by many to be a milestone in how online identities and transactions are being aligned in legal terms with their physical world counterparts.

Part of the directive covers “Qualified Certificates” – digital certificates that have been issued to validated entities, and whose identities are contained within the certificate itself.

Comodo’s InstantSSL Certificates contain the following critical identification information within the SSL Certificate:

- Common Name – the fully qualified domain name for which the SSL Certificate is to be used
- Organization Name
- Organization Unit
- Street Address
- City / Town
- State / Province
- Zip / Postal Code
- Country

All the above information is validated quickly and efficiently by Comodo, ensuring customers receive their Certificate quickly but without the risks associated with weak validation. This places Comodo at the forefront in delivering SSL Certificates that comply with legislation even before it becomes law to do so!

InstantSSL – combining strong validation with low costs

Comodo is the only SSL Provider to offer responsible companies the option of low cost, fully validated and highly trusted SSL certificates. With the availability of InstantSSL, there is no longer any need to opt for more expensive nonvalidated, untrustworthy encryption-only SSL certificates.

About Comodo

The Comodo group of companies is a leading global provider of fixed and mobile endpoint management, Unified Threat Management and Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication software, Network Vulnerability Scanning and PCI Compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintain an extensive suite of endpoint security software and services for businesses and consumers.

Innovation, a core competence in PKI, and a commitment to combat Internet-crime, distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 businesses and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in fixed and mobile online transactions.

enterprise.comodo.com

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.(888).266.6361
enterprisesolutions@comodo.com