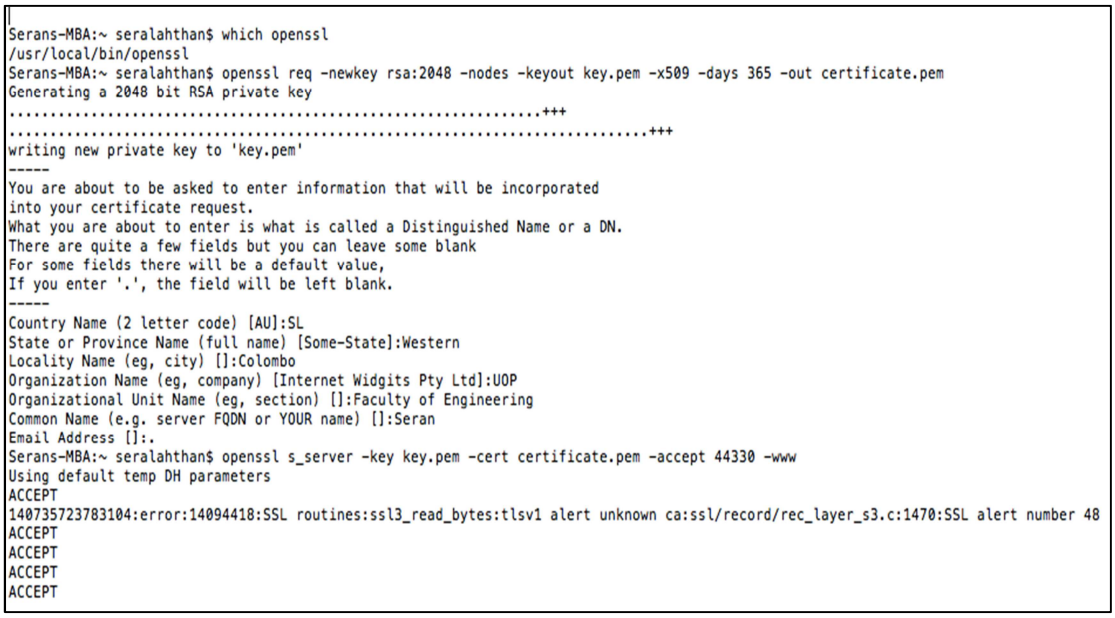

Fig. 7 shows generation of RSA private key certificate for connecting with the local server.

IV. CONCLUSIONS

In this work we implement the protocol P1 (eCK-secure and NAXOS trick free authenticated key exchange protocol) to be used with the widely-used OpenSSL cryptographic library. OpenSSL implementations are widely used with the real-world security protocol suites, such as Security Socket Layer and Transport Layer Security. According to our understanding, this is the first OpenSSL implementation of an eCK-secure key exchange protocol. Thus, our work opens up the direction to use the recent advancements of cryptography for betterment of the real-world Internet communication.

As a future work, we aim to implement a leakage-resilient AKE protocols [9], [13]-[15] for OpenSSL, which is resilient to wide range of side-channel attacks, in addition to eCK security.

ACKNOWLEDGMENT

This research is supported by Faculty Computer Science, UTHM, Malaysia and Information Technology (FSKTM), Research Management Centre (RMC), H082 Tier 1/2018 and Gates IT Solution Sdn. Bhd. under its publication scheme.

REFERENCES

[1] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory 20(6), pp 644-654, 1976.

[2] V. Boyko, P. MacKenzie, and S. Patel, *Provably Secure Password-authenticated Key Exchange using Diffie-Hellman*, EUROCRYPT 2000, pp 156 – 171, Springer, 2000.

[3] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, *Authentication and Authenticated Key Exchanges*, Des. Codes Cryptography 2(2), pp107 – 125, 1992.

[4] A. Fujioka, K. Suzuki, and B. Ustaoglu, *Utilizing Postponed Ephemeral and Pseudo-Static Keys in Tripartite and Identity-based Key Agreement Protocols*, IACR Cryptology ePrint Archive, 2009:423, 2009.

[5] D. P. Jablon, *Strong Password-only Authenticated Key Exchange*, SIGCOMM Computer Communication Revise 25(5), pp 5 – 26, 1996.

[6] H. Krawczyk, *HMQV: A High-performance Secure Diffie-Hellman Protocol*, CRYPTO 2005, pp 546 – 566, Springer, 2005.

[7] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, *An Efficient Protocol for Authenticated Key Agreement*, Des. Codes and Cryptography 28(2), pp 119—134, Springer, 1998.

[8] B. A. LaMacchia, K. E. Lauter, and A. Mityagin, *Stronger Security of Authenticated Key Exchange*, Provsec 2007, pp 1 – 16, Springer, 2007.

[9] J. Alawatugoda, D. Stebila, and C. Boyd, *Continuous After-the-fact Leakage-resilient eCK-secure Key Exchange*, IMA Cryptography and Coding 2015, pp. 277 – 294, Springer, 2015.

[10] M. Bellare and P. Rogaway, *Entity Authentication and Key Distribution*, CRYPTO 1993, pp 232 – 249, Springer, 1993.

[11] M. Bellare and P. Rogaway, *Provably Secure Session Key Distribution – The Three Party Case*, STOC 1995, pp 57 – 66, 1995.

[12] R. Canetti and H. Krawczyk, *Analysis of Key-exchange Protocols and Their Use for Building Secure Channels*, EUROCRYPT 2001, pp 453 – 474, Springer, 2001.

[13] J. Alawatugoda, *Generic construction of an eCK-secure key exchange protocol in the standard model*, International Journal of Information Security 16(5), pp 541 – 557, Springer, 2017

[14] J. Alawatugoda, *On the leakage-resilient key exchange*, Journal of Mathematical Cryptology 11(4), pp 541 – 557, Springer, 2017

[15] S. Chakraborty, J. Alawatugoda and C. Pandu Rangan, *Leakage-resilient non-interactive key exchange in the continuous-memory leakage setting*, Provsec 2017, pp167—187, Springer, 2017