Creating a SARNET Alliance

by applying the Service Provider Group Framework and by using the Ciena/GENI testbed

April 29th 2015

Leon Gommans: leon.gommans@klm.com

Content

- Introduction
- **S**ecurity **A**utonomous **R**esponse **NET**work research
- **S**ervice **P**rovider **G**roup framework
- How framework will be studied using **GENI** concepts
- Research Questions:
  - SARNET alliance feasibility?
  - Future networking: is SPG a way to define & deliver “slice archetypes”?

Note: session is about federating services assuming Identity federation has been arranged.

Internet Security envisioned in RFC 1958*

*Brian Carpenter, “Architectural Principles of the Internet”, RFC 1958, IETF June 1996.

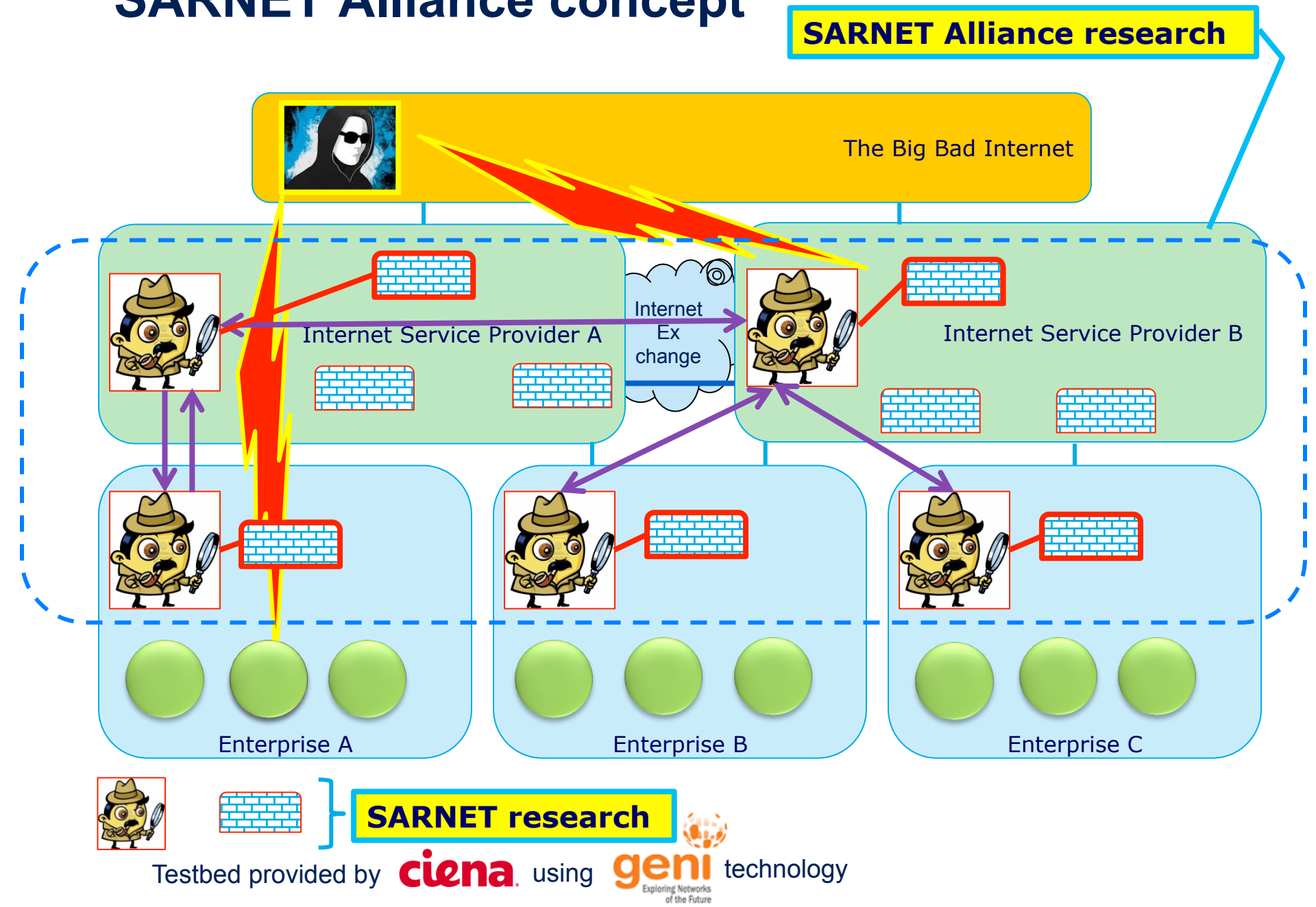
Cyber Security readiness

Creating a SARNET Alliance
Sharing intelligence and defensive power

SARNET
Security state / defense tactics automation

SARNET
Topology dynamics

SARNET Alliance concept



SARNET Projects

Security **A**utonomous **R**esponse **NET**work project:

Studies best ways to provide autonomous responses to cyber-security threats by automated security state monitoring using software defined, virtualized detection & defense mechanisms. Funded by NWO National Cyber Security Research Agenda

2 PhD students, research team: Air France KLM, Ciena, TNO and UvA.

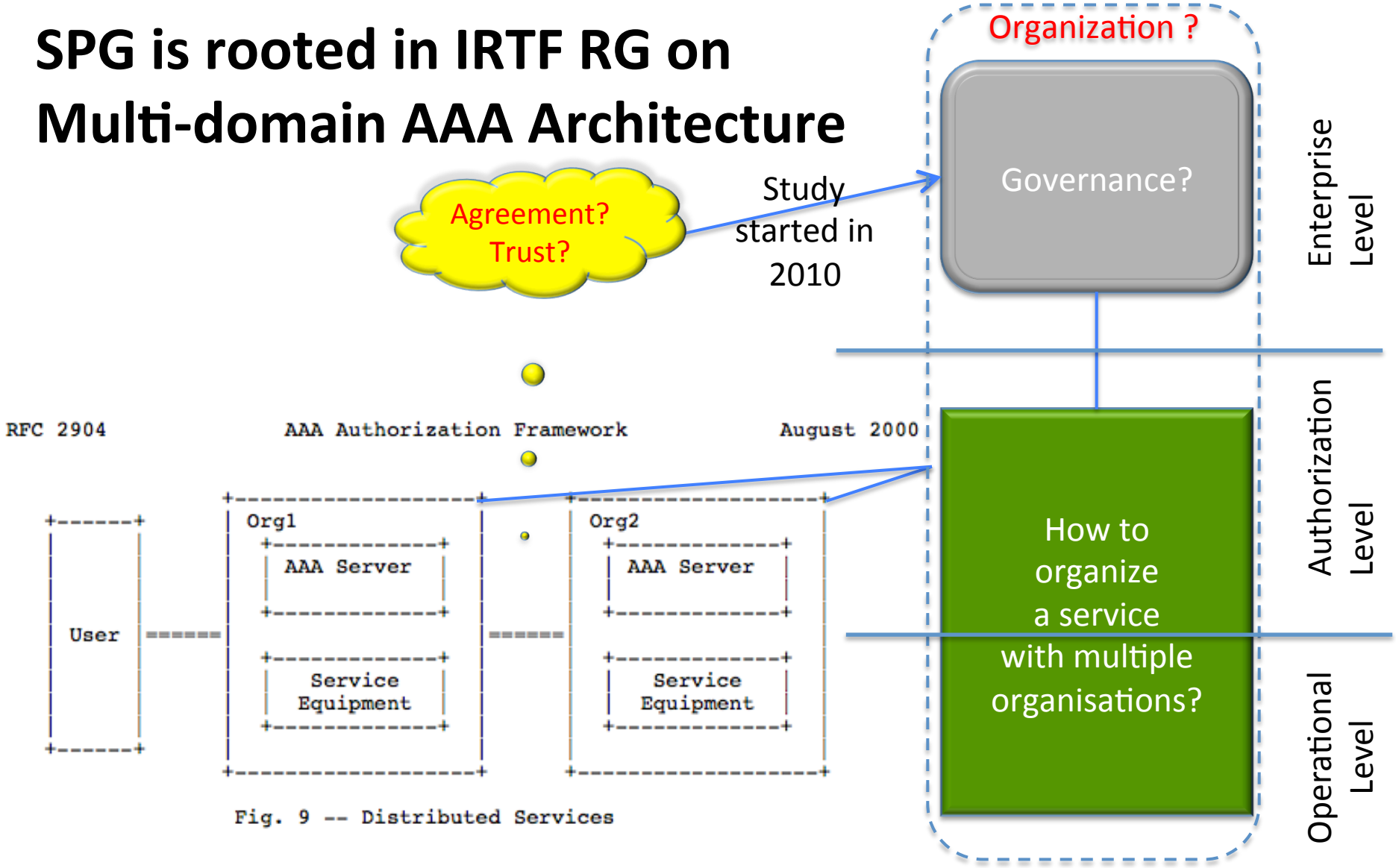
SARNET forms the context for a research project considering the applicability of the Service Provider Group concept:

Creating a SARNET Alliance project:

Studies how to organize SARNET functionalities across multiple Service Provider- and Enterprise Networks, where each participant must trust other participants to correctly detect and mitigate cyber threats, whilst authorizing each other to be involved. Funded by Dutch ministry of economic affairs

1 PhD student, research team: Air France KLM, COMMIT/, CS- and Legal faculty UvA.

SPG is rooted in IRTF RG on Multi-domain AAA Architecture



Service Provider Group framework

A Service Provider Group (SPG) is an organisation structure providing a defined service only available if its members collaborate.

Examples:

Internet2 NET+

SKYTEAM

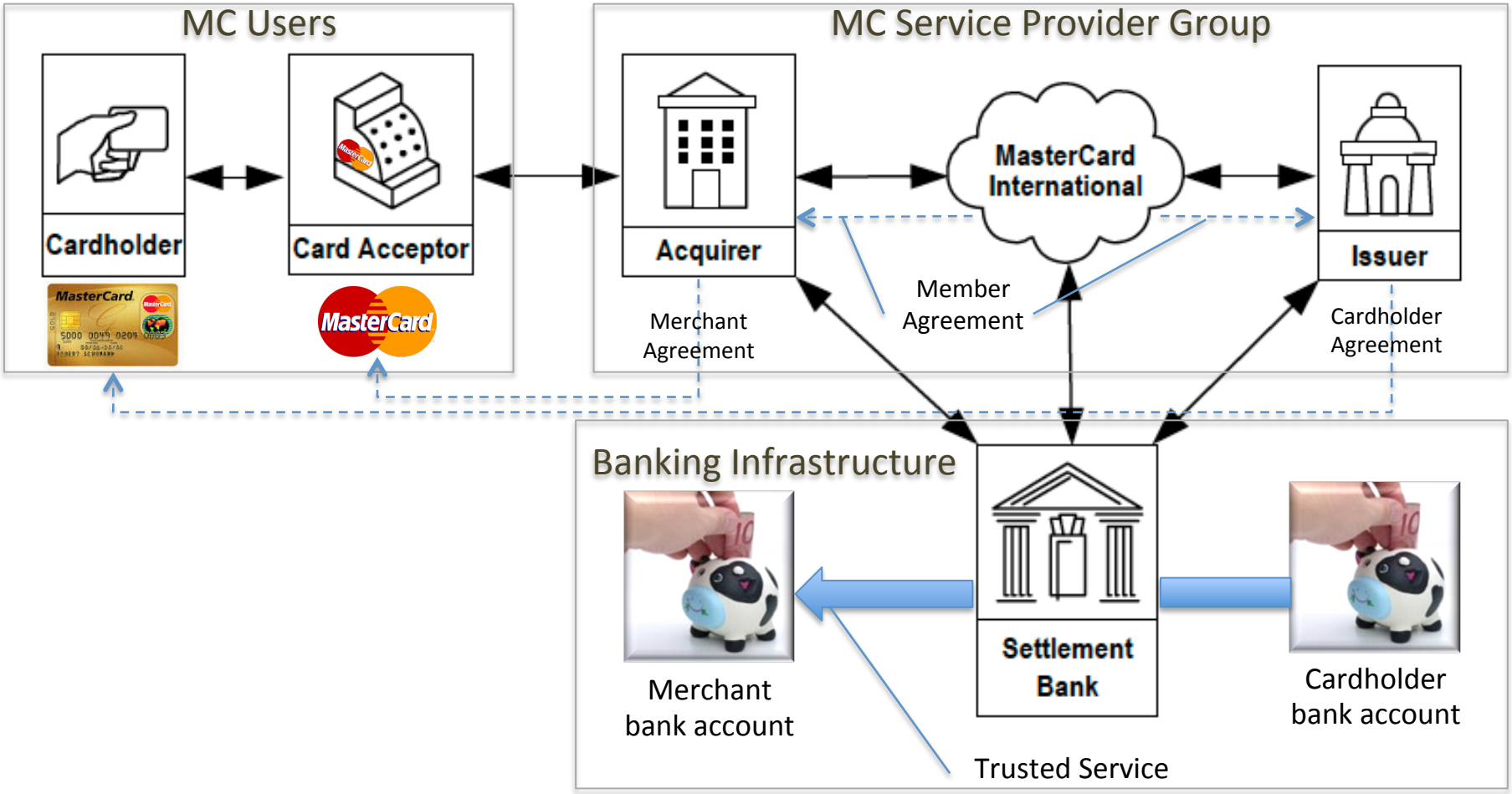
geni
Exploring Networks of the Future

glif

eduroam

MasterCard

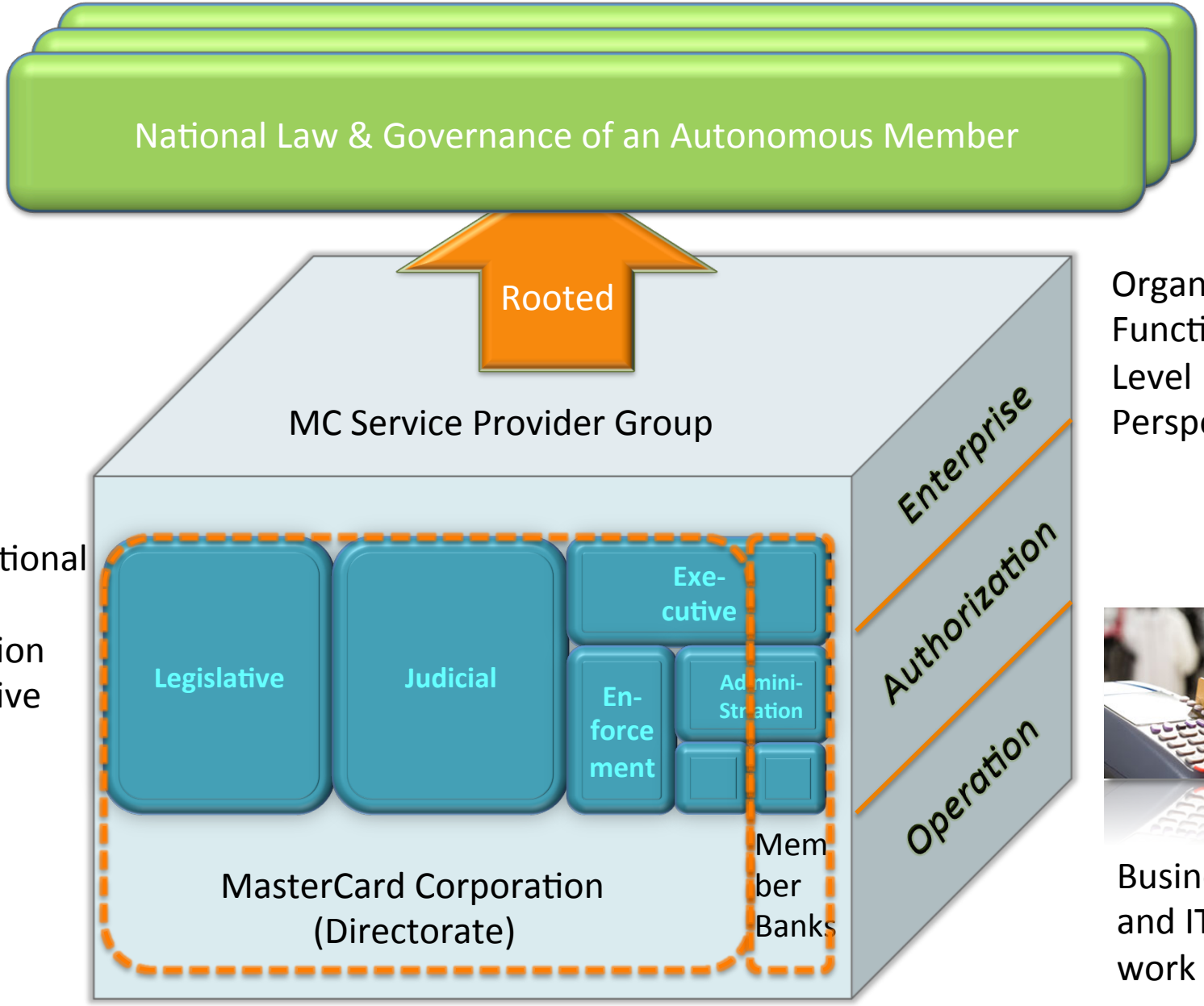
Study of a highly trusted collaborative service



MasterCard allows its member financial institutions to serve merchants and cardholders with a card payment & processing service that is trusted worldwide.

MC rule study: anatomy of the SPG

(presented I2 Spring member meeting 2012)

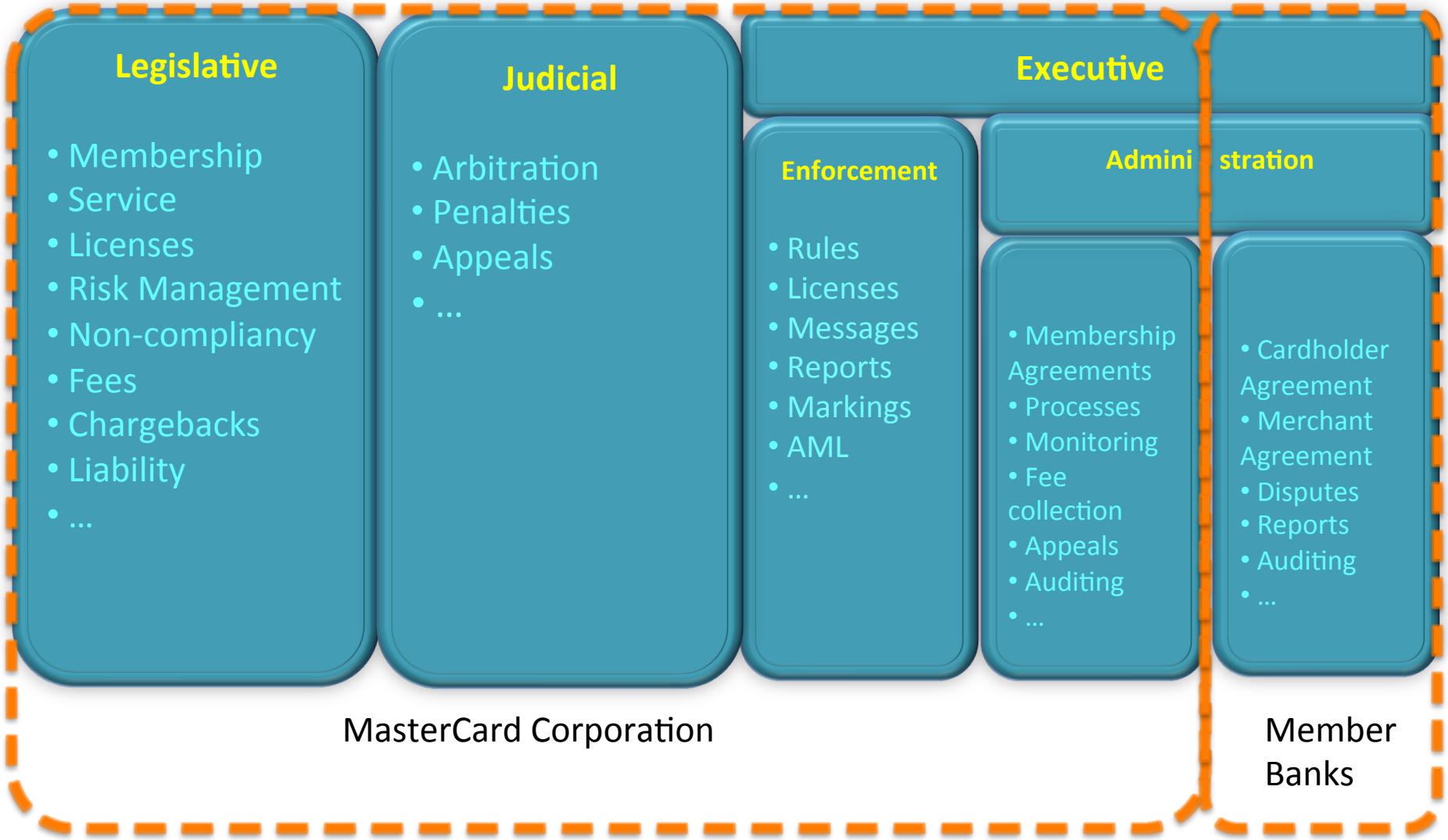


Organisational Power Distribution Perspective

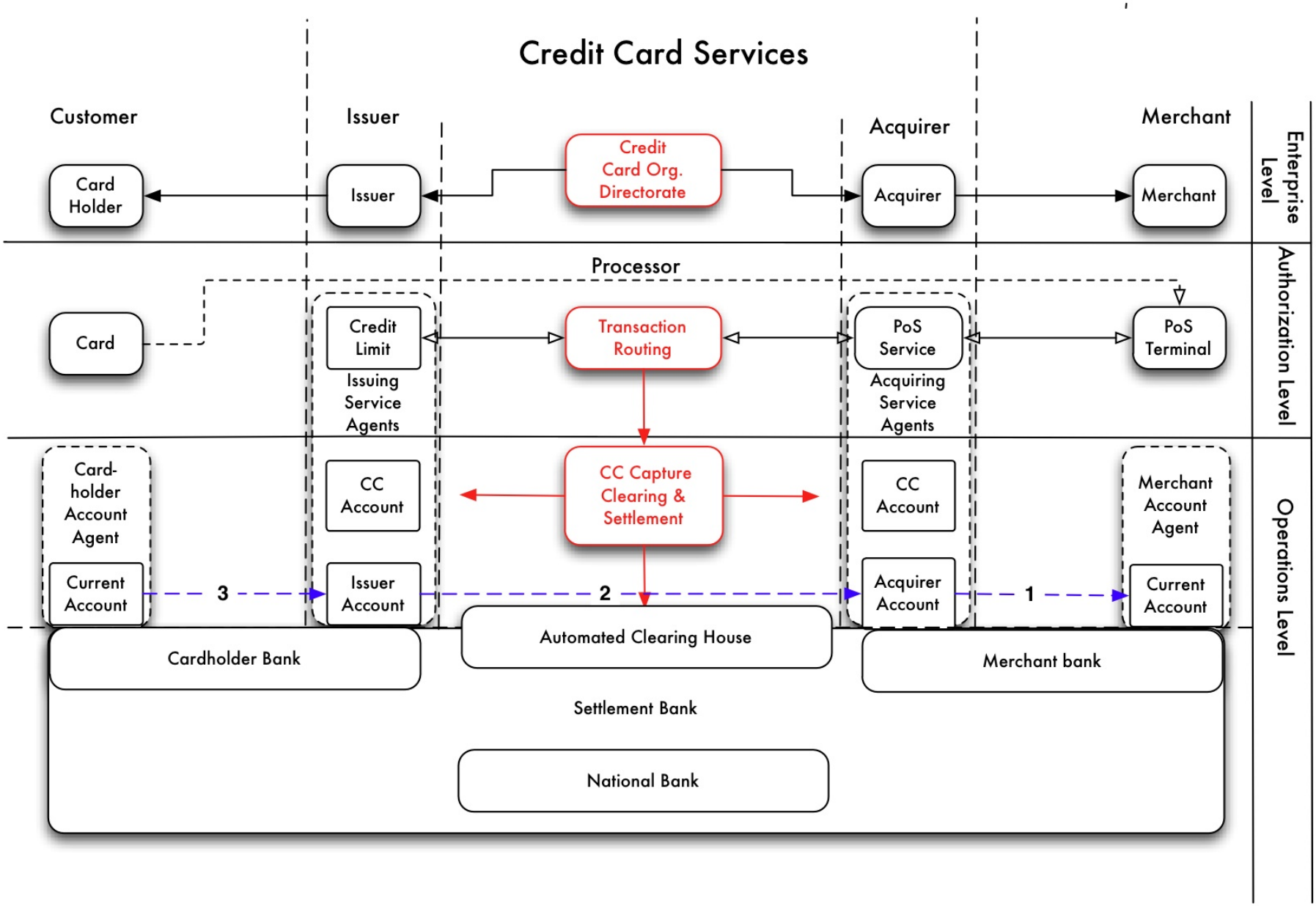
Organisational Functional Level Perspective

Business, Legal and IT have to work together

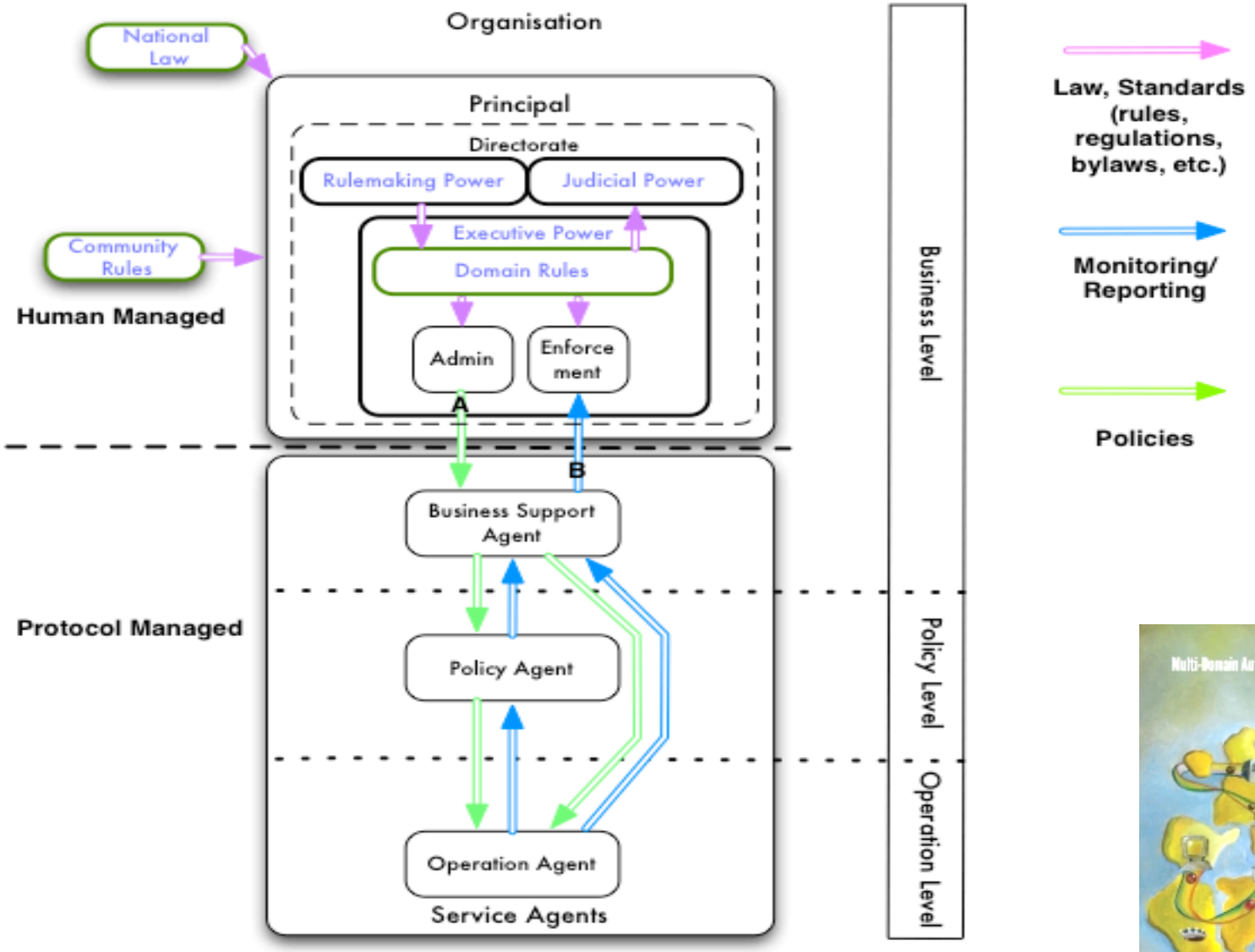
Mapping rules that create trust on types of power



Fit functional level model



SPG Framework showing key elements organizing trust.

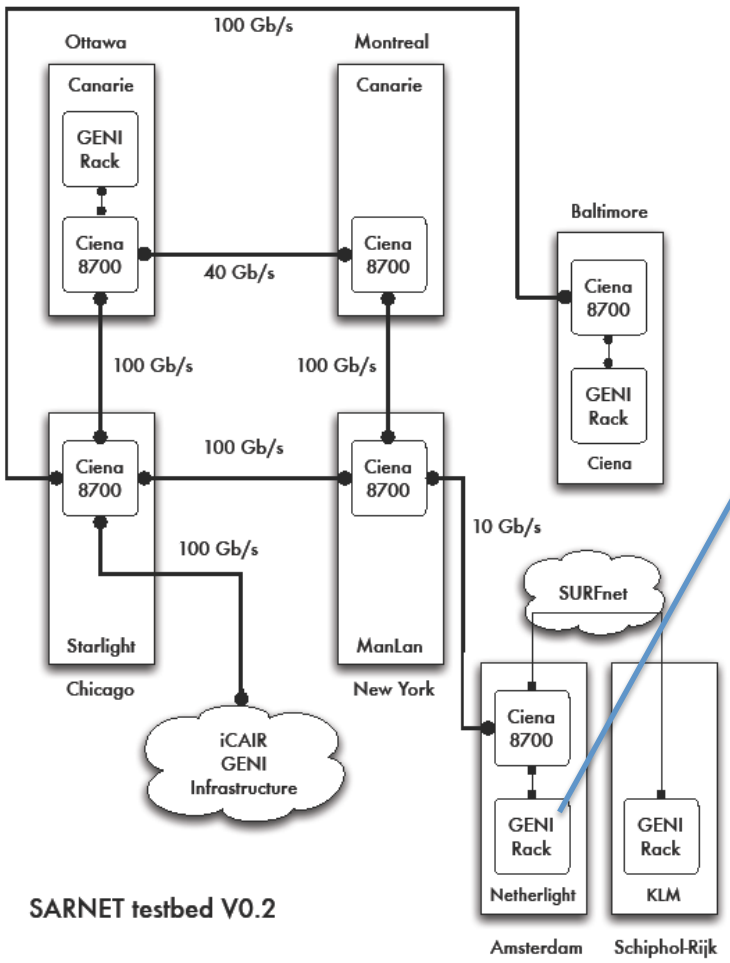


See Chapter 5 of PhD Thesis “Multi-domain authorization for e-Infrastructures” http://dare.uva.nl/record/1/432647 ISBN 9789491602269

Service Provider Group Characteristics

- Autonomous members acting together on a decision to provide a service none could provide on its own
- Appears as a single provider to a customer
- Appears as a collaborative group to members with standards, rules and policies that are defined, administered, enforced and judged by the group.
- Autonomy in the group: every member signs an agreement declaring compliance with common rules, unless local law determines otherwise.
- Membership rules organizes trust amongst members and manage group reputation and viability.

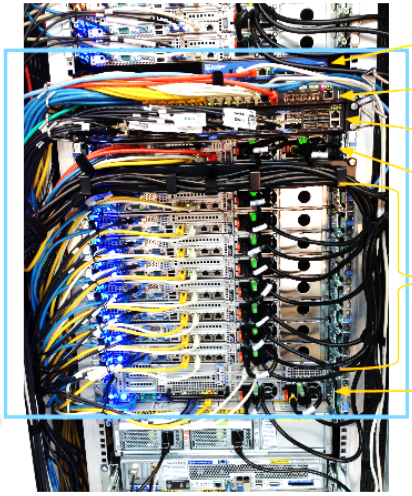
Testbed



SARNET testbed V0.2

Optical Connections are provided by Canarie, Internet2 and SURFnet

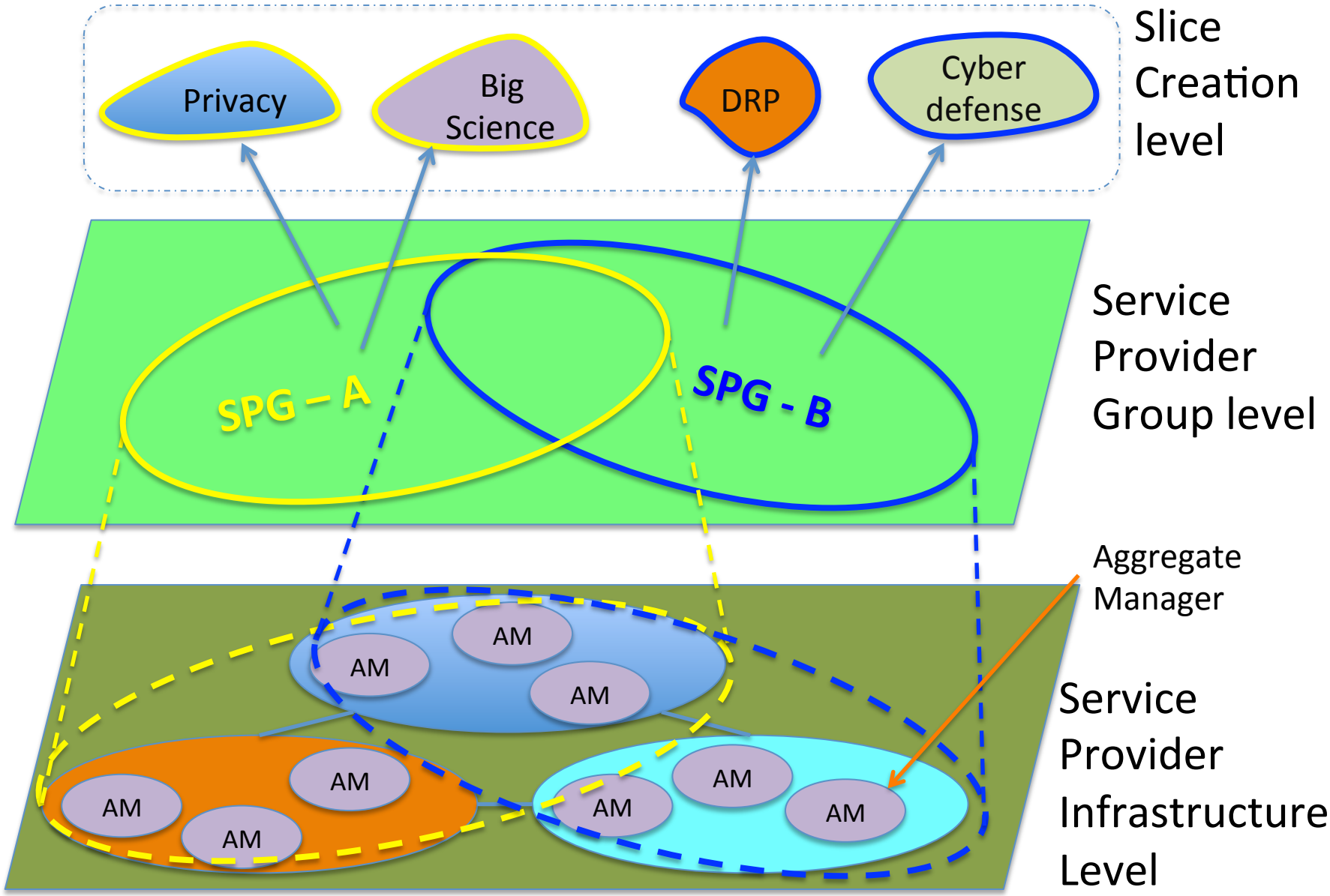
The SNE ExoGENI Rack



UNIVERSITY OF AMSTERDAM

GENI Racks serve as programmable routers, security state monitors, firewalls, security app, honeypots, SDX, etc..

Envisioned role of the SPG: define slice archetypes?



Research Questions

- SARNET:
  - Is a cyber security alliance, allowing networks to join/leave freely, feasible?
  - What is needed to organize an alliance, considering the SPG concept?
- Considering future networking concepts:
  - Is a SPG a concept that should identify and arrange slice archetypes e.g. defining cyber-security assurance levels
  - What concerns should the SPG address (e.g. economical-, legal-, administrative-, etc. slice ownerships)?

Collaboration welcomed: delaat@uva.nl