SSL

07/23/2024 13:03:37

FAQ Article Print

Category:	RRZE: Glossary	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	12:39:47 - 07/16/2010

Keywords

Identity, Security

Symptom (public)

Problem (public)

Solution (public)

Secure Socket Layer protocol. The SSL protocol uses private and public keys to authenticate a service provider's web server to the browser. The protocol also creates encryption keys to protect the integrity and confidentiality of information at it traverses the Internet. The server generates a short-term public/private key pair using a long term private key belonging to the server. The server periodically changes its short term private key, discarding any previous versions and the client uses the short-term public key to encrypt a symmetric key for use during the session. This renders records of previous sessions un-decryptable. Sometimes referred to as providing "perfect forward secrecy". A Hardware Security Module (HSM) is often used both to securely store the private keys and to accelerate the encryption-decryption process.

Standards include ISO 11770 (guidelines for key management), ISO 9564 and ISO 16609 (retail financial transactions for PIN encipherment and message authentication, respectively). ISO 1568 (management of keys used in the retail banking environment - interfaces between a card-accepting device, acquirer, card issuer and a key-holding device).

Source: "http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html"