Single Sign-on in Cloud computing scenarios: a research proposal

S. Za[1]*, E. D'Atri*[2] *and A. Resca*[3]

Abstract - Cloud computing and Software as a Service infrastructure are becoming important factors in E-commerce and E-business processes. Users may access simultaneously to different E-services supplied by several providers. An efficient approach to authenticate and authorize users is needed to avoid problems about trust and redundancy of procedure. In this paper we will focus on main approaches in managing Authentication and Authorization Infrastructures (AAI): i.e. federated and centralized and cloud based. Then we will discuss about related some critical issues in Cloud computing and SaaS contexts and will highlight the possible future researches.

Introduction

Cloud Computing was defined in [1] as "both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud".

Software as a Service approach give people the possibility to have an ubiquitous relationship with different applications and business service and to access on demand to the "cloud" from

[1] CeRSI – LUISS GUIDO CARLI University, Roma, Italy, sza@luiss.it
[2] ITHUM srl, Roma, Italy, e.datri@ithum.it
[3] CeRSI – LUISS GUIDO CARLI University, Roma, Italy, aresca@luiss.it

everywhere in the world [2]. Cloud will be composed by different e-services from several providers and every time people access them have to fulfil an authentication procedure: increasing the number of providers will increase also the authentication procedures.

Giving a personal authentication to these services, both for social or business reasons, involves problems about security of personal data and trust relationship with the provider. Olden considered this as a digital (or online) relationships because "IT influences the institutional and social trust concept. Additionally to this occurs also the concept of technological trust (trust in technology)" [3].

Trust relationships with the service provider become a critical aspect to be considered each time a user gives an authentication, as highlighted in [4] where this issue is considered in term of risk management: "What is important is risk management, the sister, the dual of trust management. And because risk management makes money, it drives the security world from here on out".

Considering this, and how important is a valid Authentication and Authorization Infrastructure (AAI) in e-commerce contexts [5], our work will focus on the concept of authentication, then we will examine two different approaches in managing this infrastructure. In particular our focus is on Single Sign On feature provided by the AAI. Finally we will present how the authentication systems can be involved in a cloud computing context and what are the possible questions to investigate in further works.

Possible solutions in authentication management

Organizations around the world protect access to sensitive or important information using the Digital Rights Management (DRM) technology [6]. Authentication plays a key role in forming the basis for enforcing access control rules, for determining what someone is allowed to do (read a document, use an application, etc.); for this reason the system must first ascertain who that individual is. Technically, we speak of “Subjects”, and the term refers to an entity, typically a user or a device, that needs to authenticate itself in order to be allowed to access a resource. Subjects, then, interact with authentication systems of various types and various sources. An authentication type is the method the Subject uses to authenticate itself (for example, supplying a user ID and a password). An authentication source is the authority that controls the authentication data and protocol. Authentication takes place both within an organization and among multiple organizations. Even within an organization, there may be multiple sources. However, traditional authentication systems generally presume a single authentication source and type. An example would be Kerberos [7] where the source is a trusted Key Distribution Center (KDC) and the type is user IDs with passwords. In a Public Key Infrastructure (PKI) [8] the source is the Certification Authority (CA) and the type is challenge/response. While both Kerberos and PKI permit multiple authentication sources, these authentication sources must be closely coupled. Often, complex trust relationships must be established and maintained between authentication sources. This may lead to authentication solutions operationally infeasible and economically cost-prohibitive. Another security problem of many current web and internet applications consists in offering individual solutions for the login procedure and user management, so the user have to register to each application and then to manually login to each one of them. This redundancy in the input of user data is not only less user friendly; it also presents an important security risk, namely the fact that the users are forced to remember a large number of username and password combinations. A study made by the company RSA (RSA 2006) shows that 36% of the experienced internet users are having 6 to 15 passwords and 18% of them even more than 15. From these numbers, it is obvious that it is difficult to manage such a big number of user data in an efficient way. In this case, users have the tendency of using simple passwords, of writing them down or simply using the same password everywhere. The purpose of Authentication and Authorisation Infrastructures (AAIs) is to provide an authentication system that is designed to resolve such problems [9]. The AAIs are a standardized method to authenticate users and to allow them to access distributed web contents of several web providers. In the context of E-Service and E-Business, it takes place that a group of organizations decides to cooperate for a common purpose. For example, each organization in the group provides one or more services to the others; their respective employees use these services after the authentication and authorization procedure by means of an Authorization and Authentication Infrastructure (AAI). After a successful authentication, each user can access specific services if he is authorized to use them. In these situations, a first decision to be made is the choice between a central or a federated infrastructural environment. The advantages of the federation environment will be shown by means of test scenarios without considering the cost factor. If the group decides to use central AAIs to control the access to one or more services, they need to decide on the provider of these services. One scenario is that the provider is part of the group, another is that the service is provided by an external company probably specialized in this. In both cases it is necessary to create a trust climate between trustee (who manages the identity information) and truster (the companies using the service). The scenario becomes more complex if a company from the group decides to participate in a different group as well. In this case, the company has to provide another organization managing a central server with its identity information, this resulting in a new trust climate. On the other hand, if the group decides for the federated AAI, each company manages its own identity information, so it is not crucial to establish a high trust climate within the group. This group of organizations is defined as “circle of trust”, in which every participant can act either as Service Provider (SP), or Identity Provider (IdP) or both. Furthermore, each party can easily join a different group because it remains the owner of its identity information. An example of technical and business standards and guidelines allowing the deployment of meaningful web services can be found in the Liberty Alliance documentation. Liberty Alliance Project[4] was formed to foster standards and specifications development implementing federated identity systems based on products and technologies that support the Liberty protocols. In the next paragraph we will show more details about the federated AAI that can be used in cloud contexts. Then we will describe another solution for managing several access service credentials by the use of one cloud based identity service to provide a SSO functionality.

A federated AAI: Liberty Alliance project

According with our hypothesis, federated identity management systems represent a possible architectural solution to change the way consumers, businesses, and governments think about online authentication. The term “federated” refers to multiple authentication types and sources too. The purpose of this solution is to establish the rules that will let different authentication systems work together, not only on a technological, but even a policy level. In this scenario issues are related to the assignment of trust levels for a credentialing system, to determining rules for issuing credentials, and creating a process for assessing the trustworthiness of credentials. With these rules in place, disparate systems should be able to share authentication data and to rely on data provided by other systems.

[4] http://www.projectliberty.org/ and http://kantarainitiative.org/

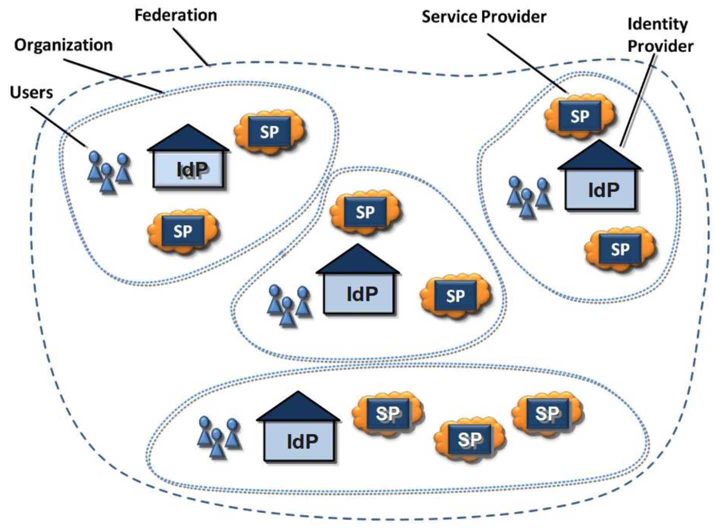

Fig. 1. Circle of trust

For instance, when a user wants to log into a bank or credit card website, an outside organization could, based on digital signature, guarantee that the user at the keyboard is indeed who he claims to be. In order to understand this architecture, some new concepts must be introduced. The "federation", also referred as a "circle" or "fabric" of trust, is a group of organizations which establish trusted relationships with one another and have pertinent agreements in place regarding how to interact with each other and manage user identities.

Once a user has been authenticated by one of the identity providers in a circle of trust, that individual can be easily recognized and he takes part in targeted services from other service providers (SPs) within that Circle of Trust. In the proposed federated architecture three main actors are involved. We use the term "Subjects" to identify: the Identity providers (IdP – in which the user's registration data reside), the Service Providers (SP – provides one or more services) and the User agent (the user application to communicate with IdP or SP - i.e. the web browser).

When a user signs in the circle of trust, his own IdP creates an “handle” and sends it to the user agent. This handle is held by the user agent until next logout and is accepted by any IdP or SP belonging to the Circle of Trust. Every time the user tries to access a trusted SP, the user agent submits the user handle to the SP. Then, the SP communicates with the user's IdP in order to gain the user's credentials (without any other user login operations). Finally, when a user signs out from any SP, the related IdP is notified about the logout process and sends a logout message to all the other SPs in which the user has been logged in. The user handle used in each session are stored in order to avoid duplicates.

Such an architecture, allows users to sign in only one time during the session (SSO) and makes them able to interact with any SP or IdP in the Circle of Trust without any other login operation until next logout. Moreover, user’s registration data are gathered only by the IdP chosen by each user with obvious advantages in terms of privacy concerns.

Cloud-based AAI: OneLogin

We're seeing a lot more discussion on the topic of single sign-on for SaaS (Software-as-a-Service) environments [10, 11]. The issue is becoming more important as security emerges as a top concern for companies considering making the move to cloud-based environments. OneLogin[5] is a company that offers single sign-on, cloud-based service that represent a solution also for small and mid-sized companies to enjoy the same level of security that usually is a prerogative only of large companies. Furhter, this kind of solution does not need to deploy security methods that employ SAML (Security Assertion Markup Language, an XML-based stan-

[5] http://www.onelogin.com/

dard for exchanging authentication and authorization data between security domains) as Liberty Alliance standard that is expensive to deploy. In this case, the user need only to: create a OneLogin account, store all his credentials for accessing several web-services, and finally install the OneLogin plug-in in his browser (previous defined User agent) to have the single sign-on functionality. In this way, authentication procedures such as the traditional user name/password system process are bypassed. In fact, users need only to provide once their own OneLogin credential directly on the login page provided by the system. This means that using the plug-in, accesses to web-services take place without providing any username/password authentication because the OneLogin plug-in do it automatically on users' behalf. OneLogin and the like's infrastructures, in some sense, sits in the cloud. In other words these infrastructures become an instrument to enable accesses to web services in situations in which dedicated servers and related personnel is not required.

Discussion

Above, two completely different AAI infrastructures (federated systems and OneLogin and the like systems) have been considered entities that allow equally single sign-on functionalities. Both of them simplify the access to distributed web contents on several web providers and, actually, at a superficial view, they work in the same way. However, the inherent nature of these two infrastructures is poles apart. OneLogin and the like systems are entities that manage identities. In other words, the several user-names/passwords or other forms of qualifications that each of us use surfing the web are piled up and activated in case it is required by users’ surfing. Further, users will decide which of these qualifications will be assigned to these systems and which ones will be managed autonomously. In the case of centralized and federated systems nothing of the kind occurs. Users are not involved at all in the identification management.

Rather, they can be completely unaware of shifts among different software systems surfing the web. As shown above, this is due to the fact that a group of organizations agree to share web services, web contents and identification management to simplify the access to them. At the basis of federated authentication systems there are reciprocal agreements in order to club together in this respect.

Further, these authentication systems have a larger potentialities in comparison with the OneLogin and the like ones. Let's take into consideration accesses to WI-FI networks. Each of us experiences that, wherever we are, switching on a lap top and checking if WI-FI connections are available, several possibilities are at hand. It goes without saying that, in this situation, a redundant service is provided. However, to connect to these networks appropriate qualifications are required. What would happen if WI-FI service providers take advantage of federated authentication systems? Further, let's think about universities of a specific country, for instance. Nowadays, all of them, more or less, are equipped with WI-FI systems and provide similar services to students. But what would happen if they decide to share an authentication system? Suddenly, undergraduate and graduate students have the possibility to take advantage of broadband connections in all universities of the country having the benefits of this kind of service.

At least from a technical perspective this is not a big issue. Above, a couple of solutions have been introduced and they are available on the market from several years. The question is why federated authentication systems are not so spread in spite of advantages that can be obtained. Here, the security issue emerges as the main obstacle in this respect. The point is on what basis do users connect to the network in question if authentication procedures are not directly managed and controlled? On this issue further research is required. It becomes fundamental to study which security issues have been overcome when federated authentication systems have been introduced successfully and which issues, on the other hand, are still at stake delegating to other organizations users' authentication.

The AAI in Cloud Computing context

Even though federated authentication systems, on the one hand, and OneLogin and the like systems, on the other hand, are completely different in nature, this does not mean that they can not be used in combination. For example, qualifications for accessing the former can be attributed to the latter. This means that is in users' hands the possibility to entrust systems such as OneLogin to allow the access to a series of web services and web contents regrouped through federated (or also centralized) systems. Obviously, all of this has some consequences. The combination between these two kinds of authentication systems facilitate considerably accesses to electronic services seamlessly. In contrast, this required to hand over sensitive qualifications to a third party (the OneLogin system for example) and for this reason the usual issue comes out: security. Even in this respect, further research activity would be beneficial in order to investigate how, actually, issues such as this one can be faced in order to favour the access to distributed web contents and web services considering, at the same time, security issues .

So far, centralized federated authentication systems have been considered indistinctly even though, as it was mentioned above, they differ significantly. In the centralized systems one of the members of the inter-organizational group manages users' qualifications for all other members. In the case of federated systems each member has custody of qualifications of its own users and on the basis of a circle of trust they are considered valid by other members. In this regard, a comparative study can be useful in order to examine pros and cons of these two solutions. At a first glance, the latter seems more apt in order to manage security issues. The fact that each organization has the possibility to supervise its own users' qualifications can represent a compromise between direct control and the delegation to a third party of electronic identification management.

Literature on cloud computing outline an alternative way to manage hardware and software systems. Due to the development of the internet, applications and databases are accessible from all over the world. However, at the basis of this way of reasoning there is a single entity that decided to outsource these activities rather than in-source them. The evolution of AAI and in particular of centralized and federated systems has changed the scenario as now also co-sourcing becomes possible. In this case, not only Software as a Service (SaaS) but also Identity as a Service (IaaS) [12] represents an alternative way of identification management. But the fact is that this type of management can enable further forms of inter-organizational collaborations or of web services and web contents.

Conclusion and future steps

Our objective is to introduce some suggestions on the development of the use of information technology following a specific perspective: the web accessibility. In this respect, SSO potentialities have been outlined. Both centralized and federated AAI, on the one hand, and OneLogin and the like systems, on the other hand, represent instruments that, actually, can outline a significantly different scenario surfing the web. And it is not only a question to move from one application to the other seamlessly. Cloud computing can be seen according to a new angle as it is not only the result of an outsourcing process by a specific entity but also co-sourcing becomes possible and new forms of inter-organizational collaborations can be figured out. In the further researches, we would investigate about security implication, even as trust and risk management, related the adoption of AAI mentioned above. Then, we would try to discover where and why some architectures are more used in respect to other ones in which context (i.e. personal or business).

References

[1] Ambrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. *EECS Department*, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28

[2] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I. (2009).Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems* 25(6), Elsevier.

[3] Geer, D. (1998). Risk management is where the money is. Forum on Risks to the Public in Computers and Related Systems, *ACM Committee on Computers and Public Policy* 20(6)

[4] Olden M., Za S., (2010). Biometric authentication and authorization infrastructures in trusted intra-organizational relationships. In *Management of the Interconnected World*, D'Atri et al. Eds., ISBN: 978-3-7908-2403-2, Springer.

[5] Lopez J., Oppliger R., Pernul G. (2004). Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security* 23 (7), 578-590.

[6] Rosenblatt B., Trippe B. And Mooney., S. (2001). Digital Rights Management: Business and Technology. *Hungry Minds/John Wiley and Sons*, New York.

[7] Kohl J. And Neuman C. (1993), The Kerberos Network Authentication Service (V5), RFC-1510, DDN Network Information Center, 10 September 1993.

[8] Ford W. And Baum M. (1998). Secure Electronic Commerce, Prentice Hall

[9] Schläger, C.; Sojer, M.; Muschall, B.; Pernul, G. (2006): Attribute-Based Authentication and Au-thorisation Infrastructures for E-Commerce Providers, pp132-141 Springer-Verlag.

[10] Lewis, K.D. and Lewis, J.E. (2009). Web Single Sign-On Authentication using SAML. *International Journal of Computer Science Issues*, IJCSI 2, 41-48

[11] Cser, A. and Penn, J. (2008). Identity Management Market Forecast: 2007 To 2014. *Forrester.*

[12] Villavicencio, F. (2010) Approaches to IDaaS for Enterprise Identity Management. http://identropy.com/blog/bid/29428/Approaches-to-IDaaS-for-Enterprise-Identity-Management (accessed June 27, 2010).