ỨNG DỤNG SINGLE SIGN ON TẠI TRUNG TÂM THÔNG TIN – THƯ VIỆN, ĐẠI HỌC QUỐC GIA HÀ NỘI

Phạm Thành Quang*

Tóm tắt: *Một trong những khía cạnh quan trọng của người dùng mạng Internet ngày nay đó là việc bảo mật, quản trị tài khoản cá nhân của mình. Single Sign On (SSO) là một phương pháp kiểm soát truy cập cho phép người dùng xác thực một lần và được truy cập vào các tài nguyên của nhiều phần mềm hệ thống. Bài tham luận này chỉ ra rằng SSO là một trong những giải pháp đăng nhập một lần mang đến sự thuận tiện, hiệu quả cho người dùng khi đã được minh chứng bởi nhiều thương hiệu lớn trên thế giới.*

Từ khóa: *Thư viện số; Đăng nhập một lần; Xác thực tài khoản; Bảo mật thông tin*

MỞ ĐẦU

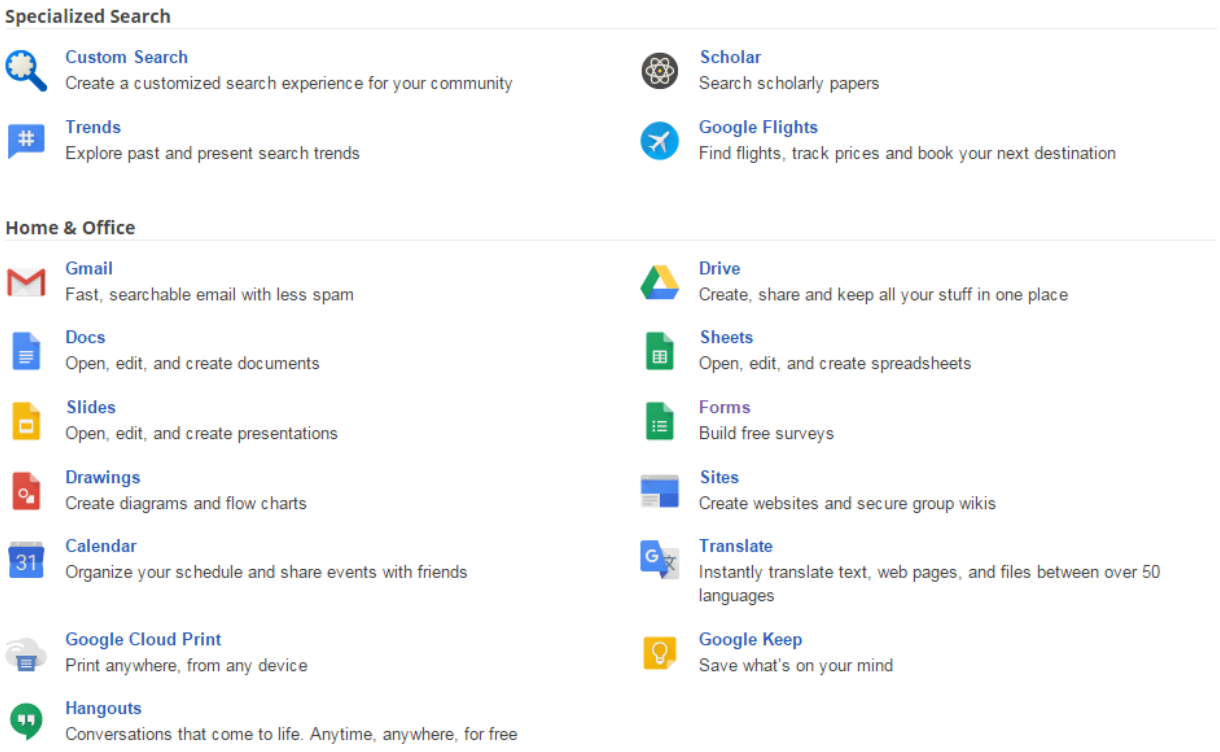
Trong thời đại phát triển mạnh mẽ của hệ thống mạng máy tính như hiện nay, xu hướng các dịch vụ cùng nhau chia sẻ dữ liệu người dùng đang là hướng phát triển chung của công nghệ thông tin, một người dùng phải quản lý rất nhiều tài khoản, mật khẩu cho các dịch vụ, ứng dụng mà họ tham gia. Khi người sử dụng phải lưu trữ quá nhiều các thông tin bí mật như trên sẽ dẫn đến những vấn đề như không đảm bảo tính an ninh, an toàn và tăng thêm những chi phí khác. Do vậy nhu cầu đăng nhập một lần – Single Sign On (SSO) cho các ứng dụng và dịch vụ này là rất cấp thiết. Cơ chế SSO đảm bảo cho người dùng hợp pháp có thể truy nhập vào rất nhiều những dịch vụ khác nhau trên hệ thống mạng phân tán nhưng chỉ phải sử dụng một tài khoản duy nhất. Người sử dụng chỉ cần đăng ký và đăng nhập duy nhất một lần vào hệ thống, khi đó trong phiên làm việc của mình họ có thể truy cập ngay lập tức vào các dịch vụ liên kết của hệ thống phân tán mà không phải đăng ký thêm định danh và thông qua quá trình đăng nhập lần nữa. Hiện nay có nhiều phương pháp khác nhau được đưa ra nhằm mục đích ứng dụng cơ chế này, nhưng trên các thử nghiệm thực tế hầu hết các phương pháp đó đều không ngăn chặn được các tấn công một cách có chủ ý từ bên ngoài. Một số phương pháp có kèm theo cơ chế đồng bộ thời gian để loại bỏ các truy nhập trái phép, nhưng điều đó dẫn đến việc tăng chi phí tính toán. Với qui mô và tầm vóc của một thư viện đại học lớn sắp tròn tuổi 20, Trung tâm Thông tin – thư viện, ĐHQGHN đã đi tiên phong trong việc triển khai giải pháp SSO giúp người sử dụng chỉ cần dùng một tài khoản và mật khẩu SSO duy nhất có thể sử dụng được tất cả các ứng dụng tin cậy. Single Sign On đã được nhiều tổ chức, công ty trên thế giới nghiên cứu và phát triển, tuy nhiên tại Việt Nam đây vẫn là lĩnh vực còn khá mới.

* Phòng Quản trị Công nghệ thông tin, Trung tâm Thông tin – Thư viện, Đại học Quốc gia Hà Nội

1. Giới thiệu Single Sign On

SSO là một cơ chế xác thực yêu cầu người dùng đăng nhập vào chỉ một lần với một tài khoản và mật khẩu để truy cập vào nhiều ứng dụng trong một phiên làm việc (session). Trước khi có SSO, một người sử dụng đã phải nhập các tài khoản và mật khẩu cho từng ứng dụng mỗi khi họ đăng nhập vào các ứng dụng khác nhau hoặc các hệ thống trong cùng một phiên. Điều này rõ ràng có thể tốn nhiều thời gian, đặc biệt là trong môi trường thông tin đa phương tiện như hiện nay, khi mà người sử dụng phải đăng nhập mỗi khi họ truy cập vào một hệ thống mới từ máy tính của họ. Do vậy, với hệ thống có nhiều website và ứng dụng thì việc sử dụng SSO là rất cần thiết nhằm đem lại nhiều thuận tiện cho người dùng và tăng tính năng bảo mật.

Ví dụ: người dùng sử dụng các dịch vụ của google: gmail, scholar, youtube, google plus, drive… khi chưa có SSO thì với mỗi dịch vụ ta phải nhập thông tin để xác thực. Với SSO người dùng chỉ cần sử dụng một email duy nhất của google để có thể đăng nhập và khai thác sử dụng tất cả các dịch vụ và ứng dụng của google. Điều đó thực sự mang lại sự thuận tiện và tiết kiệm thời gian cho người dùng tin, khi không phải đăng kí bất kì tài khoản nào khác nữa.



Một số ứng dụng và dịch vụ của Google

Đăng nhập là quá trình người dùng sử dụng định danh và các thông tin bí mật khác thiết lập một kết nối bảo mật với hệ thống, định danh và các thông tin bí mật của người dùng đã được người dùng đăng ký từ trước với hệ thống. Quá trình người dùng đăng nhập bao gồm hai bước xác thực và ủy quyền, trong đó:

•**Xác thực (Authentication)**: Kiểm tra một người dùng có hợp lệ hay không thông qua các phương thức xác thực của hệ thống. Xác thực được coi là cốt lõi của quá trình đăng nhập trong một hệ thống thông tin. Chúng ta có thể sử dụng các phương pháp xác thực như: username, password, thẻ thông minh, hay dùng sinh trắc học…

•**Ủy quyền (Authorization)**: Là quá trình kiểm chứng một người dùng đã được xác thực có đủ quyền truy cập vào tài nguyên mà người dùng yêu cầu hay không. Tài nguyên yêu cầu có thể phụ thuộc vào chính sách tên miền (cấp quyền theo tên miền) hoặc một chính sách đặc biệt nào đó (ví dụ cấp quyền theo cấp).

SSO chỉ được triển khai sau khi đã xây dựng được hệ thống xác thực và phân quyền. SSO có nhiệm vụ cung cấp cho người dùng quyền truy cập nhiều tài nguyên web, các ứng dụng trong phạm vi cho phép chỉ với một lần đăng nhập (xác thực).

2. Các giải pháp đăng nhập một lần

Hiện nay có khá nhiều giải pháp SSO được giới thiệu và đưa vào sử dụng trên thực tế:

- Open Single SignOn (OpenSSO) hoạt động dựa trên Token.
- Central Authentication Service (CAS)
- Tivoli Access Manager for Enterprise Single SignOn.
- Java Open SSO (JOSSO)

Tại Trung tâm TT-TV, ĐHQGHN hệ thống xác thực truy nhập một lần được triển khai ứng dụng theo mô hình Central Authentication Service (CAS). CAS là một giải pháp SSO mã nguồn mở được phát triển bởi đại học Yale, với các tính năng như sau:

- CAS hỗ trợ nhiều thư viện phía máy khách được viết bởi nhiều ngôn ngữ: PHP, Java, PL/SQL. Nó lấy thông tin SSO thông qua cookie. Cookie này sẽ bị hủy khi người dùng đăng xuất khỏi CAS hoặc đóng trình duyệt. Cookie được sinh ra bởi CAS, còn được gọi là Ticket Granting Cookie (TGC) chứa một ID duy nhất.

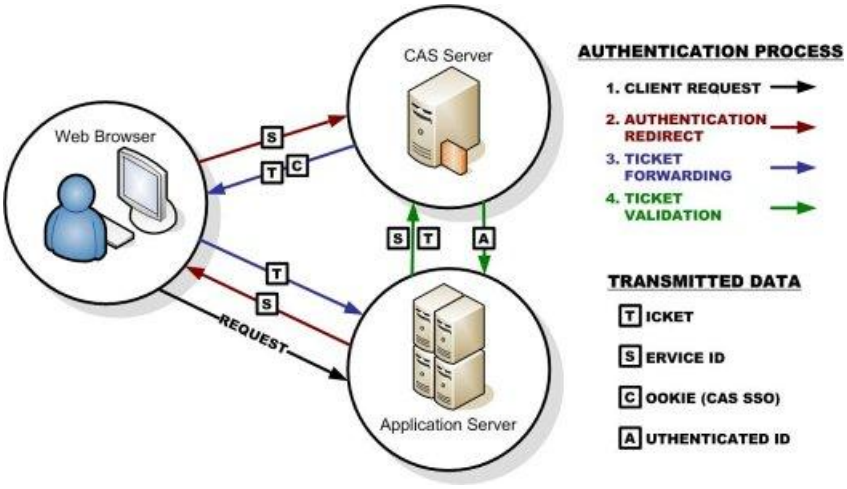
- CAS cung cấp nhiều trình quản lý xác thực (authenticate handler) khác nhau. CAS xác thực nhiều loại thông tin người dùng như tên truy cập/mật khẩu, chứng chỉ khóa công khai X509,... để xác thực những thông tin người dùng khác nhau này, CAS sử dụng những trình quản lý xác thực tương ứng.

- CAS cung cấp tính năng "Remember me". Người phát triển có thể cấu hình tính năng này trong nhiều file cấu hình khác nhau và khi người dùng chọn "Remember me" trên khung đăng nhập, thì thông tin đăng nhập sẽ được ghi nhớ với thời gian được cấu hình. Khi người dùng mở trình duyệt thì CAS sẽ chuyển đến service URL tương ứng mà không cần hiển thị khung đăng nhập.

Nguyên tắc chứng thực người dùng với máy chủ CAS hoạt động như sau:

- Người dùng nhập tên truy cập/mật khẩu vào khung đăng nhập. Các thông tin này được truyền cho CAS máy chủ thông qua giao thức HTTPS.

- Xác thực thành công, TGC được sinh ra và thêm vào trình duyệt dưới hình thức là cookie. TGC này sẽ được sử dụng để đăng nhập với tất cả các ứng dụng.



Mô hình giải pháp CAS

Hệ thống đăng nhập một lần thường gặp các vấn đề về bảo mật như sau:

- Vấn đề mật khẩu yếu: Sử dụng mật khẩu là phương phápxác thực được dùng phổ biến nhất hiện nay. Mật khẩu có thể được sử dụng nhiều lần và không được thay đổi trong thời gian dài để truy cập vào các ứng dụng là vấn đề thường gặp. Một phương pháp thông thường dùng để tấn công các mật khẩu yếu là đoán mật khẩu bằng cách sử dụng phương pháp tấn công từ điển. Chúng ta có thể khắc phục vấn đề này bằng cách thiết lập các chính sách mật khẩu mạnh.

- Vấn đề về hình thức đăng nhập: Nhà cung cấp dịch vụ tích hợp mẫu đăng nhập dành cho người dùng vào trong một trang nộidung của mình, và trong quá trình đăng nhập thông tin của người dùng sẽ được gửi trở lại cho nhà cung cấp dịch vụ để xác thực, nếu các thông tin này không được mã hóa sẽ dẫn đến vấn đề lộ định danh người dùng. Bên cạnh đó nếu các hệ mã hóa được sử dụng không đảm bảo an toàn thì cũng có thể dẫn đến các nguy cơ lộ thông tin về người dùng.

3. Ưu khuyết điểm của cơ chế đăng nhập một lần

3.1. Ưu điểm

- Tiết kiệm thời gian cho người sử dụng trong việc đăng nhập vào nhiều dịch vụ được cung cấp trên các nền tảng khác nhau của hệ thống phân tán.
- Tăng cường khả năng bảo mật thông qua việc giúp người sử dụng không cần nhớ nhiều thông tin đăng nhập (định danh và mật khẩu).
- Giúp cho người quản trị hệ thống tiết kiệm thời gian trong việc tạo lập hay loại bỏ người dùng trên hệ thống, cũng như thay đổi quyền của một hay một nhóm người dùng nào đó.
- Tiết kiệm thời gian khi tái lập lại mật khẩu cho người dùng.
- Bảo mật các cấp độ của việc thoát hay truy xuất hệ thống.
- Người phát triển ứng dụng không cần thiết phải hiểu và thực hiện nhận dạng bảo mật trong ứng dụng của họ, điều họ cần làm là liên kết đến một máy chủ định danh đã

được bảo đảm, việc này giúp những người dùng của họ có thể truy cập vào các dịch vụ khác cũng liên kết đến máy chủ đó như họ.

- Tạo nên sự đồng bộ giữa các dịch vụ và ứng dụng trong cùng một hệ thống thông tin phục vụ người dùng.

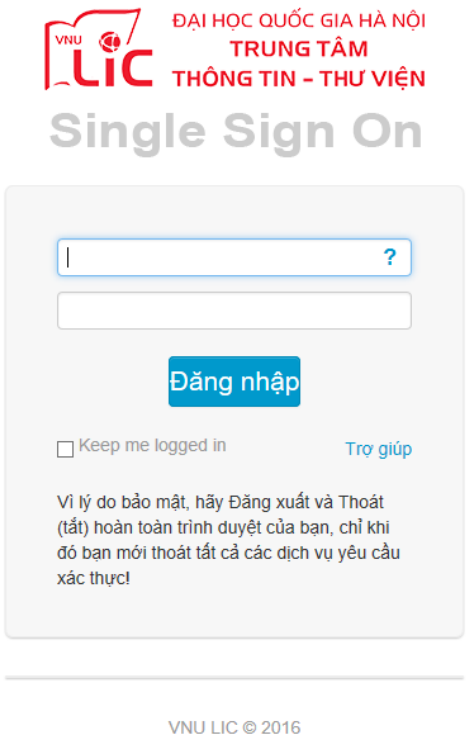
3.2. Khuyết điểm

- Đòi hỏi cơ sở hạ tầng của toàn bộ hệ thống phải bảo đảm.
- Do nhiều domain cùng sử dụng chung cơ sở dữ liệu người dùng nên việc xác thực khi người dùng đăng ký với hệ thống phải chặt chẽ, nếu không sẽ rất dễ vi phạm việc đảm bảo an ninh cho hệ thống.
- Cần có cơ chế xác thực đảm bảo khi truyền các thông tin định danh người dùng giữa người sử dụng với các máy chủ dịch vụ khác nhau.
- Chi phí để triển khai hệ thống SSO là rất tốn kém, cả về phần mềm, phần cứng lẫn nguồn nhân lực, cần phải có sự tính toán cẩn thận trước khi triển khai.

4. Ứng dụng thực tế tại Trung tâm TT – TV

Trung tâm Thông tin – Thư viện là một đơn vị trực thuộc Đại học Quốc gia Hà Nội (ĐHQGHN), được giao nhiệm vụ đảm bảo tài nguyên thông tin khoa học và công nghệ chất lượng cao, phục vụ đội ngũ cán bộ, giảng viên, nhà nghiên cứu và người học trong và ngoài ĐHQGHN. Chính vì vậy, Trung tâm cũng biết rằng trách nhiệm của mình là tạo sự thuận tiện, tiết kiệm thời gian, bảo mật dữ liệu tài khoản, tạo nên sự đồng bộ, khiến cho người dùng khai thác thông tin có cảm giác an tâm, thoải mái nhất. Cùng với việc khai trương trang website mới vào đầu năm 2016, hệ thống đăng nhập một lần được triển khai tích hợp cùng với các ứng dụng và dịch vụ của Trung tâm Thông tin – Thư viện. Hệ thống đã mang lại sự nhất quán giữa các dịch vụ và ứng dụng trong cùng một hệ thống của Trung tâm. Người dùng tin từ đó cũng cảm thấy an tâm, thuận tiện hơn khi tài khoản của họ được thống nhất trong khi sử dụng cùng một lúc các dịch vụ, ứng dụng khác nhau của Thư viện.

Giao diện SSO của Trung tâm TT – TV ra mắt đã được đánh giá rất cao về tính chuyên nghiệp, thể hiện sự tiên phong với tư cách là một đơn vị đi đầu về việc áp dụng các cơ sở công nghệ thông tin hiện đại nhất, theo xu hướng mới nhất.



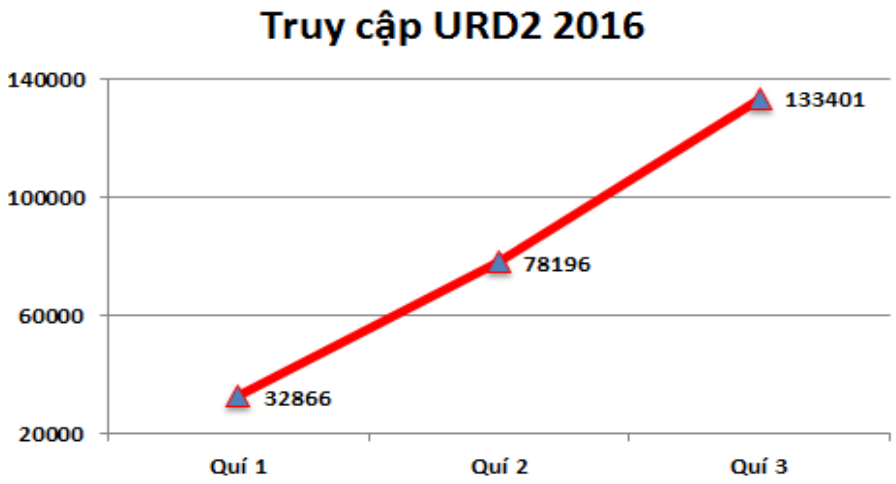
Giao diện đăng nhập một lần của Trung tâm TT - TV

Giao diện đăng nhập SSO của Thư viện cũng chính là cổng thông tin đăng nhập chung của hầu hết các dịch vụ và ứng dụng mà Thư viện tích hợp. Các cổng thông tin chính của Trung tâm bao gồm:

- LIC (Library and Information Center): http://lic.vnu.edu.vn/
- URD2 (Unified Resource Discovery and Delivery): http://find.lic.vnu.edu.vn/
- DLIB (Digital Library): http://dlib.vnu.edu.vn/

Việc triển khai hệ thống đăng nhập một lầnđã tạo ra bước ngoặt nâng Trung tâm TT – TV lên một tầm vóc mới. Đây là bước tiến thực sự mang tính cách mạng, tạo nên cái nhìn hoàn toàn mới về thư viện của Đại học Quốc gia Hà Nội. Điều đó thể hiện ở sự chuyển biến về số lượng truy cập các site thành viên của Trung tâm.

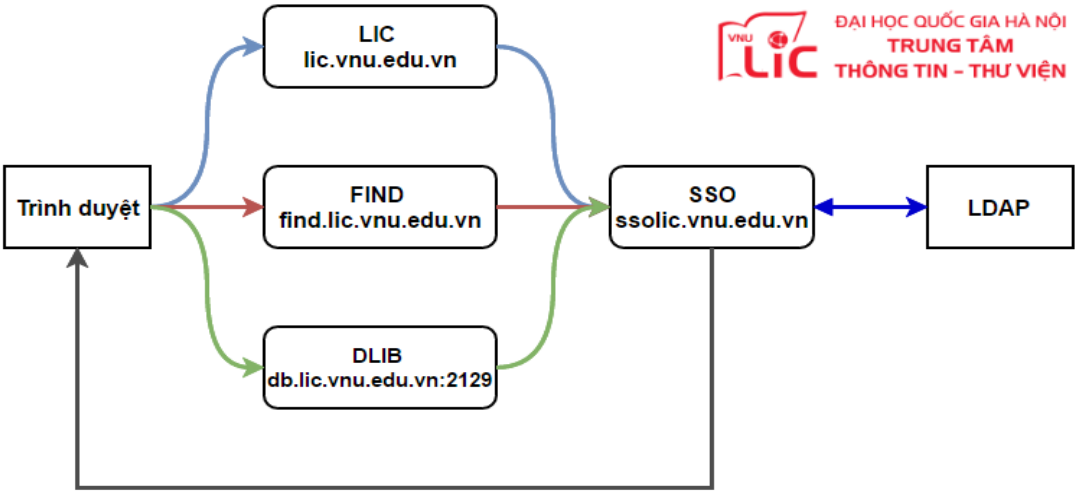
Ví dụ về lượng truy cập củaDịch vụ Phát hiện Tài nguyên học tập và Nghiên cứu Thống nhấtURD2: http://find.lic.vnu.edu.vn/



Biểu đồ truy cập URD2 năm 2016

Sự tăng trưởng mạnh mẽ của URD2 thể hiện sự quan tâm người dùng tin khi họ có nhu cầu khai thác thông tin, một phần vì sự thống nhất tài khoản người dùng giữa các dịch vụ và ứng dụng của thư viện. Người dùng tin sẽ cảm thấy thuận tiện hơn thì không phải quan tâm việc bảo mật thông tin cũng như lưu nhớ nhiều tài khoản khác nhau. Điều này rất được lưu tâm trong thời đại công nghệ thông tin, đặc biệt đối với những người khai thác thông tin chuyên sâu như các giảng viên, các nhà khoa học…

Dưới đây là mô hình đơn giản của giải pháp SSO sau khi được triển khai tại Trung tâm TT – TV:



Sơ đồ giải pháp SSO tại thư viện

Người dùng khi đăng nhập các dịch vụ của thư viện, thì tài khoản của người dùng trước đó đã được ghi nhận tại LDAP (Lightweight Directory Access Protocol -giao thức truy cập nhanh các dịch vụ thư mục), sau khi LDAP xác thực tài khoản thì lúc đó SSO sẽ cho phép người dùng đăng nhập thành công và bắt đầu sử dụng các dịch vụ và ứng dụng.

KẾT LUẬN

Với trải nghiệm cá nhân của tác giả, dù giải pháp SSO có khả năng tăng cường bảo mật thông tin tài khoản cho người dùng, tuy nhiên hiện nay có rất nhiều nguy cơ tiềm ẩnngười dùng bị tấn công từ bên ngoài đối với hệ thống mạng. Tuy vậy, trong kết quả khảo sát chất lượng phục vụ thư viện 2016, có đến hơn 80% trong tổng số gần 2000 phiếu bầu chọn đã đồng ý với quan điểm website của thư viện dễ khai thác và các phần mềm tra cứu tài liệu dễ sử dụng. Điều đó chứng tỏ giải pháp SSO góp phần không nhỏ giúp ích cho việc tra cứu, khai thác thông tin trên website của thư viện được nhanh hơn, an toàn hơn, hiệu quả hơn.

Dù cho cơ chế đăng nhập một lần vẫn còn những hạn chế nhưng không thể phủ nhận đó chính là giải pháp công nghệ thông tin mang tính thời đại, tương lai. Trung tâm Thông tin – Thư viện trong năm 2016 với trách nhiệm là đầu tàu về khai phá, lưu trữ thông tin đã có những bước tiến vượt bậc, đặc biệt là triển khai những ứng dụng mang tính bước ngoặt, giải pháp SSO là một chứng minh.

TÀI LIỆU THAM KHẢO

1. https://en.wikipedia.org/wiki/Single_sign-on
2. https://en.wikipedia.org/wiki/Central_Authentication_Service
3. https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
4. https://en.wikipedia.org/wiki/Authorization
5. https://en.wikipedia.org/wiki/Authentication
6. https://en.wikipedia.org/wiki/OpenID
7. https://en.wikipedia.org/wiki/HTTP_cookie