What are SSL and Digital Certificates?

Secure Socket Layer (SSL) is a protocol developed by Netscape in 1996 which quickly became the method of choice for securing data transmissions across the Internet. SSL is an integral part of most Web browsers and Web servers and makes use of the public-and-private key encryption system developed by Rivest, Shamir, and Adleman.

In order to make an SSL connection, the SSL protocol requires that a server should have a digital certificate installed. A digital certificate is an electronic file that uniquely identifies individuals and servers. Digital certificates serve as a kind of digital passport or credential which authenticate the server prior to the SSL session being established.

Typically, digital certificates are signed by an independent and trusted third party to ensure their validity. The "signer" of a certificate is known as a Certification Authority (CA), such as VeriSign, thawte and GeoTrust.

When should SSL be used and what can it secure?

There are two main online security problems that SSL certificates help solve:

- Authentication - proving a company's (or server's) identity online and in so doing create a sense of trust and confidence in using a Web site.
- Encryption - offering protection for the data submitted to a Web site (or between servers) so that in the event of interception, it will be unintelligible without the unique key used for decryption.

Solving these security problems allows online business to protect against the following scenarios:

- Spoofing - The low cost of Web site design and ease with which existing pages can be copied makes it all too easy to create illegitimate sites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional-looking storefronts that mimic legitimate businesses.
- Unauthorized Disclosure - when information is transmitted "in the clear", making it possible for hackers to intercept the transmissions and obtain sensitive information from customers.
- Data alteration - the content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card, and social security numbers as well as currency amounts; indeed any information sent "in the clear" is all vulnerable to alteration.

So what are the practical applications of SSL certificates?

Firstly, looking at categories of data, the most common deployment is for securing transmission of financial information in ecommerce. However, with incidence of identity theft on the rise, protecting the transmission of a broad range of personally-identifiable information is becoming ever more important. This category of data would include identity and social security numbers, e-mail addresses and demographic information as well as account registration and login information.

In terms of applications and protocols, SSL Certificates can be used to secure the following:

- Web Servers
- Mail Servers
- Databases
- FTP Sites
- Internet Chat
- NNTP