

Site Security

What is SSL? Encrypted 1003 The Encrypted 1003 utilizes secure socket layer (SSL). This allows web browsers (e.g. Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox) to communicate with our server in a secure SSL encrypted session. It is often used to securely transfer credit card numbers and other sensitive information. **Fraud Protection** These security features protect transactions from misappropriation and fraud that could otherwise occur as information passes through Internet computers. Without thorough security, information transmitted over the Internet is susceptible to fraud and other misuse by intermediaries. **Complete Protection** The Internet does not provide built-in security. This is why our 1003 residential loan application is not e-mailed. To increase security and privacy, we will be notified via e-mail of your completed 1003 application and we are required to access the completed 1003 via encryption, username, and password. The SSL protocol delivers server authentication, data encryption, and message integrity.

How does it work? Client/Server Protocols SSL is layered beneath application protocols such as HTTP, Telnet, FTP, Gopher, and NNTP, and layered above the connection protocol TCP/IP. This strategy allows SSL to operate independently of the Internet application protocols. With SSL implemented on both the client and server, your Internet communications are transmitted in encrypted form, ensuring privacy. Due to this encryption process, documents that are encrypted may take longer to download. **Digital Certificates** Web browsers deliver server authentication using signed digital certificates issued by trusted third parties known as certificate authorities. A digital certificate verifies the connection between a server's public key and the server's identification (just as a driver's license verifies the connection between your photograph and your personal identification). Cryptographic checks, which check digital signatures, ensure that information within a certificate can be trusted. **Web Addresses** You can tell whether a document comes from a secure server by looking at the Universal Resource Locator (URL) field. If the URL begins with https:// (instead of http://), the document comes from a secure server. You need to use https:// for URLs with SSL and http:// for URLs without SSL.

What does a digital certificate do? Public/Private Key Pairs Digital Certificates are protected by public and private key pairs linked by a powerful cryptographic algorithm. These keys have the ability to encrypt and decrypt information. No one else's keys can decipher messages you send that are encrypted with your public key. Also, no one else's keys can be used to pose as you by sending messages encrypted with your private key. **Digital Certificates** Web browsers deliver server authentication using signed digital certificates issued by trusted third parties known as certificate authorities. A digital certificate verifies the connection between a server's public key and the server's identification (just as a driver's license verifies the connection between your photograph and your personal identification). Cryptographic checks, which check digital signatures, ensure that information within a certificate can be trusted. **Web Addresses** You can tell whether a document comes from a secure server by looking at the Universal Resource Locator (URL) field. If the URL begins with https:// (instead of http://), the document comes from a secure server. You need to use https:// for URLs with SSL and http:// for URLs without SSL.