**SET, PCT, IETF AND SSL**

Kevin Wamuiga Kamau

P15/35060/2015

13-Dec-2018

The Private Communication Technology (PCT) protocol is designed to provide privacy between two communicating applications (a client and a server), and to authenticate the server and (optionally) the client. PCT assumes a reliable transport protocol (e.g., TCP) for data transmission and reception.

Secure socket layer is an encryption mechanism for order taking, queries and other applications. It does not protect against all security hazards and is mature, simple and widely used. SSL Phases: Handshake where server authentication and key establishment occur and data transfer. It is not a payment protocol and can be used for any secure communications, like credit card numbers. Uses enveloping where RSA is used to exchange DES keys.

Secure Electronic Transaction provides privacy, authenticity, integrity and repudiation. It is used very infrequently due its complexity and the need for a special card reader by the user. It may be abandoned if it is not simplified/improved.

The Internet Engineering Task Force (IETF) is an open [standards organization](https://en.wikipedia.org/wiki/Standards_organization), which develops and promotes voluntary [Internet standards](https://en.wikipedia.org/wiki/Internet_standard), in particular the standards that comprise the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite) (TCP/IP). It works on a broad range of networking technologies which provide foundation for the Internet's growth and evolution such as: Automated network management, Internet of things. New transport technology, IETF areas and Token Binding Protocol.

The SET protocol differs from SSL chiefly, which differs from SSL's in a number of respects:

* SET is tailored to the credit card payment to the merchants while SSL is a protocol for general-purpose secure message exchanges.
* SET protocol hides the customer’ credit card information from merchants, and also hides the order information to banks, to protect privacy. This scheme is called dual signature. While SSL protocol may use a certificate, but there is no payment gateway. So, the merchants need to receive both the ordering information and credit card information, because the capturing
* SET, which was specifically designed to address the security of all parties to an electronic payment transaction, incorporates 1024-bit encryption throughout the entire transaction. SSL, on the other hand, which was developed only to prevent data tampering in client/server applications, has comparatively weaker encryption, at a maximum of 128-bit.

The PCT protocol differs from SSL chiefly in the design of its handshake phase, which differs from SSL's in a number of respects:

* The round and message structures are considerably shorter and simpler: A reconnected session without client authentication requires only one message in each direction, and no other type of connection requires more than two messages in each direction.
* Negotiation for the choice of cryptographic algorithms and formats to use in a session has been extended to cover more protocol characteristics and to allow different characteristics to be negotiated independently. The PCT client and server negotiate, in addition to a cipher type and server certificate type, a hash function type and a key exchange type. If client authentication is requested, a client certificate type and signature type are also negotiated.
* Message authentication has been revamped so that it now uses different keys from the encryption keys. Thus, message authentication keys may be much longer (and message authentication therefore much more secure) than the encryption keys, which may be weak or even non-existent.

**REFERENCES**

- ["IETF and the Internet Society"](http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society), Vint Cerf, Internet Society, 18 July 1995. Retrieved 21 July 2014.

- R.L. Rivest, A. Shamir, L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" MIT Laboratory for Computer Science and Department of Mathematics, S.L. Graham, R.L. Rivest ed. Communications of the ACM, February 1978 (Vol 21, No. 2) pages 120-126.