This is a digital certificate, with a digital signature, that verifies that a website is who they say they are. When you connect to a web site using SSL (HTTPS), your browser says, "Papers, please!" The remote site then sends the SSL Web Site Certificate to your browser. Your browser then verifies the authenticity of this "passport". Once verified, encrypted communications ensue. The point of the SSL Web Site Certificate is that under no circumstances should anyone else be able to create a valid, signed certificate for a web site that they do not own and operate. In order to obtain an SSL Web Site Cert, you must verify by varied means that you are the owner and operator of the web site involved. **So, using HTTPS is not only for encryption of communications, but also a way to verify that the site you are communicating with is the Real Thing, and not an imposter.**

An SSL certificate keeps you and your customer's safe by protecting the information that's flowing to and from your website. It encrypts names, addresses, passwords, account and credit card numbers and more so hackers and other online criminals can't read them.

An SSL certificate serves as an electronic "passport." It establishes the website's authenticity and credibility and enables the browser and Web server to build a secure, encrypted connection. Credibility is established by checking the digital certificate, which includes:

- The Certificate holder's name (individual or company)
- The Certificate's serial number and expiration date
- A copy of the Certificate holder's "public" cryptographic key
- The digital signature of the Certificate-issuing authority

Once a visitor is on an SSL-protected page, the following visual indicators appear to show them that your site is secure and to give them the confidence to proceed:

- A "padlock" icon in the browser's status bar
- The https:// prefix in the URL