InCommon

MICHAEL SMITH[1]

[1] *School of Informatics and Computing, Bloomington, IN 47408, U.S.A.*
[*] *Corresponding authors: mls35@iu.edu*

paper2, April 12, 2017

InCommon is a federated security service that is responsible for the management of identity verification solutions serving U.S. education and research. All users within this federation allow partners to share identity information in order easily recognize the user. This federation provides numerous benefits for users and service providers through the convenience of single sign on capabilities for the user. Privacy is enhanced by limiting the distribution of personal information amongst numerous service providers. Scalability is easily facilitated due to the unified policies and management procedures. Programs such as InCommon assurance and university case studies are examined.

Keywords: InCommon, User authentication, identity management, I524

ttps://github.com/cloudmesh/sp17-i524/blob/master/paper2/S17-IO-3019/report.pdf

1. INTRODUCTION

Electronic credentialing of individuals requires an effective implementation of a set of policies and procedures. In order to be successful, identity management requires an organization to keep user information up to date, providing the trust needed for secure transactions, and determine user access of online applications. The major issues with identity management is the increasing number of cloud services or applications that are web hosted, all of which have different policies for implementing identity verification. The solution is to establish a federation which is defined as "an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transaction" [1]. Within this federation the parties come into an accordance on the policies associated with identity management. A great example of a federation that encompasses this definition is InCommon.

2. INCOMMON

InCommon was founded by the advanced technology organization Internet2. Their mission is to create an environment that facilitates the ability for educators and researchers to collaborate regardless of their location. Their network encompasses over 90,000 institutions, 305 universities, 70 government agencies with network operations center powered by Indiana University [2]

Through the InCommon service, users will not have to remember a plethora of usernames and passwords for each web service. Instead, they will be able to have single sign on (SSO) conveniences. Giving time back to faculty, staff and students for education, research and other contributions to the University. Any service provider within this federation no longer needs to manage databases of username and passwords, the users are verified and then administered security tokens to then engage with service providers within the federation. By limiting the amount of identity information required of the service provider, the users privacy is safer in the event of a security breach of the service provider.

3. ARCHITECTURE

The architecture of the InCommon framework is comprised of several key components such as SAML, Shibboleth, certificate service offerings and Duo. While different from one another these components all help assist the federation with user authentication. SAML is the language used in the transfer of data, Shibboleth is a service that assists in the implementation of SAML. The certificate service mainly comprised of SSL assist in the privacy of data passed, and Duo provides an extra layer of security with two factor authentication. Each component will be discussed in the following sections.

4. SAML

The language used by InCommon is referred to as security assertion markup language or SAML. This language is based in XML which allows for the exchange of authentication information between a user and a provider [3]. It is the industry accepted standard language for identity verification by numerous government, businesses and service providers[4]. The general user verification is done by an identity provider(IdP) which is responsible for user authentication through the use of security tokens with SAML 2.0 [5]. Service providers (SP) are defined as entities

that provide web services, internet, web storage etc. They rely on the IDPs for the verification process. A significant amount of the major web service providers such as Google, Facebook, Yahoo, Microsoft, and Paypal play a dual role and exist also as identity providers.

5. SHIBBOLETH

Shibboleth is the service that has a suite of products that assist the InCommon federation through utilization of SAML in programming languages such as C ++ and Java[6]. The normal authentication process for Shibboleth is to intercept access to a service, determine who is the identity provider for the user. Once the identity provider has been discovered a SAML authentication request is sent to the identity provider. Identity providers SAML response will have the relevant user information for verification. The extracted user information will then be passed to the service provider or resource determining user accessibility. While the process sounds complex it will occur instantaneously, after the user has entered its single sign on.

6. CERTIFICATE SERVICE

The types of certificates that InCommon have available for issue are SSL/TLS, extended validation, client, code signing, IGTF server, and elliptical curve cryptography certificates (ECC). SSL (secure sockets layer) is "the standard security technology for establishing an encrypted link between a web server and a browser. The link ensures all data is passed between the web server and browers remain private and integral"[7]. The details of an SSL certificate issued by InCommon will contain user information and the expiration date. For all educational institutions, InCommon offers unlimited server and client certificates for the annual fee.

7. DUO

In collaboration with the trusted access company Duo, Incommon offers two factor authentication through the utilization of the users smart phone[8]. A duo mobile app supports the following platforms: Apple iOS, Google Android, Windows mobile, Palm WeboS, Symbian OS, RIM blackberry, Java J2ME. The application will generate a randomly generated one time password that the user will type into the web application for a more secure identity verification. Two factor authentication does not require smartphone, other methods such as automate voice calls or SMS messages. In addition to Duo mobile, a service called Duo push is available which does not require the user to type in the password, authentication occurs directly from the mobile app. It is up to the university to determine how Duo is deployed, whether it will occur with the identity provider or the service provider. If it is deployed at the service provider destination, Duo web supports the following client libraries: python, ruby, classic ASP, ASP.net, Java, PHP, Node.js, ColdFusion, and Perl.

8. ASSURANCE PROGRAM

Many organizations and government agencies such as a national institute of health and public universities are requiring identity providers to become certified in this program. Incommon offers an assurance program that will examine and the practices of an organization and will rank them based on a number of criteria. Areas of examination include "...identity proofing(such as checking government issued ID before accepting that people are who they say they are), password handling (including making sure that passwords are not sent or stored in the clear), and authentication(such as ensuring the resistance of an authentication method to session hijacking)" [9].

There are two levels of assurance in the InCommon program, bronze and silver. Bronze is comparable to NIST level of Assurance 1, which is for common usage of internet identity management. Silver is comparable to NIST level of Assurance 2, which defines the institute as having sufficent requirements provide a security at the level for a financial transaction [10]. NIST levels of security are set by the National Institute of Standards and Technology, a government body within the U.S. Department of Commerce[11]. Compliance with a bronze level only requires a level of self certification of the requirements, where as a silver level is more difficult to achieve. A third party or evaluator that has been verified by InCommon is required to peform an audit ensuring the identity provider is meeting all the rules and requirements.

9. UNIVERSITY OF MINNESOTA

One example where InCommon was successfully deployed was at the University of Minnesota. They joined the InCommon federation on September 2010 [12]. The university contains 51,000 students, and over 300 institutes. Their previous identity management vendor charged on a per certificate basis. This differs from InCommon which offers an annual fee with unlimited certificates. This simplifies the ability for IT departments within Universities to properly budget. Additionally the university saw a cost savings of 38,000 dollars. This model also encourages enhancing security because cost does not influence which servers to secure.

10. STUDENTS ONLY

The bottom line of a university is not the only one who sees the cost benefits of InCommon [13]. Student verification provider known as students only is a way for students to enroll to verify their status as a student. This verification is then passed to businesses that would like to offer discounts to students. To prevent nonstudents from taking advantage of offerings of companies it can be cumbersome for a student to properly verify their status. With the help of InCommon Students Only helped streamline the process for students to verify their identity in a single sign on. This reassured the companies and students were able to save money without the difficulties of personally handling identity verification.

11. CONCLUSION

As the number of services on the web continue to grow it can be quite challenging for both universities and service providers to properly manage accessibility manage identities. InCommon hopes to address this issue by bringing U.S. educational institutes into the same federation. This will create a common groundwork of policies and procedures related to identity management. Through this unity, users such as faculty, staff, and students alike can benefit from the obvious conveniences of single sign on. However, they will also benefit from enhanced security and privacy. Institutions that have entered into InCommon have seen benefits such as cost savings over competitors in this market as well as simplification of the billing process for University IT. The unlimited certificate model as well as the

diverse types of certificates allows IT flexibility to issue the appropriate certificate without the worry of budgeting constraints. Partners such as Duo further improve security through two factor authentication dramatically improving the protection of the user.

REFERENCES

[1] InCommon, "Incommon overview," Webpage. [Online]. Available: https://www.incommon.org/docs/presentations/InCommon_Overview.ppt

[2] InCommon, "What is the incommon federation?" Webpage. [Online]. Available: https://spaces.internet2.edu/download/attachments/2764/final_InCommon.pdf

[3] Wikipedia, "Security assertion markup language," Webpage. [Online]. Available: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[4] Pingidentity, "Saml: How it works," webpage. [Online]. Available: https://www.pingidentity.com/en/resources/articles/saml.html

[5] empowerID, "Service providers, identity providers & security token services," Webpage. [Online]. Available: https://www2.empowerid.com/learningcenter/technologies/service-identity-providers

[6] Shibboleth, "Shibboleth," Webpage. [Online]. Available: https://shibboleth.net/

[7] SSL, "What is ssl?" Webpage. [Online]. Available: http://info.ssl.com/article.aspx?id=10241

[8] InCommon, "Incommon multifactor," Webpage. [Online]. Available: https://www.incommon.org/duo/

[9] M. Erdos, "An introduction to assurance," Webpage. [Online]. Available: http://iam.harvard.edu/resources/introduction-assurance

[10] InCommon, "The incommon assurance program," Webpage. [Online]. Available: https://www.incommon.org/assurance/

[11] Nist, "Nist," Webpage. [Online]. Available: www.nist.gov

[12] InCommon, "The university of minnesota enables security at scale with incommon," Webpage, July 2016. [Online]. Available: https://www.incommon.org/docs/eg/InC-Cert_CaseStudy_Minnesota.pdf

[13] InCommon, "Incommon flies high with students only," Webpage. [Online]. Available: https://www.incommon.org/docs/eg/InC_CaseStudy_StudentsOnly_2009.pdf