Identity Authentication and Data Access Authorization in Regional Education Informatization

Qi Feng, ZhongLin Chen, Fuke Shen
East China Normal University, North Zhongshan Road Campus: 3663 N. Zhongshan Rd., Shanghai,China
YuHong Zhu
Information Center, Shanghai Municipal Education Commission: 25N, WeiHai Rd.,Shanghai,China

Abstract:
During the procedure of the Region-informatization, various kinds of challenges need to be faced. As the main roles in the construction process, Governments, Universities, enterprises build their own information systems which cannot be interoperable due to lack of interconnection standard. So these systems’ effective data-sharing mechanism is a key issue. In this paper, from the top design of informatization eco-system, we are going to discuss the roles which these participant play and the mechanism which these participants’ system to interconnect, so that we can improve the development of Region-informatization. We take the Authentication System built in Shanghai Education as example and show the process, design, implementation and the current situation in detail.

Authentication Scheme:
To support multiple construction participants and users from multiple educational institutes, authentication must be completed by the organization itself. The authentication results of multiple organizations need to be trusted by each other in the regional federation. Shibboleth is an open source and a quite effective solution to this problem.

Shanghai Education Authentication Center:
Shanghai Education Authentication Center (SEAC) provide authentication, authorization and data-sharing for Shanghai education user. Shibboleth provides a cross-organization authentication framework and provides a nice solution for the authorization based on user attributes. However, the authorization for the application is relatively simple, which is based on the distributed authorization of the authentication node, and it is lacking of centralized authorization management. Also, the authentication data transfer to the application is also lacking of standards. The framework of distributed architecture must be centrally managed to support cooperation of multiple bodies. Therefore, we need a centralized authorization management policy to coordinate the application and authentication nodes. But, the existing distributed authentication framework cannot be abandoned. In our design, we integrate oauth2 with shibboleth. SEAC’s solution is, authentication management by oauth2 and distributed authentication by shibboleth.

Performance:
As shown in the following figure, Shanghai SEAC’s request appears periodically during the semester, and low in the summer and winter holidays. This is because in the term of weekends, teachers and students have frequent cross-organization communication, thus more use of wireless communication based on SEAC.