Federated Identity Technologies and Applications in Research and Education Networks

Konul Aliyeva
ANAS Institute of Information Technology, Baku, Azerbaijan
keliyeva3@std.qu.edu.az

***Abstract*— In this paper federated identity, the technologies it reclines, and security issues in federated identity is overviewed. A specific identity federation model, eduGAIN which is widely used by European Research and Education Networks is briefly discussed. eduGAIN is suggested for implementation in AzScienceNet, the National Research and Education Network of Azerbaijan.**

Keywords*— *federated identity, security tokens, federated identity technologies, SAML, OpenID, OAuth

I. INTRODUCTION

As the number of Internet users increases new software products, heterogeneous applications, and multiple services appear. At the same time the requirements of the users become more complex, users demand more secure and faster accesses. So we are being faced with new requirements to authentication, authorization and identity management. Here comes a new form of idendity management – federated identity management.

Identity is a set of characteristics that defines a person. Identity itself can be divided into two categories: physical identity and digital identity. Physical identity identifies a person's physical characteristics, personality, his/her daily behavior. Each person has his/her own phsical characteristics. And digital identity identifies a person's characteristics in digital world. In other words, it is the electronic representation of an entity within a domain of application [1].

Most providers of Internet-based services store user credentials in their own directories or databases which are not shared with other providers. This ends up with users having multiple sets of credentials. Thus a user will have a distinct set of credentials for each provider [2]. Simply a credential can be a password. So a user should remember multiple passwords in order to access distinct applications, websites. Nowadays people may have tens of distinct accounts and they have to remember passwords for all of them. It is difficult for human beings to remember multiple distinct passwords. In this case either the users choose a very simple password for remembering it easily or they use password management strategy which leads to increase identity theft cases. This is where we need federated identity.

Firstly, let's give a definition to federated identity. Federated Identity is the means of linking a person's electronic identity and attributes stored across multiple distinct identity management systems [2]. It is a combination of different components and concepts that come together to form one solution [3]. Federated identity management creates a trust relationship between multiple organizations for exchanging a person's digital identity information in a safe way, protecting privacy of user private information, guaranteeing its integrity and confidentiality (Figure 1).

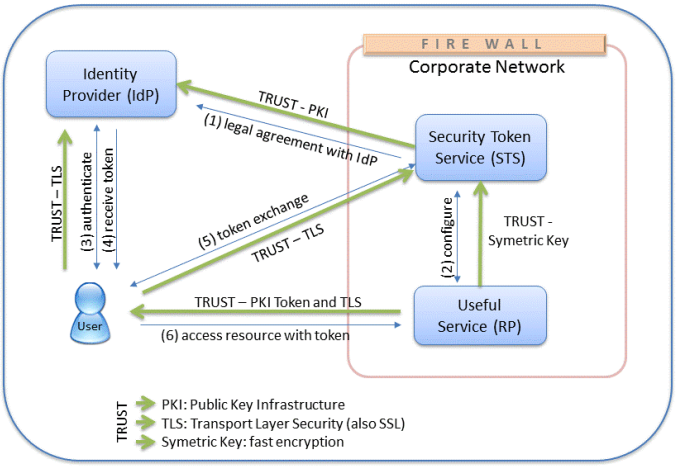

Figure 1. Federated Identity Trust Relationship Model [4]

Some well-known companies such as Google, Microsoft, Twitter, Yahoo, LinkedIn, MySpace, Paypal, Amazon are examples to digital platforms that allow users to log into another websites, applications without creating a new profile.

II. TECHNOLOGIES OF FEDERATED IDENTITY

There are standart technologies for authentication, authorization and data exchange in federations. These technologies mainly are: SAML, OpenId, OAuth, Security Tokens (Simple Web Tokens, JSON Web Tokens).

SAML stands for Security Assertion MarkUp Language. SAML is an XML-based framework, providing secure data communication between Identity Providers (IdP) and Service Providers (SP). It defines mechanisms to exchange authentication and authorization information in a secure way [5]. SAML has four main components: SAML assertions, SAML protocols, SAML bindings and SAML profiles [3].

OpenId is an open standart and authentication protocol that enables to exchange identity information between Identity Providers and Service Providers (Figure 2). It provides users to sign in a new web-site without creating a new password and username [6].

DOI: 10.25045/NCSoftEng.2017.46

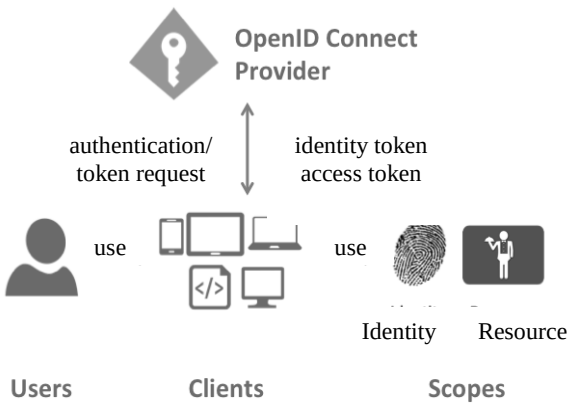

Figure 2. OpenID Connect[7]

OAuth is an open protocol that enables secure authorization in a simple and standard method from web, desktop and mobile applications [8]. It authorizes users for accessing their information on websites without giving their passwords. The mechanism is used by multiple distinct companies such as Google (Figure 3), Facebook, Microsoft, Twitter. These companies allow users to share their information with other websites.

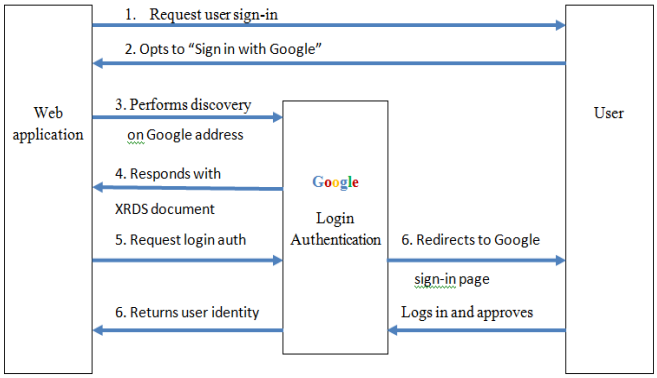

Figure 3. Google Login Authentication via OAuth [9]

SWTs use a very simple format for transmitting assertions. SWT assertions consist of name/value pairs. Because of it uses this simple format, SWTs are very lightweight. They are often used in HTTP headers and other places where space is limited.

JSON Web Token is used as a security token in federated identity. Security tokens permit to pass information back and forth between Identity Providers and Service Providers. JSON Web Token is a JSON based standard and it defines compact and self-contained way for securely trasnmitting information between parties [10]. JSON itself is derived from JavaScript programming language. It includes data types such as arrays, numbers, bytes, strings, booleans. This makes JSON more compatible with JavaScript programming language [11].

III. SECURITY ISSUES

Security has always been a main concern when dealing with identity. Users must be sure that their credentials and identity information are secure, they have been properly stored and transmitted to third parties. Main security problems in federated identity environment are misuse of the identity, identity theft and platform trustworthiness [12]. Many people concern about which applications they submitt their credentials to. If the application is compromised, then the attacker can access to the user's account, use his/her identity, which leads to identity theft. And if a user uses same credentials for various applications, it becomes more dangerous. By using federated identity, the application itself never sees a user's credentials [3]. Instead, it only sees user identity information sent from the Identity Provider. Only the Identitty Provider sees the user's credentials. Hence, if the application is compromised, users don't have to worry about their credentials' safety. Nowadays, federated identity security is one of the interesting research areas for enormous industries such as Tivoli, IBM.

IV. A FEDERATED IDENTITY MODEL FOR AZSCIENCENET

AzScienceNet is the National Research and Education Network which is established on the basis of network of Azerbaijan National Academy of Sciences. It provides institutions and organizations of Azerbaijan National Academy of Sciences with modern network services. This network provides users with various services such as cloud services, web hosting, AzScienceCert service, Eduroam, distant education, etc [13]. For each service, users should have different accounts. Thus it leads to the problems aforementioned. For the solutions of this aforementioned problems, National Research and Education Networks around the world use the eduGAIN service for trusted and secure identity. What is eduGAIN and what services does it offer? eduGAIN is the service of European Research and Education Network (GEANT) company related to issues about turst, identity and security. The eduGAIN service interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. It enables reliable exchange of data related to identity, authorization and authentication. Two main services of eduGAIN are shown below:

1. It helps students, researchers to access online services by reducing the number of accounts a user has to manage. It leads to reducing of costs, security risks and complexity;

2. It provides service providers with a wider pool of users internationally and permits users to access resources of institutions, cloud services using their one trusted identity [14].

CONCLUSION

In this paper federated identity, technologies that it reclines, related security issues and application of federated identity in the National Research and Education Networks. Technology behind the globally proven federated identity model were briefly revised. eduGAIN, a federation of identity federations is a generally used model for National Research and Education Networks. AzScienceNet can easily implement the same technology and provide trusted identity framework for its users.

DOI: 10.25045/NCSoftEng.2017.46

REFERENCES

[1] U. Rodriguez, M. Maknavicius, J. Dieguez, “Federated identity architectures”, www-public.tem-tsp.eu

[2] M. Paul, “Liberty Alliance Project White Paper. Liberty ID-WSF People Service – federated social identity”, 2015, www.project.liberty.org

[3] D. Rountree, “Federated Identity Primer”, 96 page, 2012

[4] www.ckingit.com/professional/federation/mapping-the-trust/

[5] SAML, http://www.webopedia.com/TERM/S/SAML.html

[6] E. Eldon, “Single Sign-on service OpenId getting more usage”, 2009, https://venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage/

[7] www.identityserver.github.io/Documentation/docsv2/overview/terminology.html

[8] OAuth, https://oauth.net/

[9] www.developers.google.com/identity/protocols/OpenID2

[10] Introduction to JSON Web Tokens, www.jwt.io/introduction/

[11] J. Daly, “XML vs JSON for Web Services”, 2015, www. academia.edu .

[12] E. Ghazizadeh, M. Zamani, J. l. Ab Manan and A. Pashang, "A survey on security issues of federated identity in the cloud computing," 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, Taipei, 2012, pp. 532-565

[13] www.azsciencenet.az

[14] eduGAIN, https://www.geant.org/

DOI: 10.25045/NCSoftEng.2017.46