## ABSTRAK

Dewasa ini aplikasi berbasis *web* telah menjadi hal yang umum, dan setiap aplikasi yang telah dibangun memerlukan proses otentikasi untuk memvalidasi identitas dari pengguna yang akan menggunakan layanan pada applikasi tersebut, sehingga meyebabkan pengguna harus *login* kembali jika berganti aplikasi, hal menimbulkan terjadinya banyaknya proses otentikasi. Hal ini dapat dihindari dengan mengintegrasikan sebuah *central authentication service* atau CAS agar aplikasi berbasis *web* yang telah ada dapat di *Single Sign On*-kan, sehingga semua proses otentikasi akan ditangani oleh *central authentication service* dan proeses otentikasi dapat disederhanakan.

Dangan proses otentikasi pada aplikasi berbasis *web* ditangani oleh *central authentication service* atau CAS, maka CAS harus dapat memberikan otentikasi yang kuat, salah satu metode yang dapat dilakukan adalah dengan mengunakan *Lightweight Directory Access Protocol* (LDAP) sebagai *datastore* dan *Remote Accses Dial In User* (RADIUS) sebagai *backend* dari *central authentication service* guna menghasilkan sebuah sistem *Single Sign On (SSO)* terintregrasi berbasis CAS ,LDAP dan RADIUS.

Dengan memusatkan data pengguna pada LDAP dan membebankan proses otentikasi pada RADIUS dan mengintegrasikan keduanya ke dalam CAS telah berhasil membentuk sebuah sistem SSO yang cukup stabil dan dapat diandalkan dengan tingkat keberhasilan *login* sepuluh kali berturut-turut dangan menggunakan data sample acak dari 1000 *entry* yang ada, serta berhasil meningkatkan keamanan informasi/data pengguna dengan terenkripsinya data pengguna melalui protokol RADIUS yang dapat dibuktikan dengan hasil *sniffing* pada *port* 1812.



Kata kunci:otentikasi, *Central Authentication Service*, LDAP, *OpenLDAP*, RADIUS, CAS.

## *ABSTRACT*

*Along with The universality of the HTTP protocol seduced developers for quite long time most applications are web-based today. Many of them requires authentication process to validate the identity of users who are entitled to use the service. so that causes a user must log in again if you change the application, it lead to having multiple authentication process. This can be avoided by integrating a central authentication service or CAS on existing web-based application so all the authentication process will be handled by a central authentication service and authentication can be simplified proeses.*

*With authentication process in web-based applications are handled by a central authentication service or CAS, the CAS should be able to provide strong authentication, one of the methods that can be done is by using Lightweight Directory Access Protocol (LDAP) as the datastore and Accses Remote Dial In User (RADIUS) as the backend of a central authentication service in order to produce a system of Single Sign On (SSO) based terintregrasi CAS, LDAP and RADIUS.*

*By centralizing user data in LDAP and RADIUS authentication process imposes and integrate them into the CAS has successfully established an SSO system is quite stable and reliable with a login success rate ten times in a row view using a random sample of data from the 1000 entry that exist, as well as managed to improve information security / user data with user data terenkripsinya through RADIUS protocol that can be proven by the results of sniffing on port 1812.*



*Keyword : Authentication, Central Authentication Service , LDAP, OpenLDAP, RADIUS, CAS.*