Dalam simulasi protokol Fiat Shamir ini, akan melibatkan tiga entitas, yaitu Denis sebagai pihak prover, Erlang sebagai pihak verifier, dan Ruft sebagai pihak Trusted Center. Simulasi ini membutuhkan input dari Trusted Center, prover, dan verifier, dimana nilai-nilai tersebut akan dibuktikan oleh pihak verifier, bahwa nilai yang diberikan oleh pihak prover adalah nilai yang benar atau valid.

5. Kesimpulan

Di era perkembangan ilmu pengetahuan dan teknologi, penggunaan *password* dalam teknik otentikasi merupakan teknik yang bersifat tidak aman dan lemah, karena memiliki beberapa serangan dan kelemahan yang dapat dimanfaatkan oleh pihak-pihak yang tidak berwenang. Salah satu solusi yang dapat digunakan untuk mengatasi kelemahan-kelemahan yang terdapat pada penggunaan *password* adalah dengan menggunakan protokol *Zero Knowledge*, dalam hal ini adalah protokol Fiat Shamir yang memanfaatkan *challenge and response* sebagai bentuk otentikasinya, sehingga diharapkan tidak terdapat lagi kelemahan dan serangan yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk merugikan kita.

6. Daftar Pustaka

[1.] Kromodimoeljo, Sentot. (2010). *Teori dan Aplikasi Kriptografi*. SPK IT Consulting. [2.] Nindya Neyman, Shelvie. Identifikasi dan Otentikasi Entitas.

[3.] Menezes, Alfred J., Ooschot, Paul C. Van. & Vanstone, Scott A. (1997). *Handbook of Applied Cryptography*. Boca Raton : CRC press LLC.

[4.] Schneier, Bruce. (1996). *Applied Cryptography : Protocol, Algorithms and Source Code in C*. John Willey & Sons, Inc.

[5.] Stalling, Wiliams. (1999). *Cryptography and Network Security : Principles and Practice 4nd Edition*. New Jersey : Prentice Hall, Inc.

[6.] Sumarkidjo, dkk. (2007). *Jelajah Kriptologi*. Buku tidak diterbitkan. Jakarta. Lembaga Sandi Negara Republik Indonesia.