Trust Framework for Multi-Domain Authorization

Building and organising trust amongst a group of service providers and their users

Internet2 Spring Meeting
Arlington April 25th 2012

Leon Gommans: leon.gommans@uva.nl
John Vollbrecht: jrv@umich.edu
This work is funded by GigaPort3 / Surfnet / Air France - KLM
Content

- Introduction
  - Evolution AAA Authorization Framework
  - What is the problem?
  - What we learned from MasterCard
- Service Provider Group concept
- A “GLIF” lookalike as hypothetical example
Questions from the IRTF AAA Arch work.

How to organise a service with multiple organisations?

Agreement? Trust?

User?

Governance?

Org Group?

Fig. 9 -- Distributed Services
Why are the questions important?

Suppose I want to set up a connection between UvA in Amsterdam to another University or Institute.

Although possible, setting up connections to any place across the globe for a scientist is still hard (authority, knowledge, payment, etc.)

Can this problem be solved?

• By my network provider on his own? – It will be hard, in particular when based on bi-lateral agreements, different technology standards, policies, fee structures, etc.
• By a network provider as member of a Service Provider Group? We believe it can be.

What is a Service Provider Group?

A Service Provider Group (SPG) is an organisation structured to provide a defined service that is only available if its members collaborate.
Imagine how a Network SPG could look

The SPG appears to me as a worldwide connection service such that:

1. The service is provided to me by my local provider acting as SPG agent.
2. I can make connection to places outside my own provider
3. I trust any connection to work as agreed.
4. I understand the connection characteristics I get.
5. I know the SPG will monitor my connection.
6. I know who to talk to in case of questions or issues.
7. I have an agreed way to deal (financially, operationally) with connection failures.
What does joining a SPG mean for my Network Provider?

1. It allows it to make connections to places outside its own domain.
2. Expands usage by enabling connections by customers from other domains.
3. SPG standards ensure consistency of services between domains.
4. SPG policies define monitoring, debugging and auditing of multi-domain connections.
5. SPG regulations ensure fairness amongst providers: Resource treatment, value add, competition, risk, etc.
Why did we study MasterCard as SPG?

<table>
<thead>
<tr>
<th></th>
<th>eduroam</th>
<th>Skyteam</th>
<th>EGI.eu</th>
<th>MasterCard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>WiFi Internet Access</td>
<td>Airport Priorities</td>
<td>E-Science Grid Operation</td>
<td>Payment &amp; Processing</td>
</tr>
<tr>
<td>Maturity</td>
<td>2003</td>
<td>2000</td>
<td>2010</td>
<td>1966</td>
</tr>
<tr>
<td>Documentation</td>
<td>public</td>
<td>private</td>
<td>public</td>
<td>public</td>
</tr>
<tr>
<td>Members</td>
<td>36 Federations</td>
<td>15 Airline Partners</td>
<td>30 Countries 300 Data Centres</td>
<td>25.000+ 210 countries</td>
</tr>
<tr>
<td>Risk Involved</td>
<td>Low</td>
<td>Medium</td>
<td>?</td>
<td>High</td>
</tr>
<tr>
<td>Level studied</td>
<td>Detailed</td>
<td>Low</td>
<td>Low</td>
<td>Detailed</td>
</tr>
<tr>
<td>Complexity</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
What does MasterCard do?

MasterCard allows its member financial institutions to serve merchants and cardholders with a card payment & processing service that is trusted worldwide.
The anatomy of the MC SPG

National Law, Rules and Regulations

MC Service Provider Group

MasterCard Corporation (Directorate)

Legislative
Judicial
Executive
Enforcement
Administration
Member Banks

Organisational Level Perspective

Enterprise
Authorization
Operation

Organisational Distribution of Power Perspective
Distribution of Power Perspective

Legislative
- Membership
- Service
- Licenses
- Risk Management
- Non-compliance
- Fees
- Chargebacks
- Liability
- ...

Judicial
- Arbitration
- Penalties
- Appeals
- ...

Enforcement
- Rules
- Licenses
- Messages
- Reports
- Markings
- AML
- ...

Executive
- Membership Agreements
- Processes
- Monitoring
- Fee collection
- Appeals
- Auditing
- ...

MasterCard Corporation (Directorate)

Member
Banks

Administrative
CC SPG Level Model

Credit Card Services

Customer
Card Holder
Issuer
Issuer
Credit Card Org. Directorate
Acquirer
Acquirer
Merchant

Processor
Card
Credit Limit
Issuing Service Agents
Transaction Routing
PoS Service
Acquiring Service Agents
PoS Terminal

Operations Level
Cardholder Account Agent
Current Account
Issuer Account
CC Account

Automated Clearing House
Settlement Bank
National Bank

Enterprise Level

Authorization Level
Merchant Account Agent

Cardholder Bank
Merchant Bank
Why Users Trust MasterCard

User

Trust

Emotional judgement

Willingness to rely

Rational judgement

MasterCard

Reputation

Agreements

Standards, Rules, Policies and its Enforcement
Why members trust each other

MC Service Provider Group

MasterCard

Reputation

Corporation

Agreement

Member Bank

Agreement

Member Bank

Agreement

Member Bank
Service Provider Group Characteristics

- A group of member organizations that act together to provide a service none could provide on its own
- To a customer the SPG appears as a single provider
- To members the SPG appears as a collaborative group with standards, rules and policies that are defined and enforced by the group
- SPG has “Directorate” with Judicial, Legislative and Executive power in and for SPG
- Customer signs SPG Service Agreement with member
- Member acts as agent for SPG
Three organizational levels – SPG and Customer

- SPG and customer set up service agreement
- SPG authorizes Service based on agreement and resource availability
- SPG provides Service to consumer

Organization levels provide framework that puts independent functions in separate levels
SPG concepts – Directorate provides trust exercising power in every layer

• Enterprise
  – Defines service and service agreements
  – Defines policies

• Authorization
  – Enforces policies
  – Assigns providers to service instance

• Operation
  – Monitors service instances
  – Supports customer
GLIF-like Connection Service SPG

- Service makes connections between users over multiplexed ports from user to SPG
- Providers are networks and exchanges whose connectivity allows them to make the requested connections
- Work on this kind of project is being done at GLIF, OGF NSI WG, GENI, Mantychore, OpenFlow and more
Connection SPG - Organization levels

- **Enterprise**
  - Defines connection characteristics
  - Makes/enforces rules and policy
  - Responsible for actions of other levels

- **Authorization**
  - Authorizes connection requests
  - Assigns providers to requests
  - Provisions connection instances

- **Operation**
  - Controls physical equipment
  - Monitors and reports on each connection instance
GLIF-like Service Provider Group Group

Actors

• Members –
  – Regional and national network providers
  – Exchanges [GOLEs]
  – Local or commercial networks – perhaps as associate members
  – Organizations that authorize users – not necessarily the same as members providing networks

• Customers/ Users
  – Groups, individuals, with a “service agreement” with SPG member
  – Professor Researchers or Student at School of Member
  – Networks using SPG to extend their service

• Directorate
  – Executive direction of SPG
  – Provider policy group
  – Operation Monitoring group
Connection Service SPG
Directorate Enterprise Level Activities

• Directorate with Legislative, Judicial and Executive power
  – For MasterCard it is “the Corporation” for GLIF it is tbd
• Define membership requirements
  • Specify common goals as well as resources and capabilities
• Define how users relate to members
  • Funding, security requirements
• Establish funding for SPG capabilities
• Define Connection parameters and Service levels
• Monitor and enforce member-member rules
• Develop and maintain authorization and operation infrastructures and policies
• Set up and monitor all SPG infrastructure operations
Trust infrastructure and Connection Transaction Trust

Setup - infrastructure

Dynamic connection Transaction
Authorizing GLIF-like Connections

• Customer requests a connection
• Directorate algorithm determines how to satisfy a connection request
  – Uses topology and policy information
• Authorization result
  • Approved connection for user
  • Provisioning for each participating provider agent
• Authorization depends on policy of participating actors
Authorization Transaction

- Customer requestor initiates the transaction
- Agents trust each other in level because they trust members
- Requestor is authenticated by “home” member
- Request is authorized by participating members
  - [tree/ chain or combination may be used]
- Successful Authorization → “operation provisioning” request
- Transaction path is part of infrastructure setup by Enterprise level
Authorization Paths

Basic Push Model

Basic Agent Model

Basic Pull Model

Transaction Architecture
Two levels and path between them
Levels and path can be implemented independently

Risk analysis needed of each level independently and then as a whole
Possible to plug and play level infrastructures
Authorization Paths

• Risk analysis of paths is part of Trust of SPG
• Authorization and Provisioning varies
  – Inline (pull) vs out of band requests
  – Direct (agent) vs Ticket (push)
  – Security requirements
• Risk and Security analysis supports Trust of SPG
• Cost analysis is a financial performance not trust issue
Level 1 - Operation

• Operation agents control networks and exchanges
• Operation agents setup connections on direction from authz level
• Operation level monitors connection
  – Reports to customer and Directorate
Layer architecture in “Service Provider Organization”

• Enterprise Level initiates and maintains service creation infrastructure in Authorization and Operation levels
  – Basis of trust in other layers

• Authorization Level applies policy to a request
  – Policy of SPG and of individual members
  – Creates an “approved instance” that is given to Operation level

• Operation Level carries out approved instance
  – Monitors and reports on instances
SPG Conclusions

• Enterprise level needed establish basic trust relations between members
• Trust requires rules, policy, a Directorate [and funding for Directorate]
• Separating Authorization and Operation creates infrastructure that can be analyzed and trusted
• Standardized Inter-level transaction methods allow risk analysis for each method
Questions you might help with

- How does directorate concept fit GLIF-like model
  - Is it possible to combine for profit and not for profit organizations
  - What trust is needed what risks can be taken
  - What rules and policies will need to be in place
  - How does it compare to MC or EduRoam

- Is a ticket or token (push) model useful for connection service

- How does scheduling fit the three level model

- What is the difference between a user and a member in a the connection service

- Others?