Computer Communications 68 (2015) 73–82

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Unified communications as a service and WebRTC: An identity-centric perspective

Victoria Beltran*, Emmanuel Bertin

Orange Labs, Caen, France

ARTICLE INFO

Article history:
Available online 17 July 2015

Keywords:
SaaS
WebRTC
UC
enterprise
identity

ABSTRACT

Software-as-a-service (SaaS) is gaining momentum for all business applications, including Unified Communications as a Service (UCaaS). In this context, user identity will play a key role in connecting the future fragmented communication suites in both corporations and cloud SaaS providers. However, SaaS solutions impose strong security challenges to the enterprise's Identity Management (IdM), since cloud services need to be provided with the employees' identities. UCaaS solutions should therefore enforce security properties such as trust relationship, anonymity, or control on information disclosure. WebRTC is reinforcing the trend towards cloud-based UC by adding real-time voice and video capabilities into browsers. WebRTC does not tackle IdM, and hence it is not evident how WebRTC-based cloud services can meet the corporate requirements on IdM. In this paper, we discuss various IdM models for cloud-based corporate services, and we introduce the major requirements for managing user identities in UCaaS. We assess the impacts of these requirements on WebRTC-based UC services. We finally propose a slight modification of WebRTC to meet the corporate requirements on IdM.

1. Introduction

Unified Communications (UC) [1] are aimed to improve the user availability for communication in teams through the management, integration and coordination of various communications and media in a unified manner. UC was born to alleviate corporate users from the burden of confronting with a variety of devices, tools and media types in distributed collaboration environments. UC deployment has been mainly driven by the advances on IP technology, presence, and instant messaging. Typical UC products merge on-premises telecommunication tools with the enterprise's information system. Enterprises are nonetheless increasingly more interested in turning from on-premises products into the cloud. Software-as-a-service (SaaS) solutions are the most demanded by enterprises that lack in-house expertise, wish to speed up service deployment or need to reduce costs. In such cloud computing trend, UC as a Service (UCaaS) has become popular as a solid alternative to traditional UC for corporate communication and collaboration tools. UCaaS products are collaborative communication solutions hosted by cloud providers that fine-tune dedicated hardware to ensure real-time and carrier-grade performances. UCaaS provides the same enterprise-level functions as its on-premises counterpart (i.e., VoIP, VPNs, PBX, presence, IM, etc.) without the costly investment of purchasing, hosting and managing the infrastructure. A recent Gartner analysis [2] states that 2014 is the first year in which North American multinational corporations consider UCaaS as a mainstream, viable alternative for UC deployment.

The Web nature of cloud services imposes numerous challenges to the controlled corporate networks. Specially for Identity Management (IdM), which has always resided inside of the closed corporate walls. User identity is a key enabler for UC, since on one hand it enables user authentication and login, and on the other hand it allows users to trustworthy communicate with others by verifying their identities. In the shift from on-premises UC to SaaS, to delegate identity information to cloud providers is a major security issue to any enterprise. Futhermore, how corporate identity information is provisioned to cloud services can to a great extent impact the enterprise's resources and cost for cloud integration. Nevertheless, the clear benefits of off-premises UC platforms for enterprises such as paying-as-you-go billing, flexible on-demand provision, and reduced cost of infrastructure and deployment time motivate industry to face and overcome these challenges.

The progression towards UCaaS is being stimulated by a new under-standardized real-time technology, Web Real-Time Communication (WebRTC), that is disrupting the market of real-time communications. WebRTC [3] is an emerging HTML5 technology that enables web developers to integrate real-time audio, video and data communications in their web pages. This technology enables enterprises to integrate in-content communication into their Web services

* Corresponding author. Tel.: +33 23895147.
E-mail address: victoria.beltran@orange.com (V. Beltran).

http://dx.doi.org/10.1016/j.comcom.2015.07.011
0140-3664/© 2015 Elsevier B.V. All rights reserved.

without the need of plug-ins. This capability brings advantages to enterprises that can now straightforwardly develop Web-based video collaboration and online meetings, or extensions of corporate voice services to mobile users among other Web-based real time services. In fact, a detailed research and market study about WebRTC [4] states that WebRTC is more widely commercialized in enterprises than customer use today. This includes new forthcoming cloud-based offers for collaboration and conferencing in addition to upgrades of the existing installed base of UC/PBX services. WebRTC will therefore separate aspects of business communications while remaining a part of on-premises UC solutions. WebRTC specifications do not tackle the signaling plane but only the secure exchange of media between browsers. Identity Management (IdM) is therefore completely left to each implementation. Nevertheless, a WebRTC specification [5] is standardizing a general architecture for identity provision among end-users. This architecture relies on a third-party Web service that authenticates users and is independent from the communication provider. Nevertheless, to the best of our knowledge, there is no as of now WebRTC provider that implements the proposed model for identity provision in WebRTC. WebRTC-based SaaS providers are mainly closed burbles that centralize user authentication and service on their servers, without the proposed identity provision mechanism.

Identity federation between enterprises and cloud providers, and more specifically UCaaS solutions, has not been sufficiently studied. Thus, to investigate further the integration of cloud services with the entepríse's IdM is necessary for the adoption of cloud-based UC. It is particularly necessary for WebRTC-based services, since WebRTC leaves totally unspecified how to handle user identities, thereby setting each provider totally free to implement IdM at its own. For users that require certain security requirements such as corporations, not all identity models implemented by cloud providers might be acceptable. This paper gives a general overview about identity federation and management in cloud services for corporate communications, and particularly for WebRTC-based services. This paper does not provide a new IdM solution or proposal for cloud services. Instead, we provide a global analysis about the identity requirements that SaaS solutions and WebRTC should meet to work in enterprise-grade communications. We first introduce the role of user identity in enterprise networks and the Web. We identify different IdM models between cloud-based services and corporations. We discuss about the role of identity as the glue for cross-provider UC, and we discuss about the identity features that UCaaS solutions should address. Finally, we analyze how WebRTC-based cloud providers can be integrated with the entepríse's IdM. We propose to slightly adapt the WebRTC identity model to meet the discussed identity features for corporate services.

2. Related work

Identity federation has been largely studied both in the enterprise [6] and on the Web [7]. Identity federation is a mature research field for loosely-coupled services that rely on third-party services for user authentication [8]. However, identity federation for enterprise UCaaS is today an emerging topic that combines the knowledge and technologies from different research areas: IdM, cloud computing, and UC.

Cloud computing is a hot research area that receives much attention from the research and industry community [9]. In particular, security is the aspect of cloud computing that receives more attention; it accounts for the largest portion of yearly publications since 2009 [10]. Issues related to IdM are being more and more investigated such as those related to access control and user privacy. Many survey papers give a general overview about cloud security and IdM such as [10–12].

IdM in corporate networks is a mature technology, which has been mainly studied and developed from the industry. Lately, the current cloud computing trend has also arrived to enterprise IdM. Based on a recent analysis about trends in enterprise IdM [13], cloud-based IdM is one of the major interests, alongside attribute-based access control, bring your own device and privileged user management. Nevertheless, only a small portion of cloud computing research addresses enterprise IdM and there is a need of research on this area [13]. Some works [11,14–16] have tackled different IdM models for SaaS providers. Nevertheless, these works are mainly focused on user identity federation between different cloud providers on the Internet, rather than enterprise networks. To the best of our knowledge, our work is the only one that focuses on identity models between cloud providers and enterprise IdM.

Since UCaaS [17] are nowadays receiving a fresh adoption by the industry, there are very few research works on this field. Some authors for example have addressed the open source implementation of UCaaS [18] and the usage of UCaaS for security management models in social networks [19]. Nevertheless, to the best of our knowledge, no authors have tackled the issue of IdM in UCaaS.

WebRTC is a disruptive new technology driven by major web companies that has attracted much attention in the last two years [20]. Some authos have addresses the application of WebRTC in the enterprise. The authors of [21] discuss network architectures to integrate WebRTC in corporations as well as challenges related to firewalls, media flows and access control. In [22], services architectures to introduce WebRTC in telecommunication operators' networks are overviewed. Since WebRTC leaves IdM unspecified, there are very few research works about how to handle user identities in WebRTC-based solutions. The authors of [23] propose a Web identity resolution mechanism that binds cross-provider user identities based on presence subscriptions. Although the authors of [24] do not address user identity, they propose authorization and authentication models between service providers and WebRTC PaaS providers. The discussion presented in this paper has been partially motivated from two previous works [25,26]. In [25], we discussed the current WebRTC's identity model and proposed two variations of this model. In particular, we addressed the implications of SSO protocols on these identity models regarding user privacy. In [26], we addressed identity requirements for corporate WebRTC solutions. In the present paper, we extend this work to WebRTC services provided from the cloud. Additionally, we discuss how WebRTC services can be provisioned with the identity information of enterprise users and how WebRTC can be modified to support some identity features.

3. User identity in on-premises UC

User identity is a key enabler for UC by providing two primordial functions: user login and user identity provision. The first step for a user to access any communication tool is a login process in which the user introduces (explicitly or implicitly) his or her identity and credentials. This very first step allows the communication system to identify the user, apply authorization rules, personalize the service to him or her, and do other tasks such as billing or auditing. Identity provision allows end users to identify each other, and hence to decide to establish or not their communication or not in a trustworthy manner. Identity provision is primordial to offer users with a unified experience. When calling Bob, Alice wants to present the same identity whatever the communication tool, and hence the communication identifier, that she is using.

In medium to large enterprises, identity information and user authentication is normally centralized to provide a Single Sign On (SSO) experience to employees. As its name stands for, SSO aims to let users login once and access multiple services. SSO is a mature technology that was born out of the complexity and costs associated with having many user IDs and passwords in corporate networks. Corporate services redirect users to centralized servers for authentication. When a user logs on successfully to an authentication server, he or she can transparently access to all resources or services that