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

Leon Gommans[1+3], John Vollbrecht, Betty Gommans - de Bruijn[2], Cees de Laat[3]
[1)]Air France – KLM, [2)]i-Beleon, [3)]University of Amsterdam.

Abstract.

Both within the Business and e-Science world, the use of virtualised resources is growing rapidly. These resources are increasingly delivered by multiple converged infrastructures, e.g. clouds that combine server, storage, and network resources from individual providers. Such development requires careful re-thinking of the trust framework used between providers. As the scale and complexity of virtualisation 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 found within the realm of optical network service provisioning.

1.0 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. Applications become more dependent on its reliability. 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[*], such agreement is typically based on each participant personally trusting one another. Power, for example enforcement of written group admission rules[†], 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-organisational rules that are translated into intra-organisational 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 organisations, 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

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

[†] 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)

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".

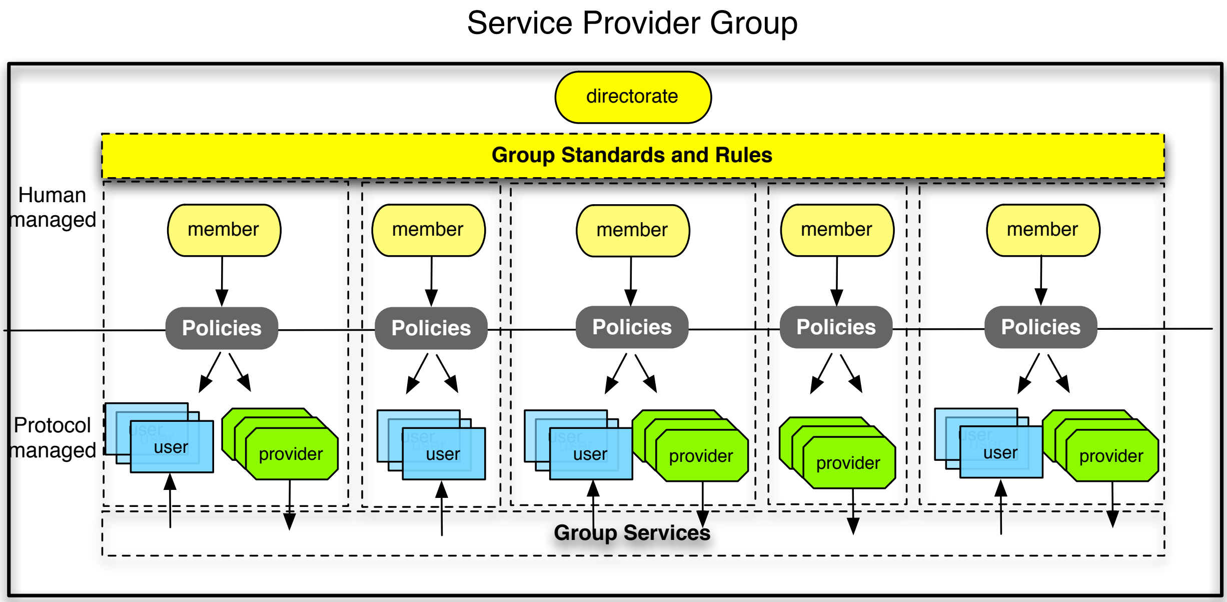

Fig 1. The Service Provider Group Framework basic elements.

The framework builds on RFC2904 (AAA Authorization Framework, see 1.1), 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.

A study of what trust and power means from the area of organizational sciences and consideration of the rules of a mature example taken from the Payment Card Industry lead us to an abstraction of a framework that contains the essential elements of a SPG. Here banks, as member of MasterCard that together handle payment transaction authorizations as a collaborating group of financial service providers, can be seen as a successful example of a SPG. The paper abstracts a framework for a SPG from observing in this example the way trust and power is established, distributed and transformed into policy-based rules governing interactions between users and members at operational level. SPG members interoperate with each other based on a common set of rules that are translated into policies via 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.

Trust and power concepts from organizational science are used to better understand how they relate to establishing rules, policies and their administration and enforcement. It will recognise why impersonal power is a means to conduce trust efficiently within and between organisations. 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 organisations. This is done by means of policies that are provisioned and enforced such that each participating organisation 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 carry different detailed meanings within each provider domain. However the effective outcome of a decision must be the same for every domain to create a uniform SPG defined network service. For example, some providers may decide as a policy to always carry connections across high available circuits always using redundancy, even if the service request specifies a best effort service. Another provider will route such connections without redundancy. Both providers know from the common rules that their policies are both correct when providing a service.

The paper also introduces briefly the concept of a Network Provider Group (NPG) that provides network connections across multiple domains. The NPG concept, an application specific incarnation of the SPG, is intended to allow independent network connection providers to interoperate to provide connections to its users as a group defined service.

Lastly, the paper will argue that well-defined rules can help multi-domain agent scenario's, where tokens based sequences are used to authorize services, is able to minimize the amount of information that needs to be exchanged in protocol objects.

1.1 Previous work.

In 2000 the IRTF Authentication, Authorization and Accounting (AAA) Architecture Research Group published RFC2904[1], describing a framework for authorization. The document identifies three basic conceptual entities involved in an authorization transaction. The AAA Server: Capable of making policy based authorization decisions, such as generically described in RFC2903[2]. The User: Making a service request that needs to be authorised. The Service Equipment: A resource in need of knowing if a User request can be granted based on the execution of some policy. The RFC organises these entities into a Service Provider that owns Service Equipment and a User Home Organisation, registering details of users involved in the authorization decision. Fig. 2 shows these elements. The diagram includes double lines that represent Service Agreements that must pre-exist in some form between the organisational elements. Note that when multiple User Home Organisations and Service Providers start to collaborate, arranging service agreements becomes more complex and is likely to become a role of some form of organisation. The SPG framework provides a way of dealing with this complexity.

```
+------+      +-------------------------+
|      |      | User Home Organization  |
|      |======|  +-------------------+  |
|      |      |  |    AAA Server     |  |
|      |      |  |                   |  |
|      |      |  +-------------------+  |
|      |      |                         |
|      |      +-------------------------+
|      |                 ||
|      |                 ||
|      |                 ||
| User |      +-------------------------+
|      |      | Service Provider        |
|      |      |  +-------------------+  |
|      |      |  |    AAA Server     |  |
|      |      |  |                   |  |
|      |      |  +-------------------+  |
|      |      |                         |
|      |      |  +-------------------+  |
|      |      |  |      Service      |  |
|      |      |  |     Equipment     |  |
|      |      |  +-------------------+  |
|      |      |                         |
+------+      +-------------------------+
```

Fig. 2 -- Service Agreements

Service Agreements are also called Trust Relationships in some of the AAA application examples[3] presented in RFC2905. Trust Relationships and Service Agreements are intertwined concepts where one cannot live without the other. Trust Relationships can be build at protocol level as result of an established Service Agreement or a Service Agreement can be seen as embedded in a Trusted Relationship between business actors and can as such be seen as a result of such relationship. In this paper we will focus on the latter notion that is more related to the human managed business level. The first notion is related to the operational/protocol level as discussed in RFC2904. It describes a number of typical sequences by which these entities may communicate to handle authorization requests (Push-, Pull and Agent sequence). Protocols languages including RADIUS, DIAMETER, COPS, SAML, etc., can be used to implement such sequences. Within the Networking domain, research has gone into exploring suitable protocols and mechanisms (a.o. GLIF[4], Internet2 ION[5], ESNet SDN[6], GEANT Autobahn[7] and G-Lambda[8]). This research is aimed at the automated creation of dedicated bandwidth network connections across multiple autonomous Service Provider Networks using one, or a combination of these typical sequences.

Recent activities in the Open Grid Forum (OGF) such as the OCCI[9] working group and Network Services Interface[10] working group (NSI-WG) have been fruitful in standardizing the interworking between service domains. The OCCI working group establishes an API and protocols for management of Cloud resources. Within the NSI work[11], as shown as example in fig. 3, Network Service Agents (NSA's) are capable of coordinating connection establishment across multiple networks in one of many possible topologies using the NSI protocol. Arranging a common set of rules and standards that determine the offered service and provides trust amongst collaborating providers, as member of a group, is however not in scope of the NSI effort. This paper may contribute by further describing the dashed elements shown here.

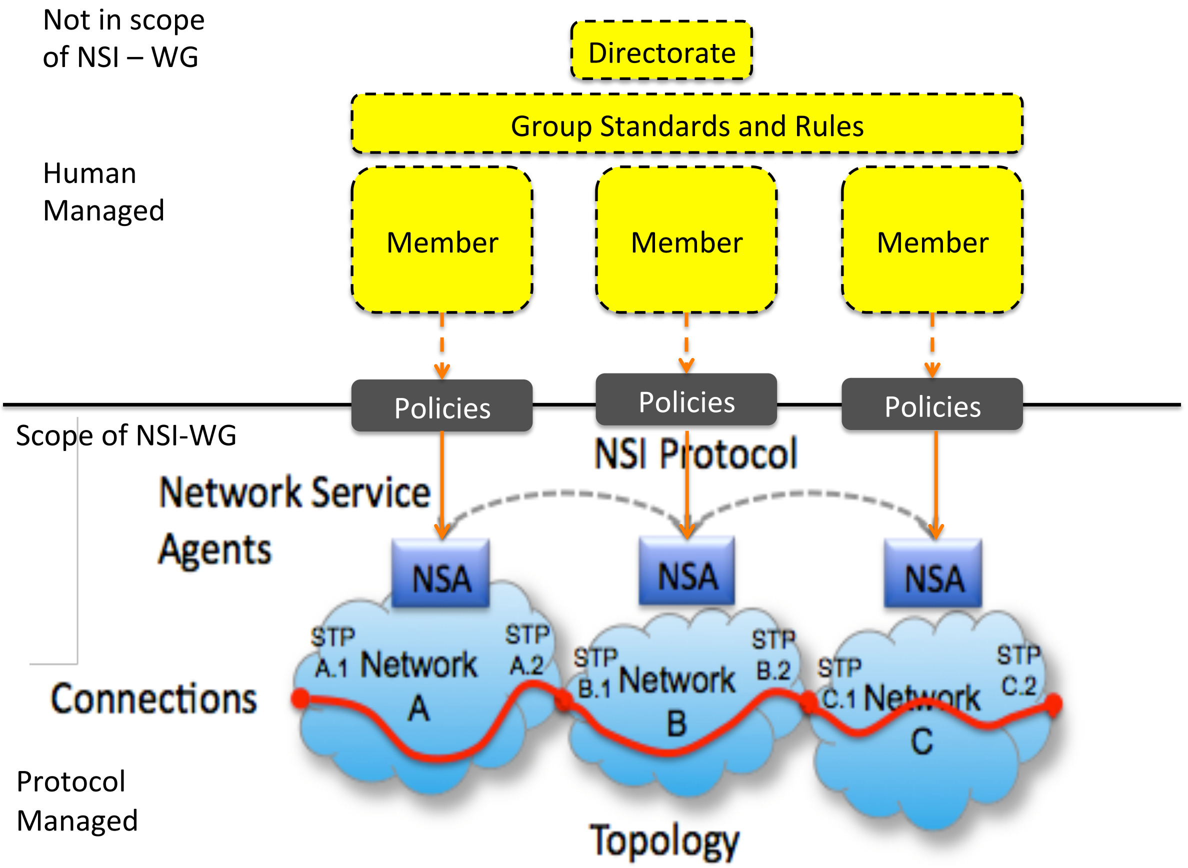

Fig 3: NSA's create automatically network connections by chaining network services from different networks. Arranging group standards and rules for collaborating members that determine policy elements that are known to be correct is not in scope of the NSI-WG effort.

Before NSA's can participate in authorization transactions, which would allow such connections to be created, RFC2904 recognizes that:

```
"There must be a set of known rules in place between entities in order for authorization
transactions to be executed. Trust is necessary to allow each entity to "know" that the
policy it is authorizing is correct. This is a business issue as well as a protocol
issue."
```

The above statement touches on the concept of trust governing authorization transactions. It is essential to understand that each entity participating in the handling of a transaction must have trust in the fact that the policy as a means to perform an authorization is the correct one. This fact creates a system where each entity knows to behave correctly in such a way that:

Trust Notion 1: Users trust the predictability of the system's outcome as a whole
Trust Notion 2: Collaborating entities trust each other to act in a correct, coordinated and predictable way, e.g. Service Providers and User Home Organisations in the RFC2904 case trust each other as members of a collaborating group.

As does RFC2904, the mentioned research initiatives assume that trust relationships based on service agreements and known rules to pre-exist before authorization transactions can take place. In order to augment the mentioned research and standard efforts (such as the NSI work), this paper will focus on the business issue side of the RFC2904 assumption.

We will show that the concept of a SPG is a viable option to arrange in particular Trust Notion 2: The case where an increasing group of providers need to collaborate as members of such a group to authorize and deliver an economic service. We have assumed that fulfilling Trust Notion 2 will be the basis to earn the Trust of Notion 1 (Users trusting the predictable outcome of a system).

To further explain the need for an SPG Framework we will now consider both needs identified generically and specifically for the optical networking case we refer to as the Network Provider Group case. We will then identify some requirements for a SPG.

1.2 The need for a SPG Framework

1.2.1 Expressed needs for a SGP Framework.

When studying the Anatomy of the Grid[12] in 2001, Ian Foster et. al. recognized that:

"The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations. The sharing that we are concerned with is not primarily file exchange but rather direct access to computers, software, data, and other resources, as is required by a range of collaborative problem-solving and resource- brokering strategies emerging in industry, science, and engineering. This sharing is, necessarily, highly controlled, with resource providers and consumers defining clearly and carefully just what is shared, who is allowed to share, and the conditions under which sharing occurs. A set of individuals and/or institutions defined by such sharing rules form what we call a virtual organization (VO)."

Ian Foster recognizes the need for a set of individuals and/or institutions that define sharing rules and rules that allow coordinated resource access and usage. Allowing VO's to define and implement sharing rules has been implemented by initiatives like EGI[13] that help National Grid Initiatives provide Grid Services across Europe to researchers and is successfully evolving.

In his position paper[14], Kees Neggers, at that time Director of SURFnet, the National Research & Education Network of the Netherlands and a founding participant of the GLIF, recommended in 2011:

"*European and national investments should together lead to a global service concept. This concept should be based on a federation of networking resources and technologies owned and operated by a variety of national, regional, European and international partners, coordinated in Europe through a collaborative effort under the GÉANT label".*

Kees envisaged a global service concept as an organisation, coordinating the delivery of a service under a single label. This concept should arrange the interactions between technologies owned and operated by a federation of autonomous partners.

Within recent cloud developments we can observe that:

1. The NIST Cloud Reference Architecture[15] recognizes the functions of a Cloud Broker and Cloud Auditor that are defined as:

- Cloud Auditor: *A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.*
- Cloud Broker: *An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.*

2. Cloud Infrastructure as a Service (IaaS) implementations are increasingly considering open source based cloud provisioning distributions like Open Nebula and OpenStack using an open standards based management interface like OGF's OCCI[16] allowing multiple external and internal cloud offerings to be *integrated*.

3. Gartner[17] defines hybrid cloud computing as: "*policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services*."

Functions of entities such as brokerage, policy based and coordinated service delivery, performing assessments, establishing and negotiating relationships, declaring the use of open standards for integration are essential to allow complex cloud scenario's to be established.

We took these general observations as evidence that there is a need in the evolving e-world to consider the development of a SPG framework that provides elements that provides rules and policies that coordinate resource access and usage, assesses and monitors services, operations, performance and security, negotiates relationships, integrates service offerings etc. An organisation based on the SPG Framework could be made responsible for performing such functions based on a common set of rules.

1.2.2 Specific Need: The Network Provider Group.

The Network Provider Group (NPG) concept, as a specific incarnation of the SPG concept, is motivated by the desire to understand how networks from different geographic areas can interact with each other to provide high bandwidth dynamic connections. National and regional optical networks have been created in different parts of the world (GLIF map[18]). Exchange points have been built where these networks interconnect (Dijkstra & de Laat[19]). Protocols for automating interconnection, developed by the NSI work group, are deployed (Chin P. Guok[20]). Some applications have been developed that take advantage of existing capabilities, and the potential to serve many more applications exists if the connection creation process can be automated (Internet2, 2012[21]) (Géant, 2012[22]).

The concern in a NPG is how resources used in such connections can be allocated with confidence to specific users. This requires resource providers to know resource requestors, and have some way of deciding whether to give a resource to a particular user at a particular time. This paper will show how this confidence can be built into the automating protocols.

The policy part of an NPG determines how collaborating members interact to define the service to be offered and how it is monitored and enforced. The operation part defines the protocol used to create and measure connections. At business level, the trust users have in the NPG service as a whole is the trust as meant by Trust Notion 1 of chapter 1.1, which is based on Trust Notion 2: The trust that deals with assurance that transactions are performed correctly at operational level by the organizations that are supposed to perform them.

NPGs are needed so that users can be sure they get the connection they request and so that providers can be sure they are providing the correct service to a known user. Within the group, each individual provider maintains autonomy and the ability to authorize its part of the connection using its own policies that are based on group rules.

1.3 SPG framework requirements.

The framework must describe how service providers, typically providing competitive services to the same market domain, could be structured to setup a collaboration that creates a chain of individually provided services. To deliver such services, the establishment of a SPG only makes sense when it provides a benefit to all of its members. The user expects the SPG to arrange a consistent service quality across multiple providers once service access has been authorized. After the SPG is put into existence and new members join, each new member must be offered efficient ways to acquire knowledge on how to correctly add its part to commonly defined services. Whilst taking its own policies and possibly National Law into account, a new member should be (within reason) able to correctly implement SPG defined rules. Members must develop policies that are used for authorization, coordination and delivery of a group service and to manage and avoid possible consequences of deviations. In essence common SPG rules and derived policies must be administered and enforced with each participating domain in such a way that all service providers act as one to allow benefit for all.

As MasterCard managed to achieve such service delivery across the globe, lets now examine how its power creates trust amongst its members and users and how its power is implemented. But before we do this, we first have to understand how we need to look at trust and power within our context.

2.0 What do we mean by Trust?

Trust is a broad concept studied in areas such as sociology and psychology. In this paper we place trust in the organisational context. Here, different actors (persons or organisations) need to have relationships that coordinate business activities that deliver goods or services. An elaborate overview of the concepts used within this context can be found in studies performed by Nootenboom[23] and Bachmann[24]. The following descriptions have been extracted from their studies and are used as a definition:

Trust in the organizational context is predominantly considered as a *means to cope with uncertainty*. Trust reduces uncertainty by allowing specific (rather then arbitrary) assumptions to be made about an actor's future behaviour. Trust inherently introduces a risk as trust can be disappointed. Finding *good reasons* can minimize such risk. Note that if the risk of disappointment were 0, then trust is not needed. Regulation and its *potential of sanctioning* is an effective remedy to confine risk by providing *good reasons*. When sanctioning is used however, it destroys trust and should therefore be used with care and reason. Commercial law and contracting practices are important elements that embed trans-organisational business relationships such that actors know what is expected from a good relationship.

Trust can be tacit, i.e. be an understanding living in the mind of one ore more persons. Such understanding can be made explicit, i.e. written down and as such be impersonalized. In this form it can act as a set of rules people or organisations can live by. When the rules are enforced, rules become the base of power. Let's look at how both forms (the personal and impersonal form) are distinguished in an attempt to position the role of a SPG.

2.1 Personal and Impersonal Trust.

Bachmann[25] specifically distinguishes between "*Personal Trust*" and "*Impersonal Trust*". *Personal trust* is trust that is formed by interaction between persons and grows with experience between one person and another. *Impersonal trust* is trust that is rooted in the tacit understanding of personal trust that is subsequently externalized and expanded into an explicit form of knowledge that is captured in law, rules, codes of conduct, etc.

With *impersonal trust* Bachman further distinguishes "*System Trust*" as trust *in the object* of trust and "*Institutional trust*" as trust *in the relationship* between actors that is embedded in the institutional framework.

System trust can be seen as *confidence in* rules and involved authorities executing such rules. A good example is the aviation system where ICAO, FAA, EASA and other (national) aviation regulatory bodies and authorities ensure the safety of citizens boarding a commercial plane. Citizens do not have to be aware of the risk involved in commercial flying but instead *have trust in the aviation system*. Important part of the system are the rules and regulations governing authorities that administer, qualify and oversee airlines, aircraft manufacturers, flight training organisations, maintenance organisations, etc. Authorities are given the power to qualify, license and monitor organisations and enforce rules, regulations, procedures, standards, etc. regarding the quality of aircrafts, its maintenance, operation, safety procedures, training, etc.

Institutional trust is trust in the relationship between actors embedded in legitimized normative rules, codes of conduct, standards, etc. Such rules, conduct, standards are legitimized by for example trade organisations, industry forums, professional associations, standards bodies, etc. Institutional trust plays for example an important role in sport, where participants are expected to compete in accordance to a set of rules established by an international sports union or federation. In competitions, participants trust each other that nobody cheats e.g. by taking drugs. Such trust is embedded in the impersonal social rules rooted in personal understanding and institutionalized by organisations such as WADA[26].

A glossary of terms used until now are summarized in table 1.

Term	**Description**
Trust *(within the organizational context)*	A means to cope with uncertainty
The risk of trust	Trust inherently introduces risk as trust can be disappointed.
Good reasons	Good reasons can be used to minimize risk.
Sanctioning	The potential of sanctioning is an effective remedy to confine risk by providing good reasons. When sanctioning is used it destroys trust.
Personal Trust	Experiences individuals make with each other in the course of frequent interaction over a longer period of time
(Impersonal) System Trust	Trust an individual has in the functioning and *in* the reliability of impersonal social structures
(Impersonal) Institutional Trust	Trust *between* individuals vis-à-vis existing impersonal social rules
Social Structure *(at individual level)*	The way norms shape the behaviour of actors within the social system.
Institutional Framework	The systems of formal laws, regulations, and procedures, and informal conventions, customs, and norms, that shape socioeconomic activity and behaviour.

Table 1: Trust concepts within the organisational context.

Bachmann notes that powerful institutional rules are able to control the expected behaviour that can both absorb risk and increase the chance that trust becomes a preferred mechanism to control the expected behaviour of actors. Unfortunately such trust is sometimes misplaced (as seen in several recent cases in the world of pro cycling). Trust is therefore not absolute and power is there to assist in an attempt to prevent misplacement. When power is used, for example by revoking titles and medals, trust is damaged.

This leads to the question of what the role of power is in relation to the concept of trust.

2.2 The role of Power.

Trust is not the only mechanism that can be used to make assumptions about an actor's expected behaviour. Power is a similar mechanism to trust as it too influences the selection of actions of an actor in the face of consequences. Power and trust are both means to achieve the same goal of coping with uncertainty. In essence trust makes *positive* assumptions about the willingness and ability of an actor to co-operate, whilst power is based on *negative* assumptions implying consequences. In practice, most relationships are based on a mixture of trust and power, where one of the mechanisms has a predominant role. Trust is often preferred as predominant role. However, when the *impact of risk* plays a significant role, relationships tend to rely more on power. Power will however only work if there is a realistic threat of sanctions.

Both trust and power can be applicable in personal and impersonal sense. In a parent-child relationship a child personally trusts a parent. Based on experience, a parent may have good reasons to personally trust the child to always attend school. If this trust is misplaced, a parent can use its personal power to ensure that a child will face consequences if its behaviour continues. The impersonal (institutional) power of the school and (system) power of the authorities may help parents in providing good reasons (consequences) to both child and parent. School (impersonally) and parents (personally) trust children not to cheat when taking a test by providing good reasons in the sense that both will stress that learning is important for the child's future and that cheating is a socially unaccepted behaviour. Good reasons are embedded in the social framework of a child. In addition a child will experience the impersonal power of school that he/she will be disqualified if caught cheating.

2.3 Trust and power types related to organisation size and risk impact.

From the example of 2.1 and 2.2 we can observe two dimensions that can be distinguished with both the personal and impersonal form of trust and power determining its predominant form: The number of actors involved (small, e.g. the parent-child situation or large, e.g. a school with many children) and the impact of risk (low or high). Fig. 4 shows these dimensions plotting the predominant trust relationship type into four quadrants depending on size and impact. This matrix will be used again later in this paper to position the role of the SPG in arranging trust and power with some examples.

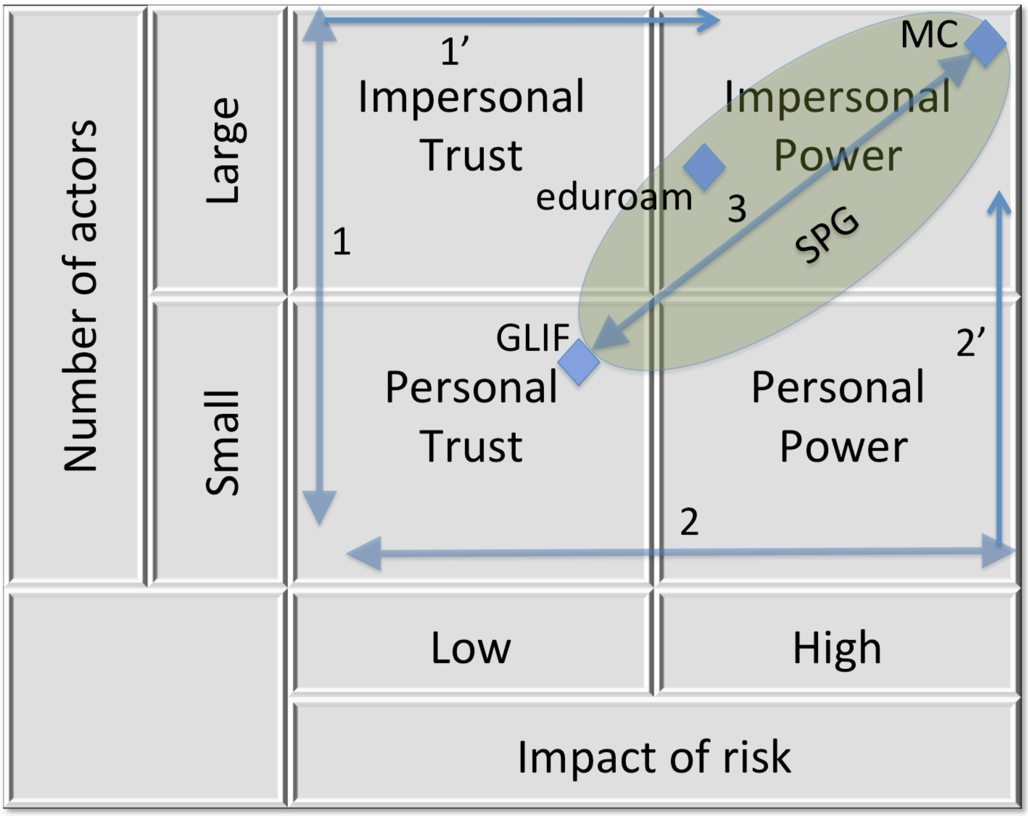

Fig 4. Predominant trust and power types related to number of actors involved and impact of risk

When moving your thought along line 1 from bottom to top, assuming consistent low impact, one can imagine that the amount of actors involved in a network of relationships determines the ease at which trust relationships can be maintained at personal level. When moving upward on line 1, one can see that an actor is limited in the ability to maintain personal relationships with other actors if the amount of relationships with different actors increases. An Nth actor has in theory to relate with N-1 actors to fully understand all existing tacit expectations of the group. Moreover tacit expectations are also likely to increase as more actors join. At some point all N actors are forced to make a part of the tacit expectations - that are understood as a group - explicit in the form of rules. This will allow the Nth+1 actor joining to understand the expectations in a more efficient way. This process is called institutionalisation. At some point, the amount of rules institutionalized will outgrow the number of tacit expectations that can be maintained at personal level. Now impersonal trust becomes the predominant way to trust an actor's expected behaviour. Impersonal trust is used as a term because actors typically also include system trust next to institutional trust. For example, the group likes to identify new actors by asking for authority issued credentials such as a passport, license, registration at chamber of commerce, etc. A relationship between a teacher of a small school and "ideal" pupils (that always can be trusted) can be placed at the bottom part of line 1. When the amount of ideal pupils increases, institutionalization of rules that need to be understood by ideal pupils becomes the predominant way of trust, moving the trust relationship type to the impersonal trust type quadrant. Note that with real pupils, the power of consequences will also be required to help determine the expected behaviour of pupils, moving the predominant trust type towards the impersonal power quadrant (arrow 1').

Line 2 is applicable to the parent child relationship mentioned earlier. For an ideal child - that always listens - the trust relationship can be placed at the far-left side of the line 2. If, however, a child's behaviour is impacting school results, the parent may decide to use its personal power by asserting consequences as the predominant way to trust the child. This moves this trust relationship type along line 2 to the personal power quadrant. Note that when results worsen, school (and in severe cases, the authorities) can become an active part of the relationship network of both parent and child. The position of such trust relationship will then to move to the impersonal power quadrant as the institutional power of school and system power of the authorities will become predominant. School and possibly authorities will take away personal trust and power from the parent (arrow 2').

When placed in this matrix, the trust relationship for example within the GLIF[4] collaboration can be positioned in the personal trust quadrant. Participating organisations personally trust each other to act in the spirit of GLIF collaboration. Participants are expected to pool their excess resources for the collective good of their communities. A single page straw man charter constitutes the basis of understanding within the GLIF. This is because too much regulation within research communities is considered to be counter-productive. It is commonly understood that regulation and associated bureaucracy endangers the freedom and agility needed for innovations to happen.

The SPG can be seen as an attempt to institutionalize personal trust and power to an impersonal form that makes doing business more effective in managing impact of risk. It also allows collaborations to grow by providing impersonal trust using personal trust, created by initiatives such as the GLIF, as starting point. The SPG concept will help such efforts to move somewhere along line 3.

When considering the combination of large number of actors and the large impact of risk (top right quadrant), regulation becomes increasingly important. In this sense Bachmann concluded that:

- in strongly regulated organisations, impersonal forms of trust and power tend to link into each other in such a way that powerful intra-organizational and environmental structures breed trust between individual actors in a highly efficient manner, whereas
- in weakly regulated organisations, by contrast, individual efforts to establish cooperation between relevant actors in the organization become more important.

The first regime fits the upper right quadrant whereas the latter regime fits the bottom left quadrant.

Bachmann noted that these organisational regimes form two extremes on a scale, where empirical cases can be found somewhere in between. Bachmann's observation intuitively fits the extremes of line 3 in fig. 4. Considering line 3 as a scale, we consider the SPG as a way to help facilitate the organisational transition from an informal and flexible initiative, mostly based on personal trust into a form that coordinates service delivery in a regulated way where power provides *good reasons* to provide trust. In this sense Bachmann confirms that: *"In strongly regulated organizations power primarily exists in the form of abstract rules and procedures. This form of power (that is impersonal power) is highly conducive to the production of institutional trust and system trust within the organization"*. In particular when organisations scale up, i.e. become more industrialized in managing economic value and involved risk, power defined by rules and regulation becomes predominant. By arranging rules and regulations, the SPG concept is intended to help organisations move to the upper right quadrant of fig. 4 as shown with the green shaded area.

In order to recognise the contours of an SPG in the light of fig. 4, it makes sense to look at an extreme case, i.e. a large-scale, highly regulated case that has matured over many years. A case that succeeded in managing risk in such a way it grew into a trusted global organisation. We believe that an example taken from the Payment Card Industry qualifies as such. We choose MasterCard (MC) as a qualifying example fitting the extreme case as shown in fig. 4. We could have chosen other examples such as Visa, Amex, etc. however as MC started as an association of a few collaborating banks, its evolution resembles the path of line 3 most closely. However, a SPG can also start the way Visa started as will be explained later. We will then use a networking example (eduroam, see 2.6) to recognize if the SPG contours fit.

2.4 Example from the Payment Card Industry.

"Master Charge" (now known as MasterCard) started as an understanding between 14 banks forming the Interbank Card Association (ICA) in 1966. Unlike other payment cards introduced earlier (Visa, Diners, etc.) a single entity did not dominate ICA and its members. Member committees were established in stead. These committees established rules for authorization, clearing and settlement, gradually creating more regulation introducing more impersonal power that allowed ICA to admit more members and manage the impact of risk.

MC arranges card payment authorization transactions to happen between four parties as shown in fig 5.

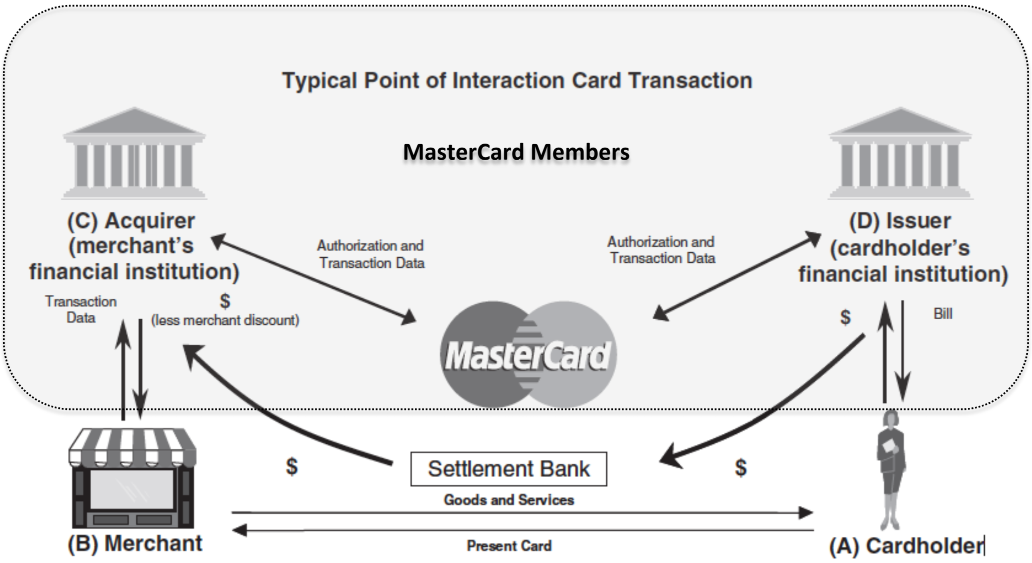
Typical Point of Interaction Card Transaction
MasterCard Members
(C) Acquirer (merchant's financial institution)
(D) Issuer (cardholder's financial institution)
Authorization and Transaction Data
Authorization and Transaction Data
Transaction Data
$ (less merchant discount)
$
Bill
MasterCard
Settlement Bank
$
$
Goods and Services
Present Card
(B) Merchant
(A) Cardholder

Fig 5. The role of MasterCard.

Cardholder (A) is issued a Card based on an agreement with Issuer (D). Amongst other things, the agreement determines the height of the payment limit that is extended to the Cardholder. Merchant (B) has an agreement with Acquirer (C) that arranges the authorization of a Merchant to accept a MC branded card and a Point of Sale (PoS) terminal capable of handling MC payment transactions. Note that Acquirers and Issuers are MC members. Merchants and Cardholders are users registered with MC Members. In general, after the cardholder has presented his/her card, the Merchant's PoS terminal will send an authorization request to its Acquirer. The Acquirer will use the MC Interchange Network to route the request to the Issuer based on the card number. The Issuer is then requested to authorize the requested amount and returns an authorization code if the payment limit is not exceeded. Once the Merchant PoS receives a positive authorization, the Merchant will hand over the purchased goods and the transaction is completed. The Merchant will receive the authorized amount (less a discount) into his bank account within a few days after the clearing & settlement process has taken place. To make this payment authorization system work between all involved parties, MasterCard Corporation Inc. has set up an elaborate set of rules for this Payment "Service Provider Group" consisting of competing but in this case collaborating financial institutes. Now that we better understand what trust means and know how an SPG is intended to help establish this, let's examine what it means that `"Trust is necessary to allow each entity to "know" that the policy it is authorizing is correct"` by considering Trust Notions 1 and 2 of chapter 1 as repeated in below table:

Trust Notion 1	Users trust the predictability of the system's outcome as a whole
Trust Notion 2	Collaborating entities trust each other to act in a correct, coordinated and predictable way

2.4.1 Considering Trust Notion 1.

When accepting a credit card as a means to pay, the merchant (as a user of the payment system) must have *system trust* in the payment- & banking system as a whole that, after his PoS terminal receives an authorization for the requested amount, the amount will be added to his bank account before handing over the goods to the cardholder. It also means that the merchant must have the knowledge to trust that he has followed the correct rules and procedures (*institutional* *trust*) when accepting the card from the cardholder and obtaining authorization for the transaction. For example, acquirers in Europe increasingly expect merchants to use PoS terminals that can use the embedded chip in the credit card that allows a PIN number to be entered on the PoS by the customer rather then using the old system with the less secure magnetic strip and customer signature. Only when using PIN, the merchant knows he will not be liable to fraud in case the card was stolen. Such liability has been shifted to the merchant when the magnetic strip / signature method is used. When using the magstripe, an element of *personal trust* is still involved as it is then up to the merchant to personally trust the cardholder to decide to ask for a picture ID (relying on *system trust* provided by national authorities) to verify the signature. Lastly the cardholder has *system trust* in both the consumer protection laws and the payment card system such that he/she will not be liable for any fraudulent transaction that might appear on the card account.

2.4.2 Considering Trust Notion 2.

By following the correct rules, regulations, bylaws, standards, etc. during its interactions with other financial institutes to correctly handle a transaction, each institute within the payment card system has the *institutional trust* that it will avoid damages or liabilities. For example, the issuer should check and decrease the payment limit when authorising the amount. If an institute chooses not to do so (e.g. by allowing default authorizations for amounts below a defined limit), all institutes know that this institute remains liable for the amount and cannot refuse the payment of the authorized amount during the clearing & settlement phase later in the process. Default authorizations will not cause damage to other banks. Also, all institutes must have enough liquidity to always be able to settle payments with other institutes. Every institute has the *system trust* that all other institutes are able to comply with this policy as all institutes reside under a National Bank that oversees compliancy.

2.4.3 Differences between Trust Notions 1 and 2.

In the light of these observations, we can see that RFC2904 only targets trust that is formalised in a Service Agreement (see fig. 2). This trust is embedded in the impersonal trust and power (rules) provided by a body such as MC. Note that Trust Notion 1 targets trust between a Person and an Organisation, whereas Trust Notion 2 targets intra-organisational trust between organisations. Clearly Trust Notion 1 involves both personal and impersonal trust elements, i.e. the organisations reputation next to impersonal trust that is arranged in the agreement with the user. Both are fundamental elements why users trust payment cards. Although difficult to separate[27], the willingness to rely on reputation tends to involve emotional factors, whereas relying on agreements tend to involve rational factors. MC must therefore use its institutional power to manage both Reputation and Agreements with users to breed trust towards its users as shown in fig 6.

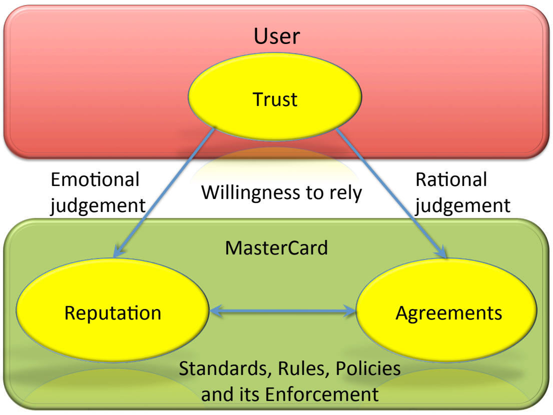

Fig. 6 the elements why users trust MasterCard.

Trust Notion 2 involves mostly *impersonal trust.* This as agreements between MC and their members arrange that members do not have to *personally trust* each other anymore as individual members. Sufficient regulation conduces the necessary *impersonal trust* as noted by Bachmann in chapter 2.3 regarding *abstract rules and procedures in strongly regulated organisations*. Agreements embedded in the institutional trust created by the MC Rules allows members to trust each other as shown in fig 7. All members trust MC to ensure new members can be trusted after joining. This trust is the basis for all interactions with the new member.

MC is responsible for managing the reputation of the member group as a whole and must have the power to be able to do so. Much of its regulation has been targeted towards avoiding reputation damage. Once a member signs its membership agreement, declaring it will comply with all MC Rules, MC Operating Regulations subsequently ensure up-to-date knowledge such that member banks can maintain compliancy.

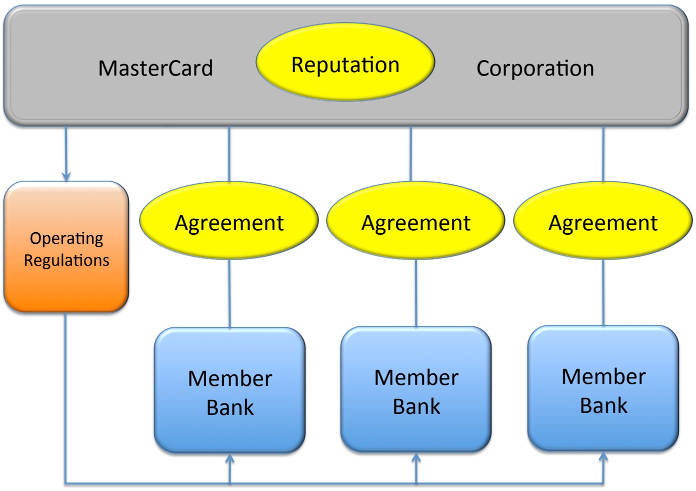

Fig 7: Why members trust each other via MasterCard.

2.6 Eduroam: A network related example of a SPG.

Eduroam[28] allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop. Eduroam allows participating research & education institutions, known as eduroam Service Providers (SP's), to provide access to students from any other participating institute that acts as Identity Provider (IdP). Eduroam is a federated roaming service that provides such secure network access by authenticating a user with their own credentials issued by their IdP. A group of National Research & Education Networks (NRENs) are in essence providing this service for their participating educational institutes under the eduroam "brand" arranged by TERENA. Fig. 2 is in essence the model used in eduroam, where a User Home Organisation is the IdP with an agreement with a User (student, researcher, etc.). SP's and IdP's have agreements with each other being a participant (group member) of eduroam.

Eduroam work started in 2003 as the TERENA Task-Force Mobility[29] with the overall aim: *"to assist in fostering trust between academic institutions and between NRENs so that these critical relationships can encourage active participation, and the development of roaming services*". In their first policy document[30], the taskforce clearly recognized that "*To facilitate the interest shown in roaming services it is important that policies are put in place at appropriate levels to ensure that benefits remain whilst threats and risks are minimized and managed within acceptable levels.*" In this document, task force members established a set of rules that outlined agreements to be signed between TERENA (facilitating in this case eduroam as SPG principal) and each participating NREN (Intra-NREN roaming policy) and agreements between an NREN and their participating national institutes (NREN level policy). In these institutionalized set of rules, NREN's and participating institutes were made responsible for administration, monitoring and enforcement of a number of rules. For example, NRENs were made responsible to write guidelines for participating institutions to assist them in drafting local site and user policies to ensure compliance with the roaming service agreements with their NREN. Participating institutes must report any security issues or fraudulent activities and log authentication sessions and network access session and be able to trace a user for both security and capacity planning purposes. Over the years, the initial agreement and their rules has evolved into a compliance statement[31] organising a confederation (federation of federations) that is funded by Géant[32]. A Global eduroam Governance Committee has been made responsible for the rules contained in the compliance statement and is also responsible for the final ruling on disputes that cannot be resolved within the community. Eduroam is available now in 60 territories worldwide.

2.7 Summary

Within eduroam, the first policy document was aimed at fostering trust between participants. It institutionalized *impersonal rules* and provided TERENA the *impersonal power* to admit by having NRENs sign agreements to participate in providing eduroam services. NREN's on its turn were made responsible to administer and enforce impersonal eduroam SGP rules towards its national institutes such that all participants had the correct knowledge to interoperate with other eduroam participants and understand what to do to minimize threats. Eduroam has a mechanism to allow their rules to evolve in a coordinated fashion. Fig. 4 shows the position of eduroam as SGP. Compared to MC, it manages less risk but has a significant amount of wordwide users; although less then MC. Note that fig. 4 does not attempt to provide an absolute scale.

Trust within MC is also conduced by a set of rules originally established by ICA. These rules have evolved over many years by MC continuously evaluating and enforcing them. Members have given MC the power to do so. This *impersonal power* ensures correct execution of payment authorization requests by making sure each of the entities precisely knows about the correctness of the policies it executes and also understand the consequences of non-compliance. This, however, does not always guarantee that *personal trust* (reputation) of its users can be maintained in individual cases as this also depends on personal expectations, new ways of fraud, changes in consumer laws, etc. MC has therefore the means and power to manage re-occurrences and changes by allowing it to continuously update its rules and regulation. With the establishment of ICA in 1966 MC started as an SPG on the left side of arrow 3 of fig 4 and slowly evolved to the right of arrow 3. Amongst a growing number of members managing more and more risk, MC maintained the necessary trust needed to allow each entity to "know" that the policy it is authorizing is correct. It was only able to do this by introducing more and more impersonal power based on its rules.

3.0 Conceptualizing the SPG Framework.

In this chapter we will conceptualize the SPG Framework from the observations of chapter 2. Here we will mainly consider the MC example and note that similar observations can be made when considering the eduroam example.

The MC Rules[33] are in essence rules that describe what it means to be a “Member” (or more recently a “Customer”) of MC. As these Rules change from time to time, we examined the MC Rules as they stood per July 2011.
The eduroam compliance statement in essence describes what it means to be a participant in the eduroam confederation.

3.1 Additional Terminology

In addition to the terms described in chapter 2, there are a few additional terms for MC and eduroam that need to be defined.

Context	Term	Description
MC	**Member, Membership**	A financial institution or other entity that has been granted membership in and has become a member of the Corporation in accordance with the Standards. “Membership” means membership in the Corporation.
MC	**Standards**	The Amended and Restated Certificate of Incorporation, Bylaws, Rules, and policies, and the operating regulations and procedures of the Corporation, including but not limited to any manuals, guides or bulletins, as may be amended from time to time.
MC	**Control**	As used herein, Control has such meaning as the Corporation deems appropriate in its sole discretion given the context of the usage of the term and all facts and circumstances the Corporation deems appropriate to consider. As a general guideline, Control often means to have, alone or together with another entity or entities, direct, indirect, legal, or beneficial possession (by contract or otherwise) of the power to direct the management and policies of another entity.
eduroam	**Identity Provider (IdP)**	An entity that is responsible for user credentials and operation of an authentication server for eduroam access for these users. IdPs are in some regions also known as “Home Institutions”
eduroam	**Service Provider (SP)**	An entity that operates an access network on which eduroam users are admitted to access Internet services once they are successfully authenticated by their IdP. SPs are in some regions also known as “Visited Institutions”.
eduroam	**Roaming Operator (RO)**	The entity that operates the eduroam service for a country or economy and that is recognised as such by the RC to which it belongs or, in case the country or economy is part of a geographic region for which no RC is established, by the GeGC. The RO may be a National Research and Education Network operator, for example. ROs are sometimes referred to as the “eduroam operators”.
eduroam	**RC**	An entity that consists of a cohesive set of ROs serving a geographical region and that is recognised as such by the GeGC. The “European eduroam Confederation” is one example.
eduroam	**GeGC**	The TERENA co-ordinated Global eduroam Governance committee (GeGC), comprises of representatives from ROs and RCs; they have written the compliance statement.

Table 2: Additional MasterCard & Eduroam terms

3.2 Analyses of MC rule examples.

By using some examples taken from the MC Rules, lets consider of how powerful MC is in interacting with its members and how various types of trust and power play a role.

MasterCard Corporation was (until recently) a membership organisation for financial institutions. When applying for membership, MC has the power to determine if an organisation does fulfil all its requirements. Members must be financial institutes that are recognized by a National Authority. Here, MC has *system trust* in competent National Authorities.

Issuers must have a License from the Corporation before they can issue cards to Cardholders. MC has the *institutional power* to arrange - via Licenses - the area's in which issuing activities may take place.

The power of MC goes beyond its members: An Acquirer must have a Merchant Agreement with their Merchants before the Merchant is authorized to accept Cards. According to the rules, MC has the *institutional power* to determine what provisions members must put into their agreements with merchants or cardholders and as such be in control.

More examples are given in the appendix. These examples show how MC manages Trust Notion 2 (chapter 1.1.) in an attempt to earn Trust Notion 1.

It is important to note that MC considers a failure to comply with any Standard, to adversely affect the Corporation and it's Members. It also undermines the integrity of the MasterCard system. The Integrity of the System is an important factor in the willingness of all involved parties to rely on it, i.e. trusting (both personally an impersonally) the reputation of the system.

3.3 Conceptualising the MC rules into the SPG.

In this chapter we will use the previous observations to conceptualise a framework describing how the SPG contributes toward building trust from impersonal power formed by its Standards. Here we recognize the personal and impersonal trust and power elements discussed in chapter 2.

3.3.1 Organising the Institutional Power using the Trias Politica.

Observing the MC Standards, i.e. the institutional power of MC Corporation, made us wonder how such power, and the ways it comes to play within MC and its member organisations can be organised in a more abstract way. A well-known abstraction, the "Trias Policia" by Charles de Montesquieu[34] recognizes three different types of power: Legislative, Judicial and Executive power. By classifying the MC Rules into these three categories we were able to observe what parts of power is given to MC members and what power resides in the domain of MC Corporation. We also could see what type of rules MC established in each of the power categories. We used below interpretation to classify the MC Standards. We could then find examples of MC Rules fitting into each category. A subsequent study of the eduroam rules provided more confidence in the applicability of this approach.

Power		
Legislative	**Judicial**	**Executive**
Power to make rules.	Power to determine interpretation of rules.	Power to administer and enforce rules.

Table 3: Used interpretation of Trias Politica

Note: with administration we mean the translation of the Standards into information needs, policies, procedures such that it can be applied to and supported by (automated) processes. We will use the term "rulemaking" instead of "legislative" as legislative implies creation of law by a deliberative assembly, whereas organisations, such as MC and eduroam create rules rather then law.

3.3.2 Functional Level perspective.

The RFC2904 AAA Authorization Framework describes a functional level that handles policy-based decisions authorizing access to resources. The policies are based on common rules and whatever has been agreed between the parties involved in the decision. As such, we can recognize the authorization transaction handling functions as the ‘Policy level’ that sits in between a level that determines what these policies are required to be (Business Level) and a level that represents the resources and its controls what these requests and applied policies are about (Operational Level). Table 4 contains a high level description of the main functions of each level.

Level	Description
Business Level	Builds and maintains a business structure that delivers defined services according to established rules and agreements between providers acting as a group. Responsible for administering and enforcing rules. Accountable for service delivery towards users.
Policy Level	Responsible for handling service authorization transactions by executing administered policies and controlling the operational level. Provides information that allows monitoring and enforcement.
Operational Level	Responsible for delivery of authorized service according to a service request and provides the proof of correct delivery. Providing information that allows monitoring and enforcement.

Table 4: Functional Levels

The Business, Policy and Operational levels have agents within each member’s organisation that are capable of putting the policies into operation driven by automated protocol exchanges. This will be further explained after we have explained more about the SPG framework.

3.4 The SPG Framework

As will be motivated by referring to actual rules, a further study of the MC Standards and previous considerations lead us to the compilation of the SPG framework as illustrated by fig’s 8, 9 and 10. MC and its Member’s are considered to be a form of SPG. Considering the eduroam rules provided evidence that the framework also fits in this context.

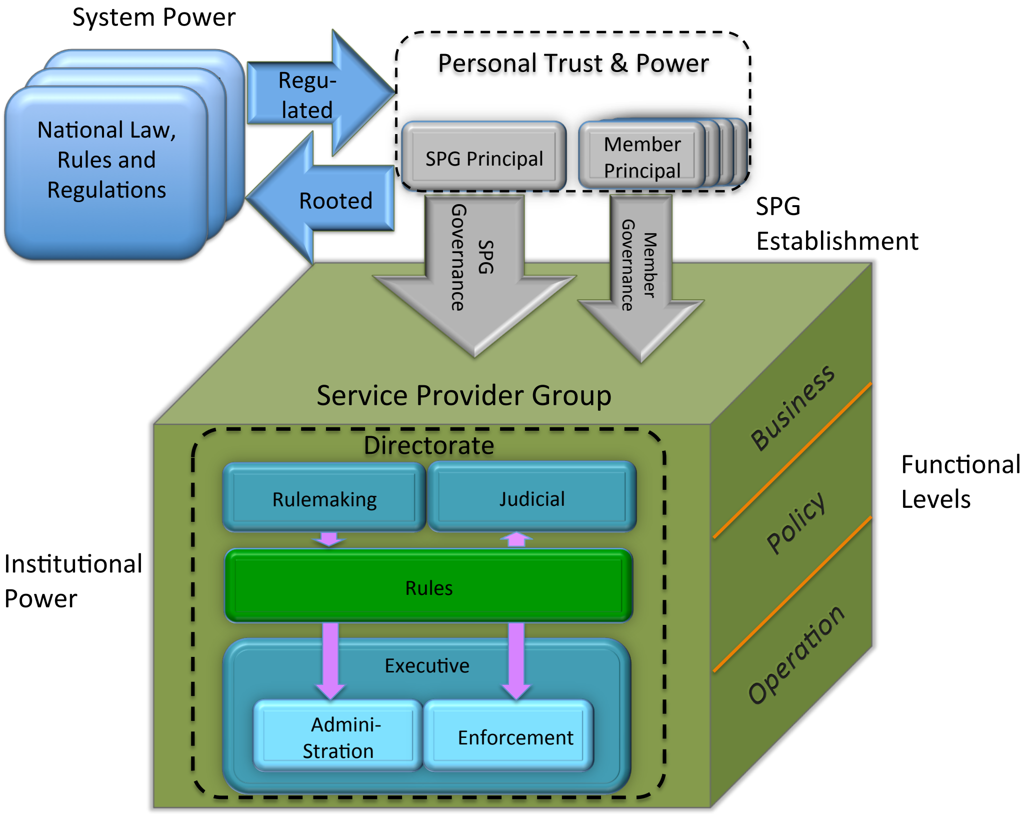

Fig 8. The SPG Framework high-level perspective.

3.4.1 High-Level perspective

Fig. 8 shows that the SPG can be considered from three perspectives: The establishment perspective, the power perspective and the functional perspective. A Principal is the actor of a service provider that can be held accountable for all its business activities and decisions. The assumption is that Principals, personally trusting each other, will establish a SPG after recognizing and agreeing on a mutual business benefit. MC was established as such by 14 banks as the International Card Association in 1966. The SPG Principal could also be a single entrepreneur using his network of trusted business partners. Bank of America established BankAmericard (later to become Visa) this way by starting with licensing their card service to other banks in 1965[35]. Eduroam was based on the recognition within TERENA that there was a need for allowing guest students hassle free network access using their own IdP credentials to authenticate from.

Based on consensus for a common business strategy, Principals will establish a SPG. During the formation of a SPG, Principals will either elect a SPG Principal (typically based on a combination of personal trust and power i.e. size of the contribution to the group) or the SPG Principal is the founding entrepreneur. The SPG Principal is subsequently held accountable for the activities, agreements and service delivery of the SPG as a whole. A Member Principal will determine what part of its resources will be made available to the SPG. The SPG Principal must define requirements for such contributions.

When creating its organisation, a Principal establishes a Directorate role as an efficient way to coordinate its activities. A Principal (via its Directorate) holds the institutional power of its organisation. Such power is used to control the three functional levels of an SPG organisation. The SPG consist of multiple SPG member organisations and a single SPG governing organisation.

When considering MC as a SPG, the chairperson and board of directors of MasterCard Inc. can be considered the Principal of the SPG governing organisation. The governing organisation's Principal appoints a CEO as it's Directorate head and is made responsible for establishing the three institutional powers (Rulemaking, Judicial and Executive) that will govern the SPG as a whole. This as the rulemaking power governs the behaviour of MC and its members by creating the MC Rules. The MC Executive Power is based on these Rules.

When considering Eduroam as SPG, TERENA acted as Principal that created a taskforce that performed rulemaking. Much of the executive power was given to the NRENs to oversee the national institutions. The later establishment of the Global eduroam Governance Committee formally can be seen as the SPG Directorate that established the Rulemaking and Judicial element. The Executive elements have been established as a confederation organizing the RC's / RO's as members that sign an agreement with the SPG Principal (Géant/Terena).

Any organisation's Principal must comply with National Law and their legal requirements. Here the SPG governing organisations Principle makes its Directorate responsible to oversee that it and its members activities always comply with applicable laws, even if a Member's National law and regulation contradicts SPG Standards. MC Rule 3.2 states to this respect: *Each Member at all times must conduct Activity in compliance with the Standards and with all applicable laws and regulations.* MC and Member organisation activities are as such rooted in applicable *system power* via the responsibility of the Principal.

Also National Authorities change regulation from time to time. For example, nowadays MC members may be required by their national authority to conform to BASEL III guidelines[36]. The SPG and its members are then also regulated by *system power* of the national authorities where applicable. Fig. 8 shows therefore two arrows between the Principles and the national Law, Rules and Regulations.

3.4.2 Organisation Viewpoint

Fig. 9 provides more detail describing the basic concepts shown in Fig. 8 considering the SPG Framework from an organisational viewpoint.

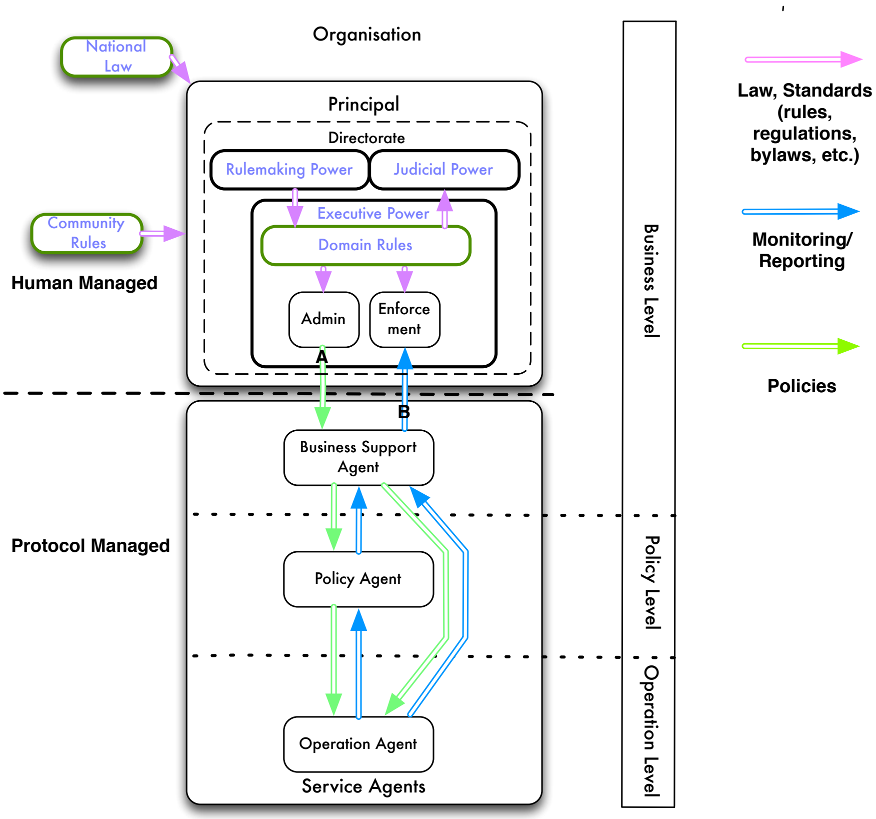

Fig 9. The SPG framework organisation viewpoint.

Fig 9. Shows details that are applicable to a participating Member organisation within the SPG. The Business level contains the Principal that holds the three powers via its Directorate. The Executive Power administers and enforces its activities using a Business Support Agent (BSA). The framework distinguishes Administration and Enforcement as separate elements of the Executive Power. Executive Power is defined as the authority to ensure activities are carried out according to the rules whilst facing potential consequences for non-compliance. Interpreting rules and implementing the resulting policies governing the operation and decisions within the relevant processes we define as administration. Keeping oversight over the outcome of processes and resulting services delivered we define as enforcement. Members

Principals are put in control by the SPG governing organisation for its activities that must be performed and overseen according to the community rules (standards). This can be observed from MC Rule 1.5.5-1: a *member must at all times be entirely responsible for and Control all aspects of its Activities, and the establishment and enforcement of all management and operating policies applicable to its Activities, in accordance with the Standards*; The term Control (table 2) implies that a Member must have the power to do so (even if choosen to outsource parts of its activities).

Within eduroam, the community rules clearly makes the Principal of a Roaming Operator (RO) responsible: Rule 4.1 of its compliance statement says: *The RO is responsible for ensuring the eduroam service operation within a particular country or economy.* Rule 4.3 states: *The RO has the authority to determine the eligibility of eduroam IdPs, being organisations engaged in research and/or education, in its country or economy*. Here the RO can make its own ruling to determine the eligibility of an IdP, however it must take national law into account to determine the legitimate status of an organisation as being involved in research and/or education.

A BSA is the overall management entity allowing a human interface into the system providing control, monitoring and reporting functions regarding the services provided. Administering the delivery system with the necessary policies based on applicable rules performs the control of the service delivery. The policies administered are based on the rules autonomously determined by the domain itself (domain rules) considering the institutionalized community rules provided by the SPG governing organisation and National Law. The service delivery system is build using functional service agents: The BSA, Policy agents and Operational Agents that handle service authorization transactions and service delivery. The Member organisation administration controls the BSA by determining for example what part of the available services will be assigned to the SPG, what its usage limits are, what users can request as a SPG defined service, what kind of information needs to be reported and/or enforced, etc. This type of information is provided via green arrow A. Via blue arrow B, the BSA will also provide information that need to be enforced according to the rules. Within a service provider domain, a BSA can (automatically) configure different forms of Policy- and Operational agents. As Fig. 3 imagines, a BSA could for example configure various types of Network Service Agents (NSAs)37,38. the OGF NSI working group is suggesting. The NSI NSA concepts then implements the protocol managed policy- and operational levels of a Network Provider Group.

3.4.3. Organisation Interaction viewpoint.

Fig 10. Shows how the SPG governing organisation interacts with its Member organisations. Member organisations that provide services (e.g. in the MC model the Acquirer) or Member organisations that register and represent users (e.g. the Issuer).

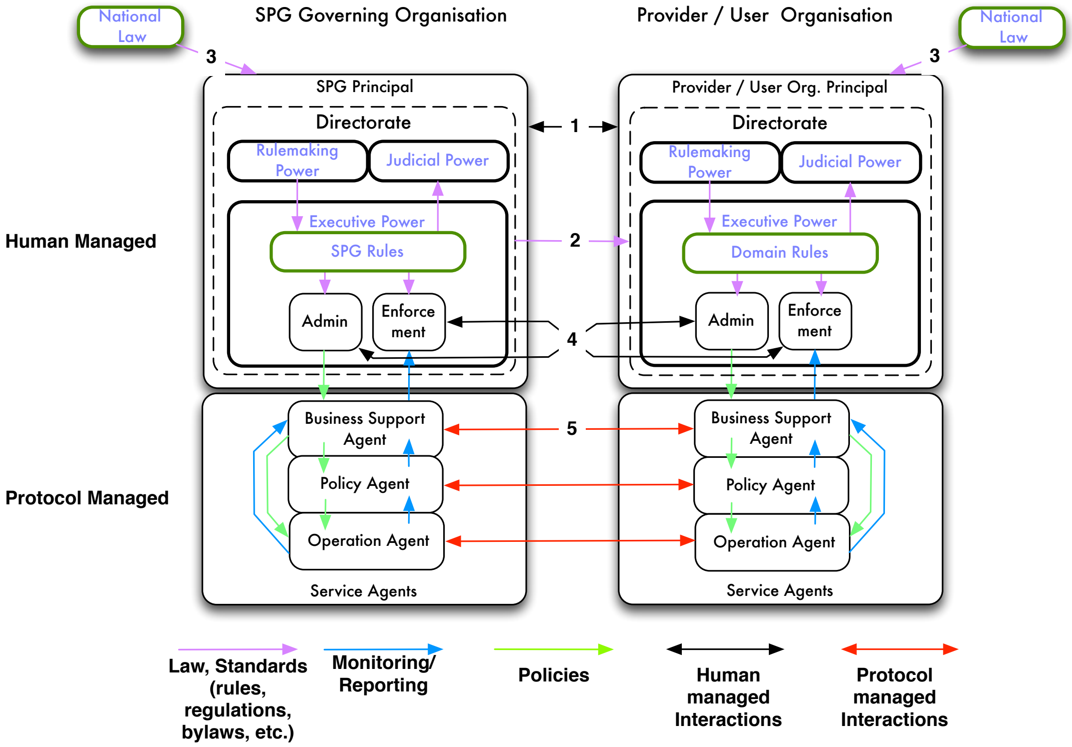

Fig 10. *Interactions between SPG and its Members (Provider/User Organisations).*

The Administration side of the SPG Executive Power refines the SPG Rules by adding bylaws, operational regulations, policies, etc. forming the SPG community rules (standards). By promulgating and enforcing these community rules (that change from time to time) the SPG governing organisation as such ensures that Members "`know when the policy it is authorizing is correct`." Hereto the Principal of a Member has signed an agreement (arrow 1) with the Principal of the SPG. Both MC rules (see table 2 definition of Standards) and Eduroam rules have provisions that allow rules to be amended. Eduroam states in this respect: *"This document is subject to change by the Global eduroam Governance committee (GeGC), based on feedback from ROs, RCs or individual eduroam users."*
This agreement is the root that builds trust between organisations as was illustrated in fig. 7 of the MC example. As result, the SPG Directorate provides the SPG community rules to the SPG Member Directorate (arrow 2) such that it can be integrated into the policies administered to the member's BSA and allow its enforcement. Note that the SPG executive power can also influence a SPG Member's Users behaviour as can be seen from MC Rule 5.1.1 and 5.3 (see appendix) where Merchants (as the User of an Acquirer) are not allowed to sell illegal goods and accept a credit card as payment method. The eduroam compliance statement for ROs contain statements that govern their SPs and IdPs (as users of the RO) by stating for example: *"By signing this document, an RO commits to ensure that the eduroam IdPs and eduroam SPs in its country or economy implement and adhere to the rules set forth herein."* Here the RO is expected to have executive power (administration & enforcement) over its IdP's and SPs.

MC Rule 1.5.5-3 states that a Member must *ensure that all policies applicable to its Activities conform to the Standards and comply with applicable laws and regulations.* This Rule states that the Members Principals must take into account applicable national laws and regulations and must also allow their activities to be regulated as shown by arrows 3. Member administrations must interpret their own Rules and the SPG Standards in the context of their National law and regulations and translate and implement them accordingly into their own policies. For example an Acquirer should create a policy for accepting credit card transactions that are used for commercial gambling. Accepting such transactions is depended on national or federal law (such as the US Unlawful Internet Gambling Enforcement Act[39]). Acquirers are responsible to implement a policy accordingly not to accept transactions from Merchants that fall under such law. When the outcome of theses policies is sufficiently enforced, it ensures the implementation of both *system trust* (national laws and regulations) and *institutional trust* (i.e. MC Standards) within the SPG avoiding liabilities. As seen earlier (rule 4.3), eduroam requires IdPs to be research and education institutes. There may be legal requirements to be recognized as an education institute.

The Enforcement side of the Executive Power is responsible for monitoring compliancy with the Rules and its refinements and should signal any issue found based on information that the Administration requests and Enforcement receives. Both Member- and SPG Directorates must oversee such requesting, signalling and enforcement as shown in with arrows 4. Business Support Agents may support such process, using automated protocols exchanges that automatically request and/or report information (arrow 5). The BSA will manage where such policies must be applied in the Policy- and Operation Agents.

The SPG Directorate Judicial power handles any disputes regarding the interpretation of rules and standards for SPG defined services and will decide on possible (disciplinary) measures. MC Rule 3.1 states to this respect: *From time to time, the Corporation promulgates Standards governing the conduct of Members and Activities. The Corporation has the sole right in its sole discretion to interpret and enforce the Standards. The Corporation has the right, but not the obligation, to resolve any dispute between or among Members including, but not limited to, any dispute involving the Corporation, the Standards, or the Members' respective Activities, and any such resolution by the Corporation is final and not subject to appeal or other reviews*.
The eduroam compliance statement says in this respect: "*In case of a dispute regarding the status of an entity (IdP, SP, RO) in the eduroam service that cannot be resolved by the responsible RO or RC, the GeGC will give the final ruling."*

Other SPG governing organisation activities could include soliciting, sales and marketing, admitting and administering members, defining services, keeping oversight and enforcement, handling complaints, etc.

3.4.4 BSA Responsibilities

A Principal will, by using its Executive power, delegate responsibilities (green arrows) to the BSA. The BSA will make one or more Policy and Operational Agents responsible for handling Service Authorizations and correct Service Delivery. The BSA is responsible for the Service Delivery architecture, i.e. the layout and management of Service Agent functions and their relationships across its infrastructure. Policy Agents are responsible for authorizing Service Requests based on administered policies and enabling Service Access. The exact meaning (semantics) of a Service Request (object) can be largely determined by the administered policies. The conditions of Service Delivery that are handled by Operation Agents are defined by the result of the administered policies. BSA's are expected to have the all required knowledge about how the administered SPG rules and policies can be implemented and enforced within its organisation. As such a BSA is responsible for implementing and enforcing the correct semantics of service request objects.

The Business Support Agent is responsible for collecting, aggregating, processing and reporting information to the Enforcement part (blue arrows). Such information originates from the Policy and Operation Agents that deliver Services. The Business Support Agent manages such collection and translates it into appropriate signals that trigger enforcement. It determines where Policy and Operational agents are required to collect what information and subsequently configures these agents with the correct policies.

When policies are correctly administered and enforced policies are "*known to be correct"* to handle the responsibility of authorizing a service request and putting corresponding services into operation. This "knowledge of being correct" is an important observation that influences the information need required in the protocol interactions exchanging request- and control objects between Agents.

3.5 Importance of SPG Standards for the information need within protocol object exchanges.

The more the Service semantics are handled by the impersonal power of standards via correctly implemented policies, the less need there is to communicate specifics about a service by protocol objects during the creation and fulfilment of a request. For example: The semantics and attributes describing a "Gold Service" may be entirely defined by the standards and its implemented policies. Communicating the fact that "A Gold Service" is needed between A and B for a specific time window may be sufficient to fulfil such a request. All SPG Members understand via the impersonal power of the standards precisely what "Gold Service" means and exactly know how such service should be provisioned using its policies. After making a request to the policy agent of an SPG member or the SPG itself, a user may be handed back a signed service reference by means of an abstract token that the Service has been arranged as requested as described in [Gommans[40]]. What such token means and how it should be created and subsequently treated could be entirely defined by SPG standards. Once inserted in the service infrastructure it may mean "give me Gold Service for the next 10 minutes". Each member is able to recognize such at token when enforcing individual service accesses across multiple SPG members. Each member may interpret a token differently as long as the result matches SPG requirements. A Bronze token implying "good for best effort service" may receive high available service in one domain whereas it may receive non-redundant services in others. This can be done because policies *are known to be correct* and therefore this knowledge does not have to be repeated within protocol information objects. This allows token mechanisms to be an efficient way to communicate authorizations across multiple domains once SPG standards are in place. However, as motivated in RFC2904, there are many other sequences available to request and deliver an authorized service. More work is needed to value each possible sequence given the fact that policies are known to be correct.

3.6 Reputation Management.

Agents also must provide the necessary accountability information (blue arrows) such that the enforcement organisation part of the executive power can keep oversight and enforce SPG standards. This is an important aspect allowing the SPG governing organisation to use credible impersonal power amongst SPG members. It also provides the ability of the SPG governing organisation to manage its reputation towards the SPG users and amongst SPG members. SPG members may be asked to report to the SPG governing organisation and/or allow assessments to be performed. The SPG governing organisation must be allowed to perform such assessments. What information could be asked to report is defined by SPG Standards. SPG Members are free in arranging such information themselves, as long as it fulfils SPG requirements. Eduroam compliance statement 4.9 states in this respect: *"The RO MUST make sure that the eduroam IdPs and eduroam SPs in its country or economy maintain sufficient logging information to allow the user identification process to terminate successfully.*"

3.7 The SPG framework applied to connection oriented networking.

Lets consider an application of the SPG framework in the case were a group of network providers are collaborating to provide connections as shown in NSI example (fig. 3) of the introduction. Let's assume that the principals of participating provider organisations, owning suitable lambda's and/or exchange points, have found business reasons to create a Network Provider Group (NPG). As said in the introduction, the NPG is an incarnation of the SPG framework applied to connection oriented network provisioning. The principals decide to create a NPG governing organisation by appointing a NPG principal. The NPG principal establishes a NPG governing organisation that is made responsible for coordinating the NPG activities using a directorate. The NPG directorate establishes institutional power by defining standards (rules, operating regulations, bylaws, etc.) for its members and defines under these standards what a service is and what delivery of a service means. Members have to agree to sign a service agreement with the NPG governing organisation and declare it will comply with the SPG standards that will change from time to time. Users, registered with each member are potential users of the NPG provided services. The user relationships will remain the responsibility of an NPG member acting as user organisation. Users, via its user organisation, can now request NPG services. NPG policies and terms become embedded in the service agreement with the user such that the user has an understood contract with the NPG governing organisation represented by the NPG member. The member now acts as an NPG agent for services provided by the NPG. The NPG principal is ultimately accountable for services delivered by the NPG. Members are accountable to the NPG governing organisation for the quality of delivered service contributions. Agents (e.g. OGF NSI-WG defined NSA agents) are configured and used to handle the responsibilities and accountabilities that provide the group services using policies.

4. Future work

We have shown a high level framework for a SPG that certainly needs more detailing. Future work is needed to describe in more detail what each power typically comprises of by studying more cases like MC and eduroam such as eduGAIN, EGI and various Géant connectivity services. Also the functional levels need more detailing in terms of functionalities and interworking with for example entities as described in the Network Service Architecture work of the OGF NSI working group and work that is done by the authors on Network Provider Groups.

The fact that SPG rules are administered as policies to Service Agents that *are known to be correct* is an important concept that needs further investigation. It plays an important role when determining the information and security needs for protocol objects being exchanged using sequences such as described by RFC2904.

The SPG framework is expected to be generic enough to be applied to many collaborating Service Provider cases as can be found within the infrastructure cloud arena build on converged infrastructures. Future studies are performed into these cases.

5. Conclusion

Increasingly, organizations rely on multi-domain converged infrastructure services performing their research and development or doing business. These services are composed of an aggregation of (competitive) individual infrastructure services. Such service composition is similar to competing banks offering MasterCard Card payment services or providing worldwide eduroam WiFi Internet Access services. Such services can only be provided by a collaborating group of autonomous service providers. The delivery of such end-to-end services needs coordination and oversight to ensure quality, manage risk and liability. The willingness to rely on such services is associated with trust. Trust in the chain of services becomes a chain of trust. When any part in such a chain fails, the trust in the service as a whole fails.

Power, in the form of impersonal rules, is an efficient way to conduce trust amongst large number of members of a Service Provider Group. In strongly regulated organizations, power primarily exists in the form of abstract rules and procedures. This form of power (that is impersonal power) is highly conducive to the production of institutional trust and system trust within organizations. As trust is not absolute, power is needed and must imply realistic consequences for non-compliance.

With MasterCard as an example of a SPG we can see that its rules provide knowledge to all its members and users such that everybody understands how the system should be used correctly. Intentional misuse (fraud) by users and/or service providers is detected and handled in a powerful way, but also in a way that users, when obeying the MC rules and regulations, are not harmed as MC has judicial power. When Cardholders, Merchants, Issuers and Acquirers know that the correct policies have been used during the authorization, everybody can trust that the end-to-end service will work reliable: Cardholders will only pay for ordered and received products, Merchants always get paid for the delivered goods or services and financial institutes have an agreed and viable way to manage and minimize fraud. The power of MasterCard will take the weak parts (non-compliant parties) out of the chain by excluding them as Cardholder, Merchants or financial service provider.

An organisation structure with role for a governing organisation was envisaged by Ian Foster for Grid infrastructures and by Kees Neggers for Network infrastructures. Helped by statements from NIST and Gartner and directions open Cloud standards are heading, we were encouraged to investigate how such a role can be described as a framework for a multi-domain service provider environment.

From observing MC we derived a framework for a Service Provider Group as a way to efficiently provide impersonal power needed to conduce trust amongst service providers such that all involved entities `"know" that the policy it is authorizing is correct`. The SPG Framework targets the business issue of organising such trust between service providers that can only deliver a service to a user if they collaborate. The roles of creating, executing (administration and enforcement) and judging SPG Rules are essential organisational entities. They must be established to provide and maintain rules that are accepted to give a SPG governing organisation the necessary power and credibility.

The Service Provider Group framework recognizes that it must be setup by a SPG Principal that obtains its mandate from Member Principals. In this phase personal trust between founding members is most important. When technology allows automated policy based setup and/or increasingly more participants join the collaboration, the SPG Framework is a way to arrange *impersonal power* that takes away the need to *personally trust* people to coordinate group activities. We have argued that a Service Provider Group is a concept that arranges *impersonal power* by establishing rules that can be translated into policies by administrations and applied to Service Agents of participants by using a Business Service Agent as linking element. Business Service Agents ensure with Policy and Delivery agents that executed policies can be trusted as "*known to be correct".*

Assuming that the knowledge about policies is correct, has important implications for the information needed inside protocol objects that are exchanged to authorize and deliver services. The more knowledge the administered policies provide, the less need there is to communicate such knowledge inside protocol objects. This allows the exchange of abstract or simple tokens between service providers as proof of service authorization.

MasterCard, that initially stood example for the SPG framework, has proven to be a way of providing and maintaining trusted end-to-end services for the benefit of both customers and service providers. The SPG governing organisation should keep both benefits in mind to be viable. We motivated that the SPG framework is also applicable to multi-domain network connection infrastructures and clouds.

Eduroam is a successful confederation joining Service- and Identity Providers as worldwide participants providing WiFi Internet Access that a student can trust to work hassle free. We have shown that several elements of the eduroam Compliance Statement do fit the essence of SPG framework.

6. Acknowledgement.

The authors wish to thank Mr. Alex Bewier of International Card Services, for his constructive feedback on the abstractions describing the Payment Card Services and its interactions.

We like to thank David Spence, Guy Roberts, Jerry Sobieski, Yuri Demchenko, and many other people from the GLIF and OGF community for their discussions.

We like to thank Internet2, OGF and the GLIF community for their support and opportunities to meet and present the concepts at their meetings and for their feedback. The authors like to thank Internet2 for waiving fees when attending their member meetings.

This work was partly supported by the SURFnet Research on Networks project and the Netherlands COMMIT project (P20.3).

The lead author would like to thank Mr. Timor Slamet, Director Technical CIO/IS of Air France - KLM, for the time and opportunity provided to work on this paper and KLM for the support given.

Appendix: Additional examples of rules that show the power of MasterCard.

From the MasterCard Rules we can observe some additional rules showing the power of the organisation:

MC and the Acquirer have the power to enforce the correct use of their Brand Marks as it both may audit the Merchant's activities when it uses the MC Brand Marks pursuant to a Merchant Agreement. An Acquirer is in violation of MC Rule 5.1.1: *Before entering into, extending, or renewing a Merchant Agreement, an Acquirer must verify that the Merchant from which it intends to acquire Transactions is a bona fide business* - if it knows a Merchant sells illegal goods.

With Rule 5.3: *Each Acquirer must monitor on an ongoing basis the Activity and use of the Marks of each of its Merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards* MC has the power to ask the Acquirer to monitor its Merchants.

Rule 5.10 shows how far reaching this power of MC can go: *If the Corporation becomes aware of a Merchant's noncompliance with any Standard, the Corporation may notify the Acquirer of such noncompliance and may assess the Acquirer, and the Acquirer must promptly cause the Merchant to discontinue the noncompliant practice.* Clearly the Acquirer itself must have the power to monitor and terminate the Merchant agreement if the Merchant does not discontinue the noncompliant practice.

Note that the MC Rules defines its Standards that not only include the Rules itself but also its bylaws, operating regulations, policies, etc. Standards are based on the Rules and contain more details as a result of the interpretation of the Rules.

References

[1] J.Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, **RFC2904 AAA Authorization Framework**, IETF Aug. 2000.

[2] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, **RFC2903 Generic AAA Architecture**, IETF Aug 2000.

[3] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence , **RFC2905 AAA Authorization Application Examples,** IETF Aug 2000.

[4] http://www.glif.is

[5] http://www.internet2.edu/ion

[6] http://www.es.net/network/

[7] http://www.geant2.net/server/show/ConWebDoc.2544

[8] http://www.g-lambda.net

[9] The Open Cloud Computing Interface working group: http://occi-wg.org

[10] http://www.ogf.org/gf/group_info/view.php?group=nsi-wg

[11] Guy Roberts, Tomohiro Kudoh, Inder Monga, Jerry Sobieski, John Vollbrecht, **GFD.173 Network Service Interface Framework V1.0**, OGF 2010. http://www.ogf.org/documents/GFD.173.pdf

[12] Ian Foster, Carl Kesselman, Steve Tuecke, **The Anatomy of the Grid,** The International Journal of High Performance Computing Applications, Fall 2001 vol. 15 no. 3 200-222, Sage Journals, doi: 10.1177/109434200101500302

[13] http://www.egi.eu

[14] Kees Neggers, **Position Paper for GEANT High Level Expert Group,** Surfnet 18 Januari 2011 www.surfnet.nl/Documents/rapport_201104_SN_Position_Paper_for_GEANT_High_Level_Expert_Group.pdf

[15] Fang Liu, Jin Tong, Jian Mao, Robert, Bohn, John Messina, Lee Badger and Dawn Leaf, **NIST Cloud Computing Reference Architecture,** SP500-292, NIST September 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[16] http://occi-wg.org

[17] http://www.gartner.com/it-glossary/hybrid-cloud-computing/

[18] GLIF, G. L. (2011). *GLIF Maps.* Retrieved from http://www.glif.is/publications: http://www.glif.is/publications/maps/

[19] Freek Dijkstra, Cees de Laat, **Optical Exchanges**, GLIF: http://www.glif.is/publications/papers/20041029KdL_OpticalExchanges.pdf

[20] Chin P. Guok, David W. Robertson, Evangelos Chaniotakis, Mary R. Thompson, William Johnston, Brian Tierney, **A User Driven Dynamic Circuit Network Implementation,** Lawrence Berkeley National Laboratory, 2009, http://escholarship.org/uc/item/9pv0k61r

[21] Internet2, **Internet2 Innovation Platform FAQ**, 2012, http://www.internet2.edu/pubs/Internet2-Innovation-Platform-FAQ.pdf

[22] GEANT. (n.d.). **GEANT exhibiting at Supercomputing 2012.** Retrieved Nov 30, 2012, from www.geant.net: http://www.geant.net/Media_Centre/News/Pages/GEANT_at_SC12.aspx

[23] Bart Nootenboom**, The Trust Process in Organisations**, Edward Elgar Publishing, 2003, ISBN 1 84376 078 9

[24] Reinhard Bachmann, **Trust, Power and Control in Trans-Organisational Relations**, EGOS Studies 2001, 22/2 pg 337-365, 0170-8406/01 0022-0012

[25] Reinhard Bachmann, **The Trust Process in Organisations**, **chapter 4,** Edward Elgar Publishing, 2003, ISBN 1 84376 078 9

[26] http://www.wada-ama.org/

[27] Bart Nootenboom, Frederique Six, **The Trust process in Organisations, chapter 1**, Edward Elgar Publishing, 2003, ISBN 1 84376 078 9

[28] https://www.eduroam.org/

[29] http://www.terena.org/activities/tf-mobility/

[30] Terena Mobility Task Force, **Deliverable I: TF-Mobility roaming policy document, version 1.2**, http://www.terena.org/activities/tf-mobility/deliverables/delI/Roaming_policy_document_v.1.2.pdf , Terena 2003.

[31] Eduroam compliance statement, https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf

[32] http://www.geant.net/Services/UserAccessAndApplications/Pages/eduroam.aspx

[33] MasterCard Rules July 2011 (versions change frequently) http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf

[34] ***La défense de L'Esprit des lois***, Charles de Montesquieu, Barrillot & Fils, Geneve, 1748

[35] http://en.wikipedia.org/wiki/Visa_Inc

[36] Basel Committee on Banking Supervision, **Basel III: A global regulatory framework for more resilient banks and banking systems,** Bank for International Settlements, December 2010, ISBN print: 92-9131-859-0

[37] Guy Roberts, Tomohiro Kudoh, Inder Monga, Jerry Sobieski, John Vollbrecht, GFD.173 Network Services Framework v1.0, OGF, 2010

[38] Tomohiro Kudoh, Guy Roberts, Inder Monga, **Network Services Interface: An Interface for Requesting Dynamic Inter-datacenter Networks, NSI paper at OFC2013,** http://www.opticsinfobase.org/abstract.cfm?URI=OFC-2013-OM2D.3

[39] **PROHIBITION ON FUNDING OF UNLAWFUL INTERNET GAMBLING, Adoption of Unlawful Internet Gambling Enforcement Act,** FEDERAL RESERVE SYSTEM, 12 CFR Part 233 Regulation GG; Docket No. R-1298 - DEPARTMENT OF THE TREASURY 31 CFR Part 132RIN 1505-AB78.

[40] Leon Gommans, Li Xu, Fred Wan, Yuri Demchenko, Mihai Cristea, Robert Meijer, Cees de Laat , **"Multi-Domain Lightpath Authorization using Tokens"**, Future Generation Computing Systems, Vol 25, issue 2, 2008, pp 153-160, DOI 10.1016/j.future.2008.07.013