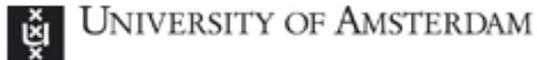


Creating a SARNET Alliance

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

Ameneh Deljoo

January 14th 2016



Ameneh Deljoo: a.deljoo@uva.nl

Leon Gommans: l.gommans@uva.nl; Tom van Engers:

t.m.engers@uva.nl,

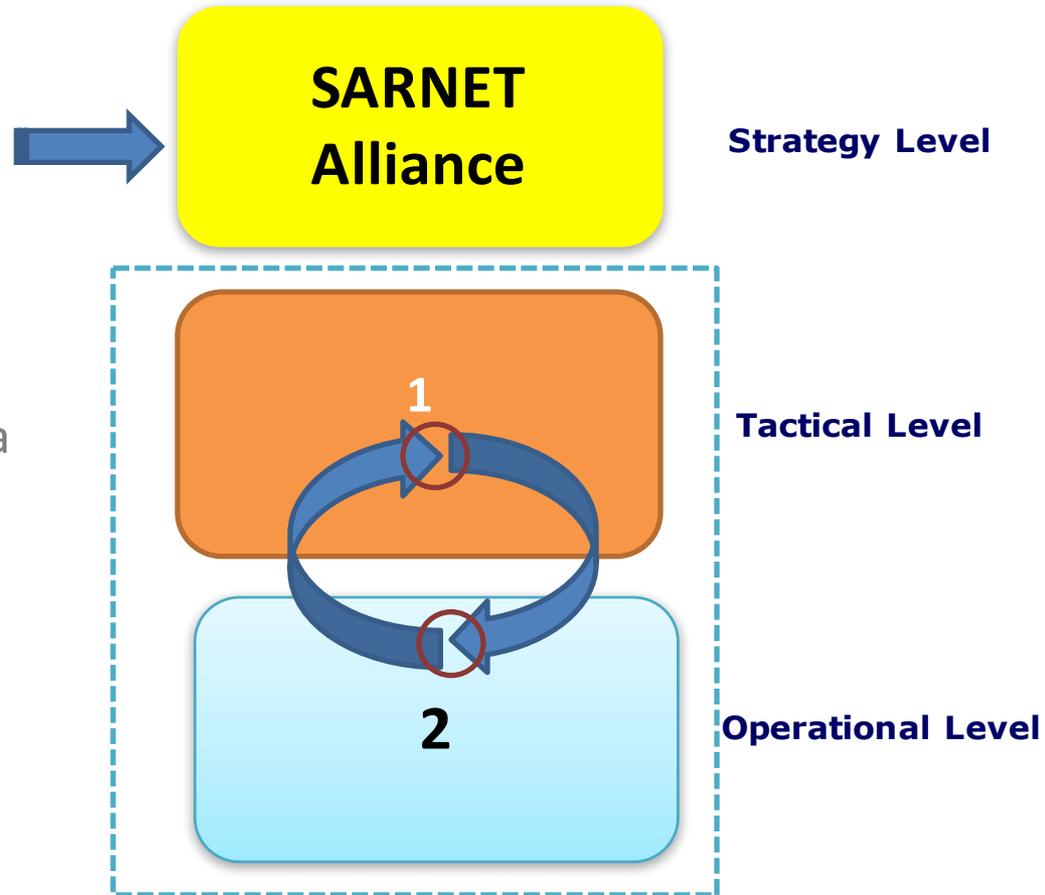
Cees de Laat: delaat@uva.nl

Content

- Introduction to SARNET
- **S**ecurity **A**utonomous **R**esponse **NET**work Alliance research
- **S**ervice **P**rovider **G**roup framework
- Modeling a SARNET Alliance using Agent Based Modeling
(first steps).

Security Autonomous Response NETWORK Research

- **Ameneh Deljoo:** Why we need SARNET Alliances? Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders
- **Stojan Trajanovski :** 1. Design functionalities needed to operate a SARNET using SDN/NFV 2. deliver security state and KPI information (e.g. cost)
- **Ralph Koning:** Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state and KPI information (2).



Cyber Security readiness



Secure
Transport

Alliance

Detect &
Filter

Protective
Perimeters

Creating a SARNET Alliance
Sharing intelligence and defensive power

SARNET

SARNET

Security state / defense tactics
automation

Topology dynamics

SARNET Alliance research

Why: Understand the **value of collaboration** between alliance members in terms of **risk reduction** increasing trust, **cost benefit and revenue impact**.

What: Provide **a-priori insight** into the **rationale of creating an alliance**.

How: Use the **Service Provider Group Framework*** to institutionalize **trust** by arranging common **rules**, its **execution** (administration & enforcement) and **judgement**.

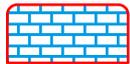
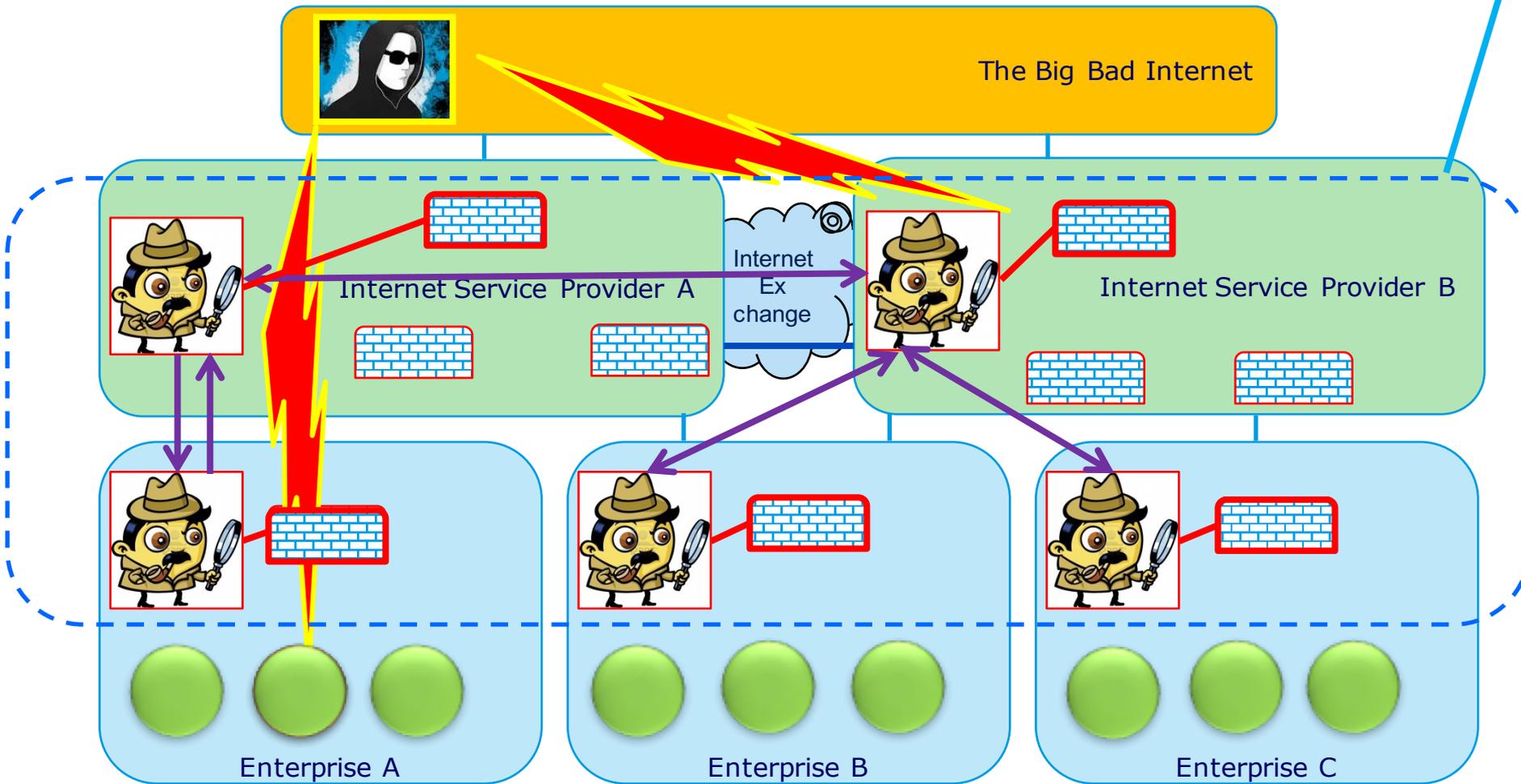
With what: A **distributed computational model** of an alliance that analyses the **policies** each autonomous member constructs from the common set of **rules**.

Result: The models can become base of an **Information Security Management System** that establishes, reviews, maintains and improves information security amongst alliance members.

* Leon Gommans, John Vollbrecht, Betty Gommans-de Bruijn, Cees de Laat, **The Service Provider Group framework A framework for arranging trust and power to facilitate authorization of network services**, Future Generation Computer Systems 45 (2015) pg 176–192

SARNET Alliance concept

SARNET Alliance research using Service Provider Group concept



SARNET research



Testbed provided by **ciena** using **geni** technology

Exploring Networks of the Future

Creating an Alliance via bi-lateral agreements

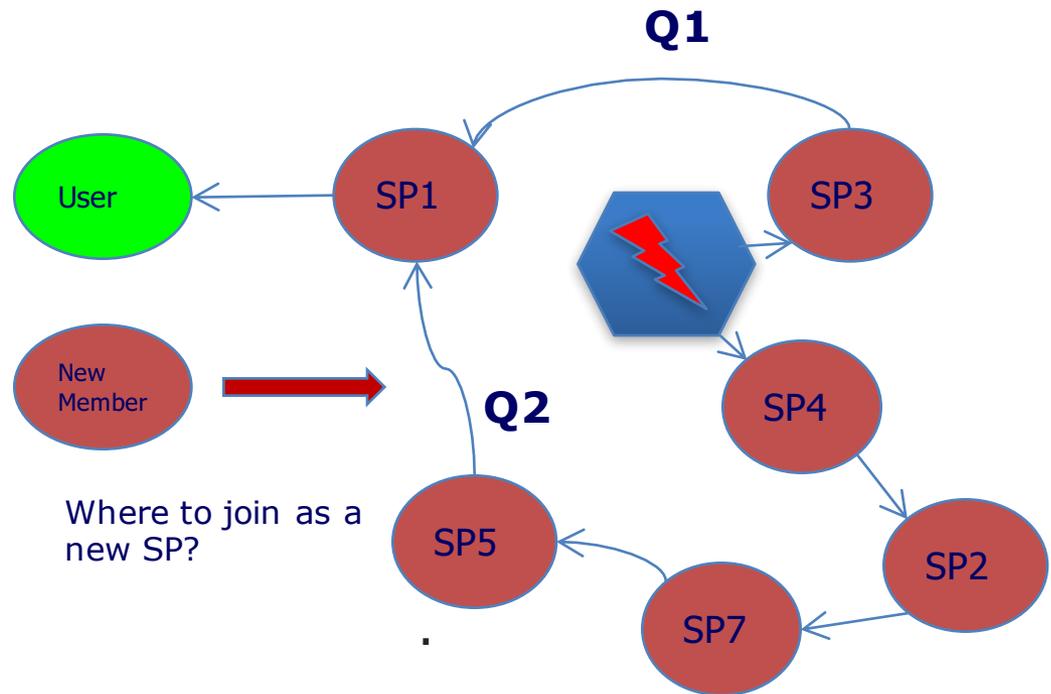
SP3 and SP5 (via SP7, SP2 and SP4) may deliver the same security intelligence to SP1.

Delivery of intelligence will most likely be at different quality (e.g. considering the speed of detection).

A user, expecting consistency, may be unaware of the difference in quality SP1 decides to select.

How should a new SP member join this alliance?

How does each member benefit from sharing intelligence or offering defence?



Problems with mutual Collaborations

- Trust
 - Will others leak my data?
- Legal Liability
 - Will I be sued for sharing customer data? Will others find me negligible?
- Competitive concerns
 - Will my competitors outperform me?
- Shared data quality
 - Will data be reliable?

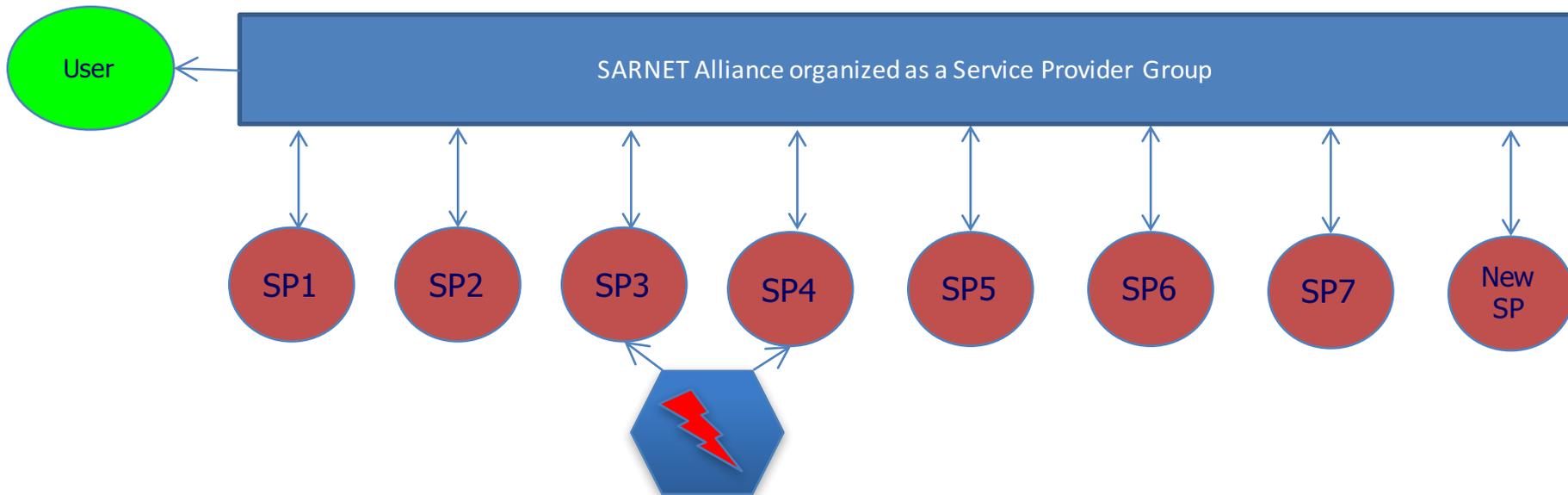
Service Provider Group Examples

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

Examples:



Establishing an Alliance as a Service Provider Group



- The user signs an agreement with the SPG (may use one of the SP's as proxy).
- The SPG arranges uniform delivery quality to a user
- SPG provides common rules for new members, creating trust between members.
- SPG may enforce service quality of each member
- SPG may act as an exchange for security services
- SPG may clear & settle value exchanges between members for services provided/used

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.

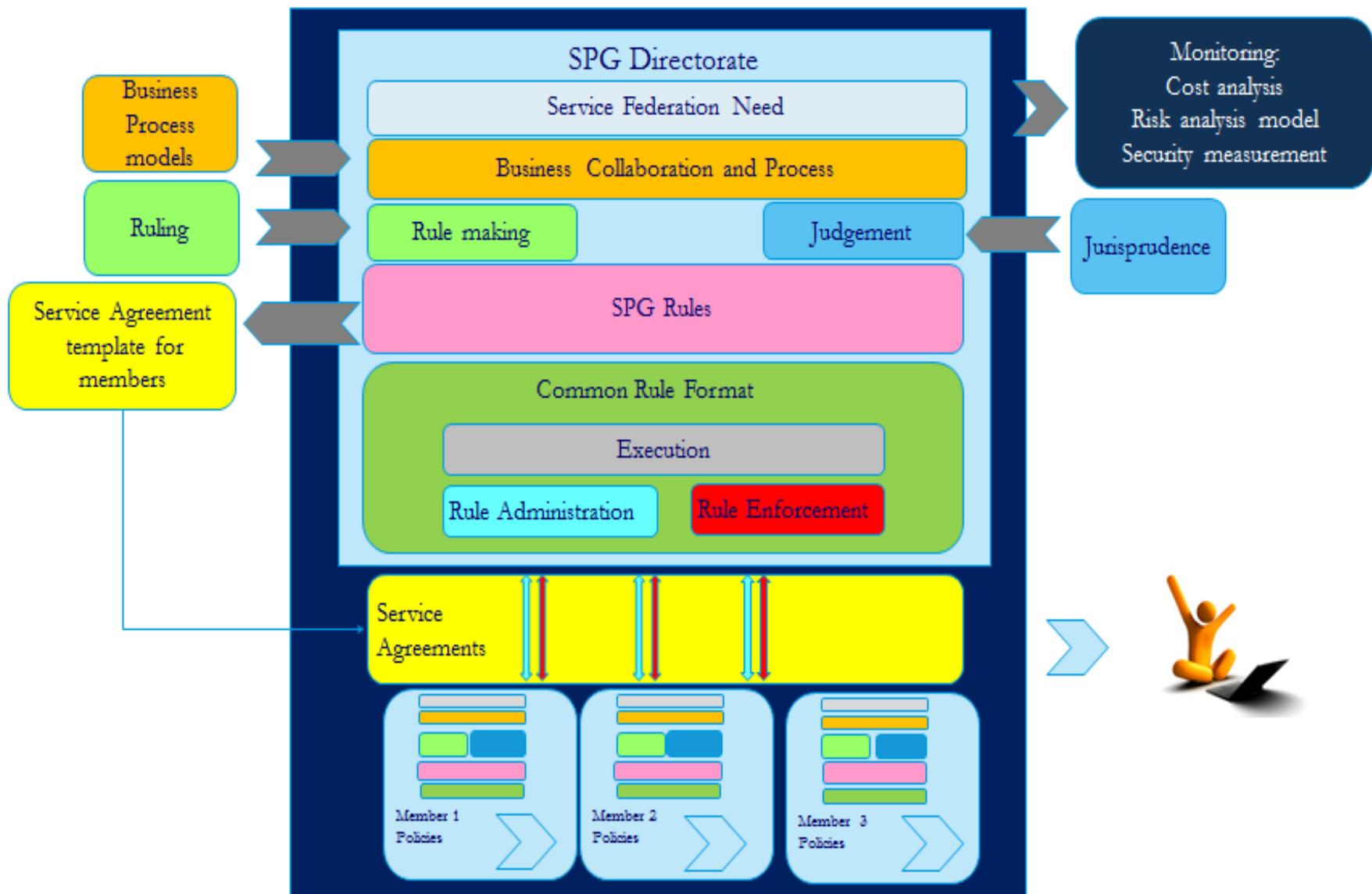
Service Provider Group behaviour

Our next step

Understand the value of collaboration by

- Applying Agent Role Modelling in multi-domain scenario's
 - Agents are self governed autonomous entities that pursue their own individual goals based only on their own beliefs and capabilities (Abdelkader, 2003).
- Modelling Normative and Institutional context
 - Inter-agent description
 - Message Sequence Diagram
 - Topology
 - Identify an intentional/institutional factors
- Create executable model to research how policies, applied by each autonomous member and common regulation affects **trust in the group** and **member cost & benefits.**

Service Provider Group

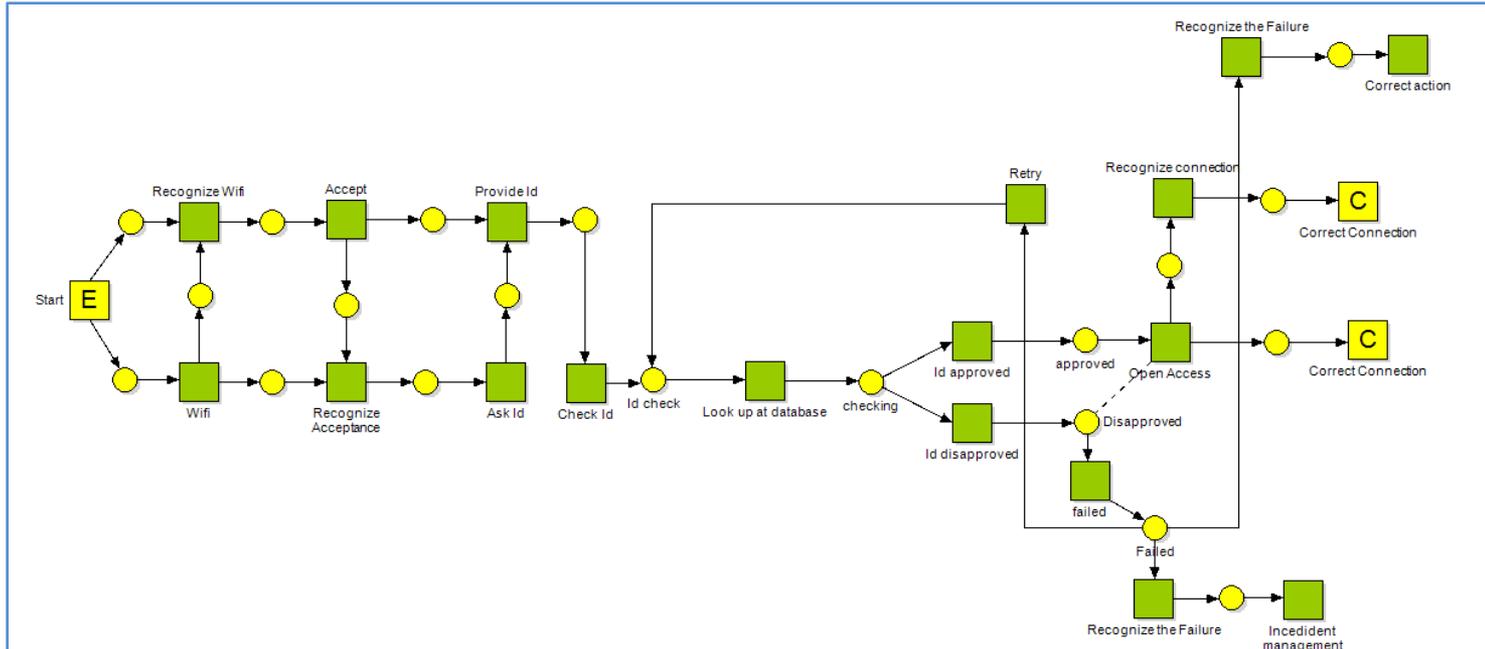


Modelling Framework

Main component	
Signal layer	Message / Act
Action layer	Action / Activity
Intentional layer	Intention
Motivational layer	Motive

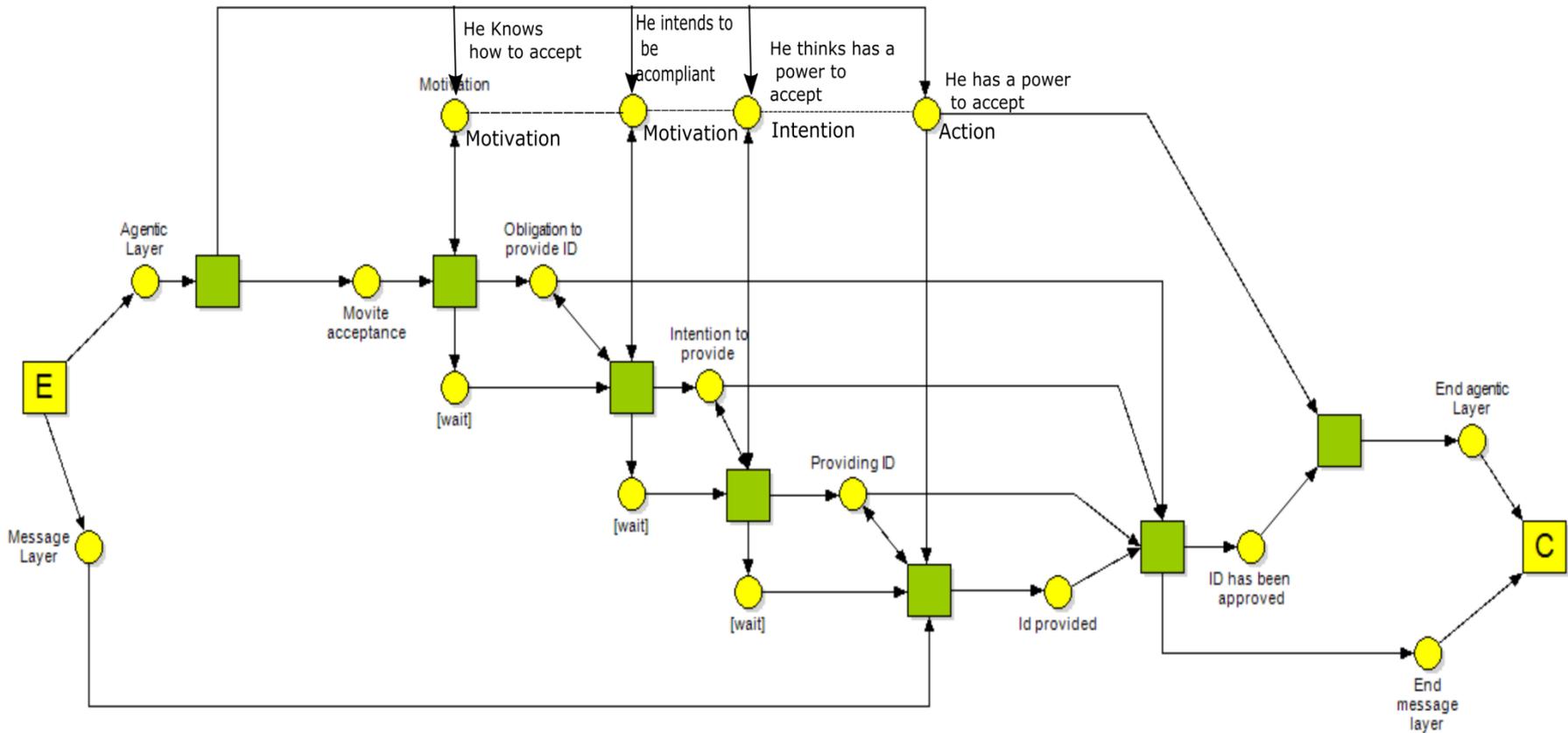
In our model, we refer to four layers of components:

- the signal layer—**acts**, side-effects and failures (e.g. technical failure, user abuse): outcomes of actions,
- the action layer—**actions** (or activities): performances intended to bring about a certain result,
- the intentional layer—**intentions**: commitments to actions, or to build up intentions,
- the motivational—**motives**: events triggering the creation of intentions.



Petri net of EduRoam Case

Intention, Motivation and Action



Petri net of EduRoam Case