ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

The Service Provider Group framework
A framework for arranging trust and power to facilitate authorization of network services

Leon Gommans [a,b,*], John Vollbrecht, Betty Gommans-de Bruijn [c], Cees de Laat [a]

[a] University of Amsterdam, Netherlands
[b] Air France–KLM, France
[c] i-Beleon, Netherlands

HIGHLIGHTS

- We created a framework arranging power and trust amongst a group of service providers.
- The framework identifies essential elements and functions of a Service Provider Group.
- A Service Provider Group allows well-defined services to be delivered as a group.
- A Service Provider Group conduces trust between members by using its power.
- Members "know when the policy it is authorizing is correct".

ARTICLE INFO

Article history:
Received 30 November 2012
Received in revised form
13 March 2014
Accepted 1 June 2014
Available online xxxx

Keywords:
Authorization
Authorization framework
Trust
Power
Optical networking
AAA

ABSTRACT

Both within the Business and e-Science world, the use of virtualized resources is growing rapidly. These resources are increasingly delivered by multiple converged infrastructures, e.g. clouds that combine server, storage, and network resources from different providers. Such development requires careful re-thinking of the trust framework used between providers. As the scale and complexity of virtualization grows, so does the complexity of authorizing resource chains that are arranged across multiple providers. This type of authorization requires pre-establishment of trust relationships between providers and arranging some level of power. This paper studies the roles of trust and power when considering the requirements of authorization protocol exchanges between providers. Establishing power in the form of impersonal rules is a key element to conduce the necessary trust between providers. The Service Provider Group (SPG) is a way to arrange such power. The SPG framework provides a way to organize thinking about multi-provider services and can be used to describe emerging collaborations such as those found within the realm of optical network service provisioning.

1. Introduction

Increasingly, automated mechanisms are used that exchange protocol messages arranging, authorizing and provisioning end-to-end chains of compute, storage and network elements as a service. Delivery of end-to-end services needs coordination and oversight to ensure quality, manage risk and possibly liability. Users typically do not want to carry the burden of such coordination and oversight. The ability to arrange end-to-end services by a group of providers reliably (with adequate coordination, oversight and transparency in accordance with the terms and conditions of service agreements) influences the willingness of both users and service providers to rely on each other. Willingness to rely on something or somebody is an important understanding that is associated with trust.

To avoid damaging trust of users vested in an offered service, it is important that each provider in the chain shares a common, well-defined understanding of the terms and implications of a service agreement when authorizing the use of its contribution. Trust is needed to define service agreements that are embedded in a commonly understood set of rules. Power is often needed to enforce its terms and implications. When a group of service providers come together and recognize the benefit of collaborating,[1] such

* Corresponding author at: University of Amsterdam, Netherlands
Tel.: +31 613067014.
E-mail address: l.gommans@uva.nl (L. Gommans).

http://dx.doi.org/10.1016/j.future.2014.06.002
0167-739X/

[1] An example is GLIF, that was established by 33 participants at the 3rd annual Global LambdaGrid Workshop, held August 27, 2003 in Reykjavik, Iceland.

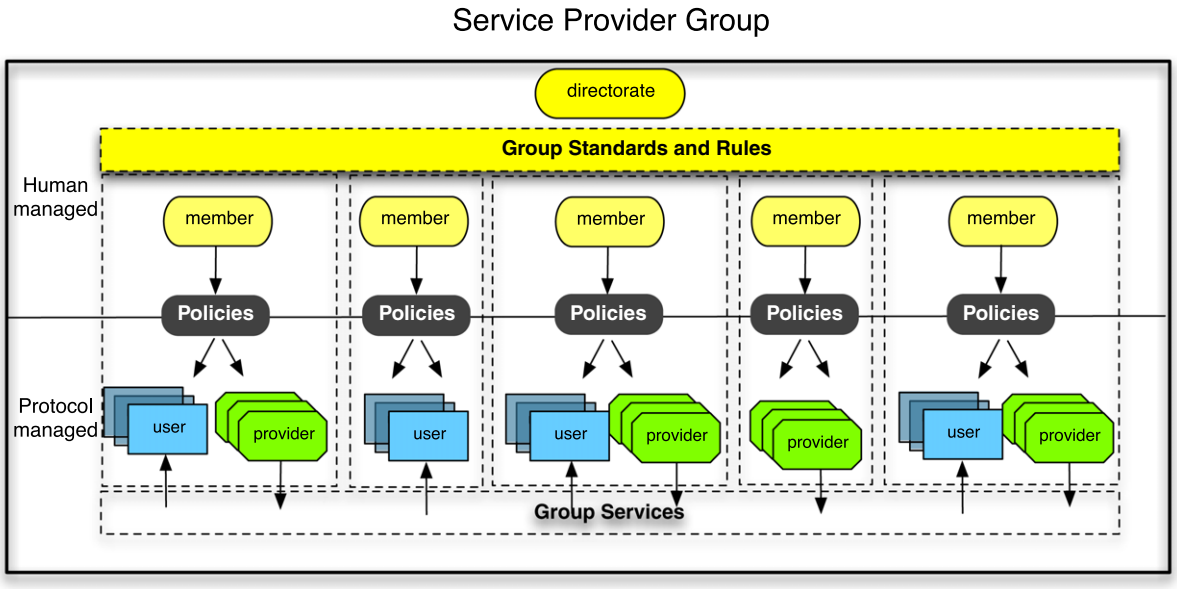

Fig. 1. The Service Provider Group Framework basic elements.

agreement is typically based on each participant personally trusting one another. Power, for example enforcement of written group admission rules,[2] is used to ensure a participant can be trusted to contribute according to the spirit of the group.

As the number of participants in a group increases, the level of automation increases and the services are being increasingly relied upon, the concepts of personal trust and power will inherently become more impersonal. Establishing a Service Provider Group (SPG) is one way to arrange *impersonal power* (rules) such that it conduces trust amongst group members. Instituting a SPG is a way to establish and maintain a common set of inter-organizational rules that are translated into intra-organizational policies such that *each entity knows that the policy it is authorizing is correct*. We make the assumption in this paper that protocols, exchanging authorization transactions between organizations, will provide enough message confidentiality, authenticity and integrity such that the security of an exchange is never disputed.

We consider a SPG as a group of member organizations that act together as a business. A SPG provides one or more services that none of its members could provide on their own. To a user, the SPG appears as a single provider. To members the SPG appears as a collaborative group with standards and rules that each member translates into conforming policies. The policies regulate the provisioning of services and the user terms and conditions that are enforced by the group. A user signs a service agreement with a member representing the SPG. Members may or may not have users or may or may not provide services as a contribution to the group. A member has signed a membership agreement with the group. The SPG has some sort of directorate role that oversees the interactions and interoperation of its members. Fig. 1 shows the basic elements of a SPG. The paper will focus on the "human managed" business part of the SPG resulting in policies that are capable of determining the operational part of the service provisioning that is typically "protocol managed".

The framework builds on RFC2904 (AAA Authorization Framework [1]), which recognized that rules must be in place before authorization transactions can take place. Fig. 1 shows that SPG group rules and standards are defined at business level involving human members that translate them into policies. Policies are executed using protocols by elements that provide services. Policies also govern user interactions obtaining group services.

In Section 2, we start with a study of what trust and power means from the area of organizational sciences and see how the SPG can be positioned herein. We then consider in Section 3 the rules of a mature example taken from the Payment Card Industry and put it into the trust and power context. This leads us in Section 4 to a framework containing the essential elements of a SPG detailed in Section 5.

This study has been motivated by the fact that members of MasterCard together handle payment transaction authorizations as a collaborating group of financial service providers. As such, we argue that this collaboration can be seen as a successful example of a SPG. The paper abstracts a framework for a SPG from observing the rules MasterCard uses to establish trust and power that are subsequently transformed into policies governing interactions between users and members at operational level. SPG members interoperate with each other using policies and protocols that are monitored and enforced. An existing networking example, eduroam providing WiFi access to students worldwide, is used to verify observations made to establish the framework.

To better understand the relationships between trust, power, rules, administration and enforcement of policies, etc. concepts from organizational science are considered to explain them. It will recognize why impersonal power is a means to conduce trust efficiently within and between organizations. We then propose a framework that recognizes three types of power that loosely resembles the concept of the Trias Politica. We will show how these powers are used to administer and control the functional levels of organizations. This is done by means of policies that are provisioned and enforced such that each participating organization is able to rely on the fact that *policies are known to be correct*. Being able to rely on such knowledge has important consequences for the protocol(s) used to communicate authorization decisions. Precise knowledge and power to enforce it allows the semantics of authorization decisions to be abstracted as much as possible when being communicated across entities. When applied to connection oriented networking, a decision that authorizes an end-to-end connection, for example represented by a token, may

[2] For example: GLIF is open to any owner/custodian of lambda infrastructure (lightpaths, exchange points, etc.) that is willing and able to make that infrastructure available to other GLIF participants on an agreed basis when it is not required for its own needs. (Source GLIF Strawmen Charter).

Please cite this article in press as: L. Gommans, et al., The Service Provider Group framework, Future Generation Computer Systems (2014), http://dx.doi.org/10.1016/j.future.2014.06.002