Proceedings CLME2017/VCEM
8º Congresso Luso-Moçambicano de Engenharia / V Congresso de Engenharia de Moçambique
Maputo, 4-8 Setembro 2017; Ed: J.F. Silva Gomes *et al*.; Publ: INEGI/FEUP (2017)

ARTIGO REF: 6618

SISTEMA DE AUTENTICAÇÃO CENTRALIZADA E *SINGLE-SIGN ON* UNIFICADO BASEADO NO *CENTRAL AUTHENTICATION SERVICE* PARA SERVIÇOS WEB NO ISUTC

Vanessa dos Santos Mabunda[1(*)], Fernando Mira da Silva[2]

[1]Instituto Superior de Transportes e Comunicações (ISUTC) - Maputo, Moçambique
[2]Instituto Superior Técnico (IST) - Lisboa, Portugal
[(*)]*Email:* vanessa.mabunda@isutc.transcom.co.mz

RESUMO

Os sistemas de informação são a base para o desenvolvimento de actividades em quase todo o tipo de organizações. Estes sistemas são geralmente compostos por aplicações desktop ou até mesmo aplicações Web. Por questões de segurança, estas aplicações só podem ser manipuladas por utilizadores autorizados, por isso, requerem uma autenticação. A tendência convencional é de os utilizadores possuírem as suas identidades associadas a cada aplicação, fazendo desta forma que os mesmos se autentiquem para cada aplicação que pretendem utilizar, dentro do domínio da organização.

A melhoria da usabilidade dos sistemas de informação, seja em sistemas de *e-government*, académicos ou de outra natureza aconselha a utilização de sistemas centralizados e federados de autenticação e *Single Sign-on*, de forma a garantir a consistência e segurança de credencias e evitando a multiplicação de utilizadores e senhas. A autenticação centralizada garante que em um domínio organizacional as informações de identidade sejam mantidas por um único sistema, eliminando os múltiplos conjuntos de credenciais e não só: é possível implementar a tecnologia *Single Sign-On* [Oubraski, 2009], para permitir que o utilizador se autentique uma única vez, permitindo a cada utilizador acesso a todos os recursos pretendidos [Peltier, 2007] com uma autenticação e credenciais únicas.

Neste trabalho descreve-se a implementação no ISUTC de um Sistema de Autenticação Centralizado utilizando CAS, discutindo-se em particular a arquitetura adotada, as funcionalidades implementadas e as garantias de segurança e privacidade dos dados associadas. No ISUTC a autenticação é feita com recurso ao *Lightway Directory Access Protocol* (LDAP). Por questões de segurança, o LDAP é comummente utilizado para facilitar a autenticação centralizada utilizando o conjunto *username* e *password*. [Mularien, 2012]. Aos utilizadores da rede do ISUTC são disponibilizadas algumas diversas Web com fins académicos e de gestão de sistemas. Para que um utilizador seja autenticado por um serviço Web, uma ligação entre este serviço e o repositório de credenciais LDAP é criada com o objectivo de garantir a autenticidade das credenciais introduzidas.

O Web SSO proporciona o SSO entre um servidor Web seguro e aplicações Web. Este tipo de SSO pode eliminar a necessidade de se iniciar a sessão duas vezes, quando um cliente tenta aceder a um recurso Web em um servidor que requer autenticação para registar o seu próprio utilizador. [Buecker, 2012]

O *Central Authentication Service* (CAS) é um *framework* de código aberto que implementa o mecanismo SSO para proporcionar uma autenticação centralizada a um único servidor e redireccionamentos HTTP. [Ardagna, 2006] A sua integração com aplicações Web pode ser

feita com recurso a módulos no servidor aplicacional ou na aplicação Web, através de clientes CAS. A arquitectura do sistema CAS é formada pelo modelo cliente-servidor que se comunicam por meio de vários protocolos. [Jasig, 2015]

Uma vez que o CAS proporciona autenticação ele comunica-se com repositório de credenciais existente, o LDAP. Somente o CAS tem acesso a esse repositório, desempenhando assim o papel de Provedor de Identidade às aplicações. Deste modo, todas as aplicações Web do ISUTC passam a recorrer ao CAS para autenticar os seus utilizadores. Sempre que um utilizador aceder a qualquer aplicação Web protegida pelo CAS, ele será redireccionado ao servidor CAS para que este o autentique. A arquitectura do Sistema de Autenticação Unificado descrito é apresentada na Figura 1. Com a implementação do CAS, as aplicações passam a tomar decisões de autorização com base nos atributos dos utilizadores, graças ao protocolo SAML. Esta arquitectura permite também a sua adoção por aplicações que não possuem internamente um mecanismo de autenticação próprio.

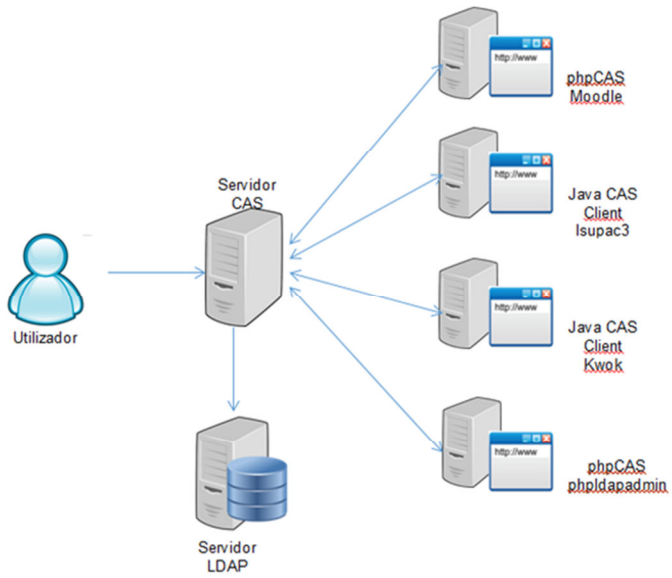

Fig. 1 - Sistema de Autenticação Unificado.

Discute-se igualmente como o sistema descrito pode facilmente ser estendido a outras organizações e serviços públicos e integrado em sistemas de federação de identidades, permitindo a integração da autenticação de serviços autónomos.

REFERÊNCIAS

[1]-Ardagna, Claudio Agostino, Ernesto Damiane, Sabrina De Capitane di Vimercati, Fulvio Frati, e Pierangela Samarati. “Cas++: An Open Source Single Sign-On Soution for Secure e-services.” In Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11, de Louise Yngs, Simone Fischer-Hübner e Kai Rannenberg, 208-215.

[2]-Buecker, Axel, Nilesh Patel, Dirk Rahnenfuehrer, e Joris Van Herzele. “Enterprise Single Sign-On Design Guide.” IBM. Setembro de 2012.

[3]-Jasig. Architecture. 2015. http://jasig.github.io/cas/4.0.x/planning/Architecture.html (acedido em 12 de Maio de 2015).

[4]-Mularien, Peter, e Robert Winch. Spring Security 3.1. Packt Publishing, 2012.

[5]-Oubraski, Ido. CompTIA Security+ Certification Study Guide. Elsevier, Inc., 2009.