Policy Auditing in Data Exchange Systems

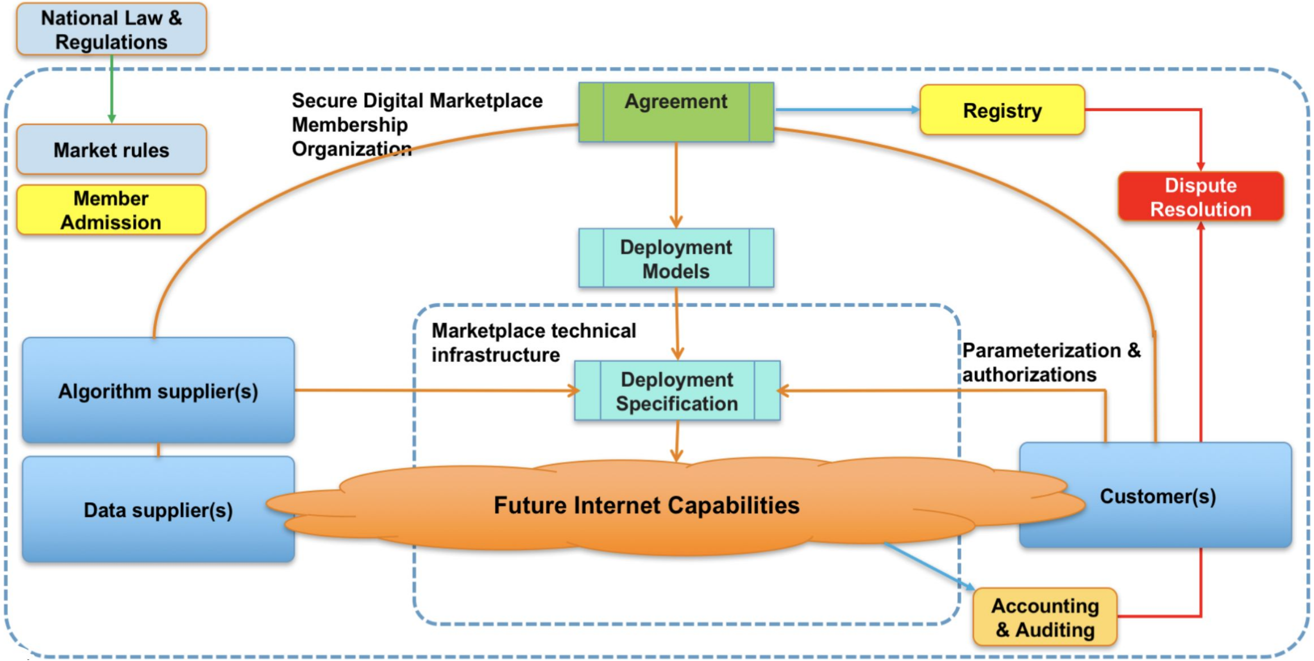
Speakers: Paola Grosso, Xin Zhou, Reggie Cushing

Co-authors: Ralph Koning, Adam Belloum, Sander Klous, Tom van Engers, Cees de Laat

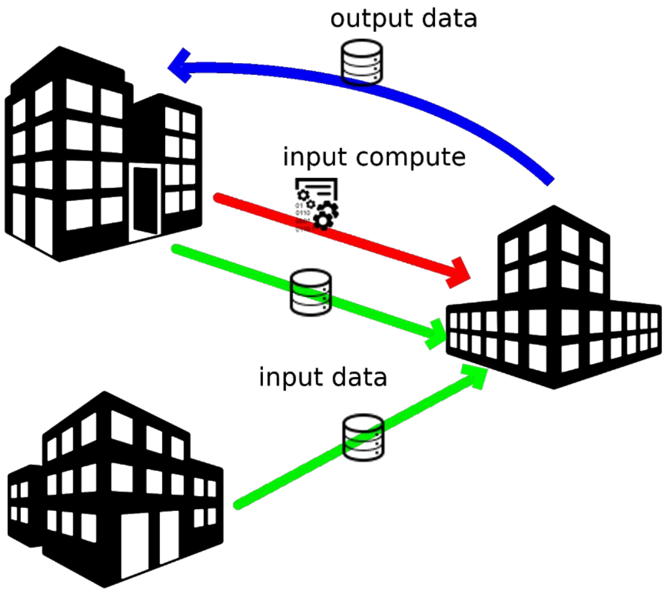
XNet 2020

Systems and Networking Laboratory

DL4LD


National Law & Regulations
Market rules
Member Admission
Secure Digital Marketplace Membership Organization
Agreement
Registry
Dispute Resolution
Deployment Models
Marketplace technical infrastructure
Deployment Specification
Parameterization & authorizations
Algorithm supplier(s)
Data supplier(s)
Future Internet Capabilities
Customer(s)
Accounting & Auditing

General motivation

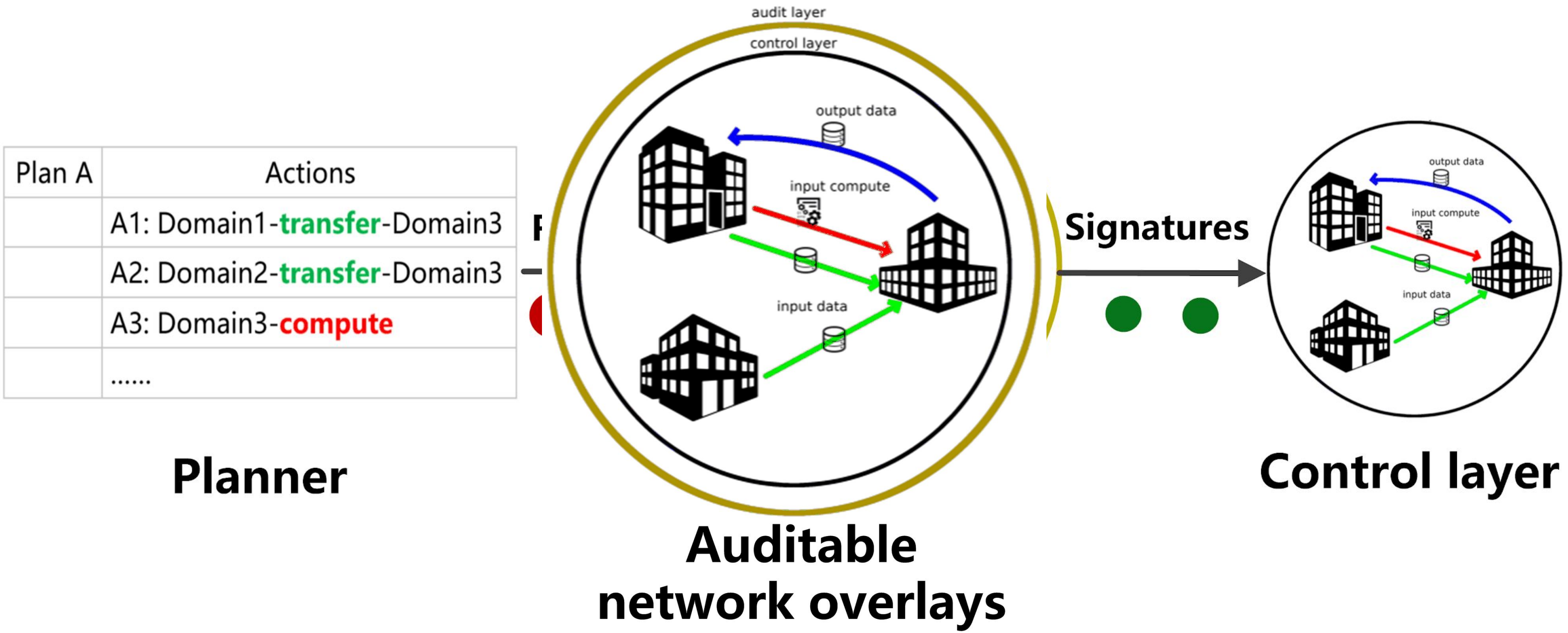


- Competing companies can, together, generate value from collaborating on data and compute. Examples include airlines industry, ports, healthcare.
- Clearly this poses a challenge of how to facilitate such collaborations through technology. Here we focus on the policy enforcement aspect of a multi-domain infrastructure.

Challenges

- **Multi-domain Policy Enforcement and Monitoring**
  - How to evaluate if operations on data are adhere to the policy?
  - How to ensure only compliant operations being executed?
- Multi-domain Identity and Trust Management
  - How to manage identities for the different components in a multi-domain system?
  - How to leverage and identity system to maintain trust between components?
- Multi-domain Application Workflows
  - How to define distributed applications running in a multi-domain environment?
  - How to coordinate resources and schedule applications?
- Multi-domain Collaborative Infrastructure
  - How to address components in a multi-domain infrastructure?
  - How to communicate securely?

A brief review of former work

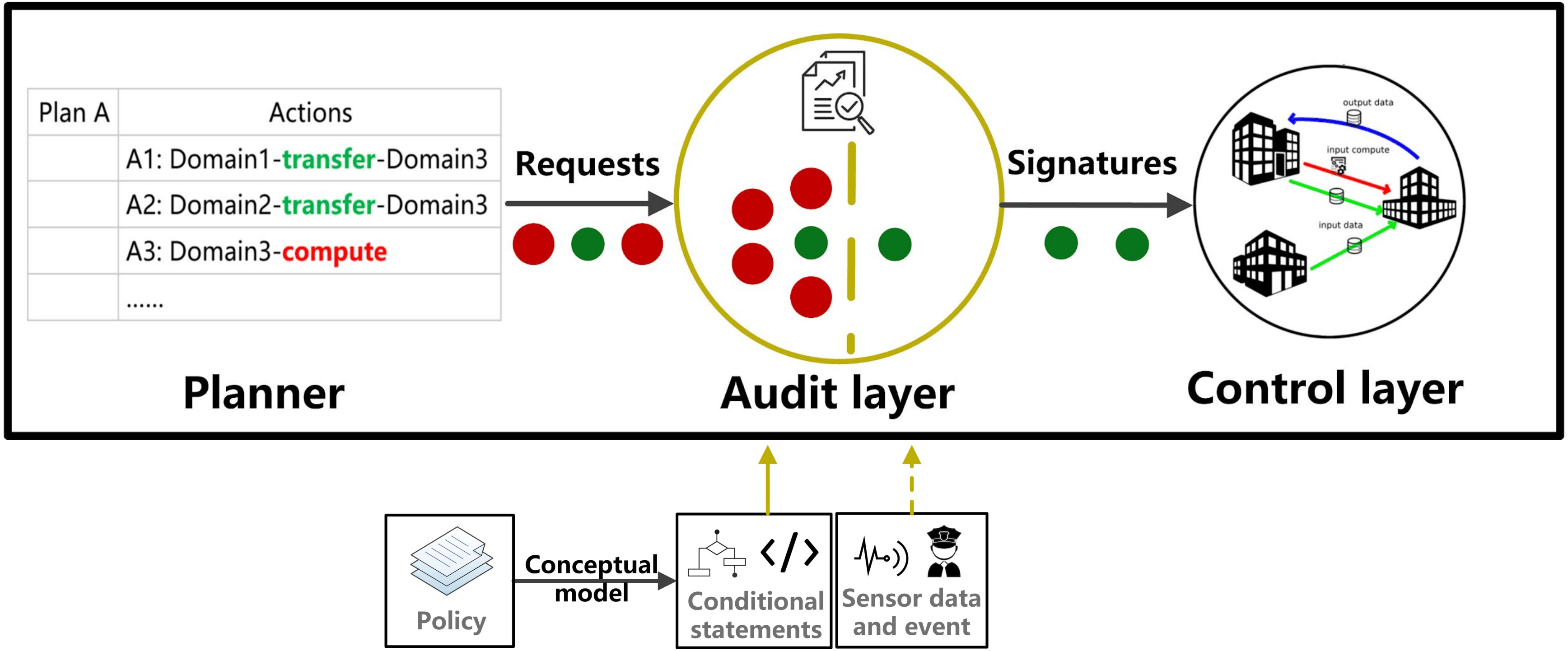


Plan A	Actions
	A1: Domain1-**transfer**-Domain3
	A2: Domain2-**transfer**-Domain3
	A3: Domain3-**compute**
	……

[1] Cushing R, Koning R, Zhang L, et al. Auditable secure network overlays for multi-domain distributed applications[C] 2020 IFIP Networking Conference (Networking). IEEE, 2020: 658-660.

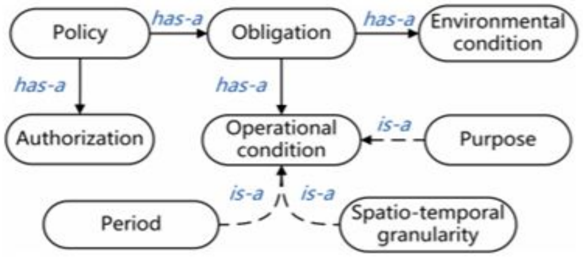
Extension on the audit layer

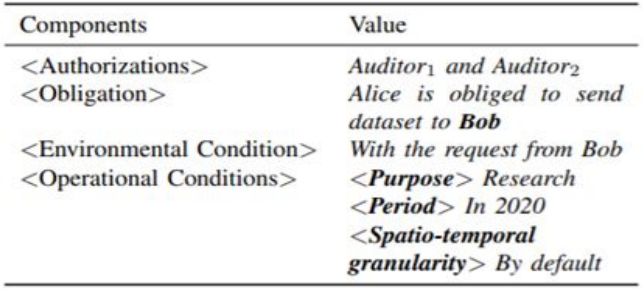
Auditable network overlays



Plan A	Actions
	A1: Domain1-transfer-Domain3
	A2: Domain2-transfer-Domain3
	A3: Domain3-compute
	……

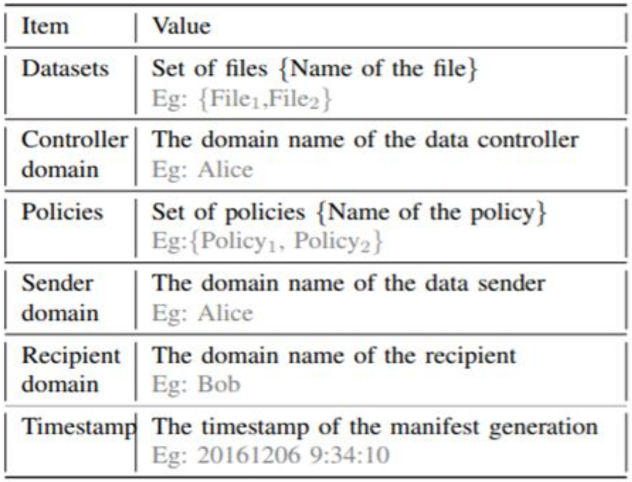
Conceptual model





Components	Value
<Authorizations>	*Auditor$_1$ and Auditor$_2$*
<Obligation>	*Alice is obliged to send dataset to* ***Bob***
<Environmental Condition>	*With the request from Bob*
<Operational Conditions>	*<**Purpose**> Research* *<**Period**> In 2020* *<**Spatio-temporal granularity**> By default*

Policy component



Item	Value
Datasets	Set of files {Name of the file} Eg: {File$_1$,File$_2$}
Controller domain	The domain name of the data controller Eg: Alice
Policies	Set of policies {Name of the policy} Eg:{Policy$_1$, Policy$_2$}
Sender domain	The domain name of the data sender Eg: Alice
Recipient domain	The domain name of the recipient Eg: Bob
Timestamp	The timestamp of the manifest generation Eg: 20161206 9:34:10

TABLE I
MANIFEST: METADATA OF DATASETS/FILES

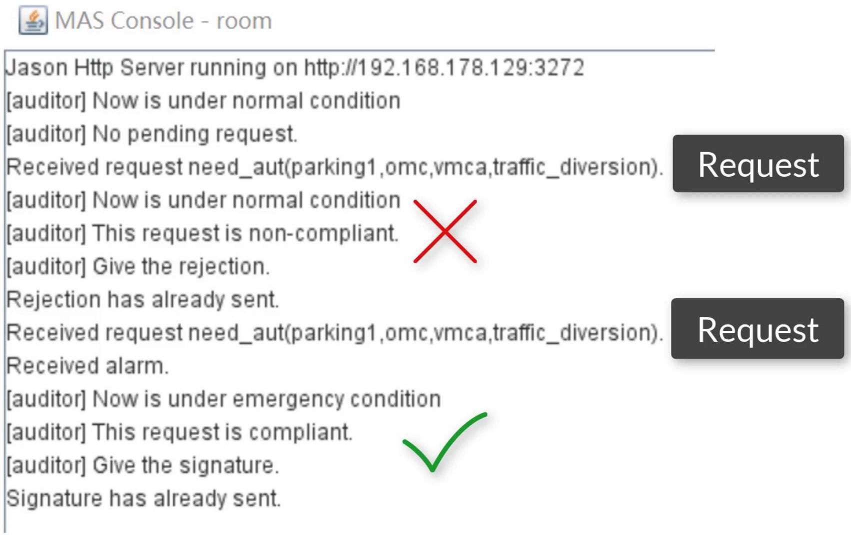
Manifest

Jason

- One of the most solid development environments for a belief-desire-intention (BDI)
    - **Belief**: policy, environment condition
    - **Desire**: audit, send signatures/rejection
    - **Intention**: the executed desires

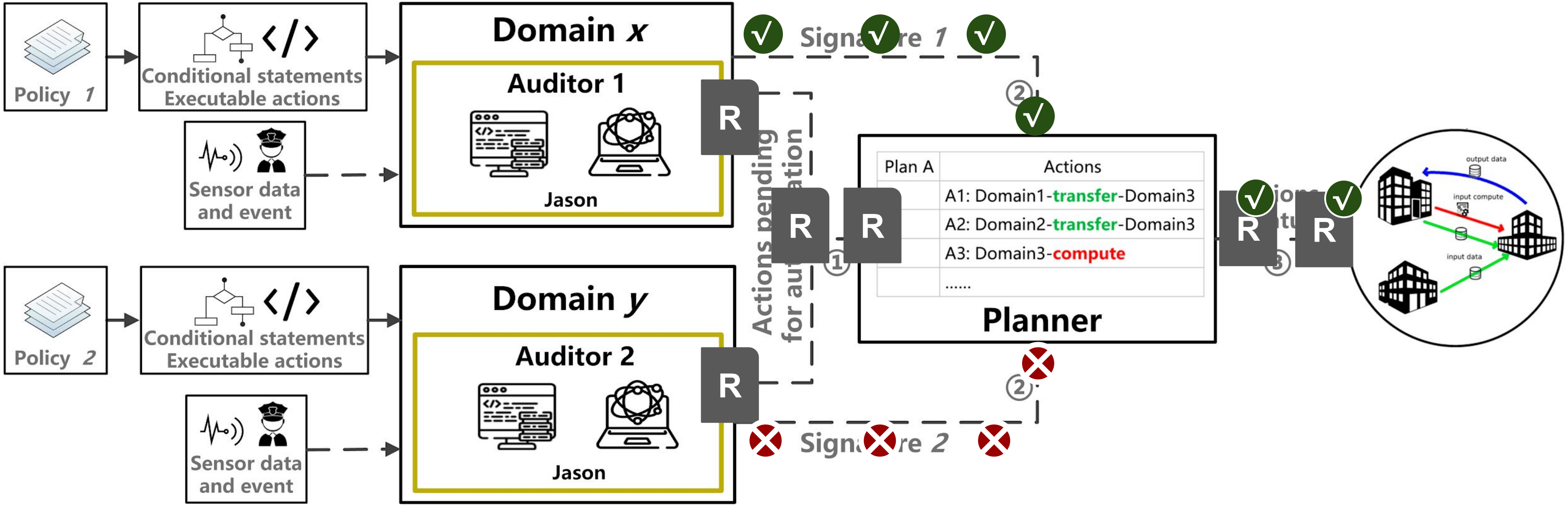
Jason

- Features
  - Auditors need to be **responsive** to requests and environment
  - Auditors need be able to reason, judge, and output **autonomously**



```
Jason Http Server running on http://192.168.178.129:3272
[auditor] Now is under normal condition
[auditor] No pending request.
Received request need_aut(parking1,omc,vmca,traffic_diversion).
[auditor] Now is under normal condition
[auditor] This request is non-compliant.
[auditor] Give the rejection.
Rejection has already sent.
Received request need_aut(parking1,omc,vmca,traffic_diversion).
Received alarm.
[auditor] Now is under emergency condition
[auditor] This request is compliant.
[auditor] Give the signature.
Signature has already sent.
```

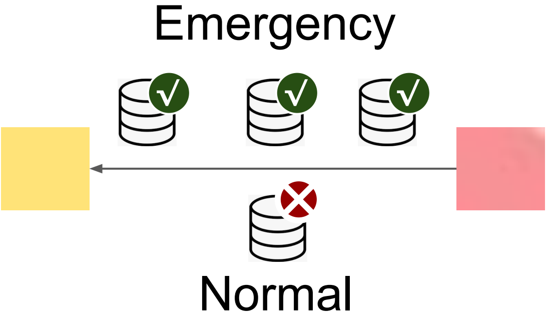
Authorization flow of the auditable network overlays



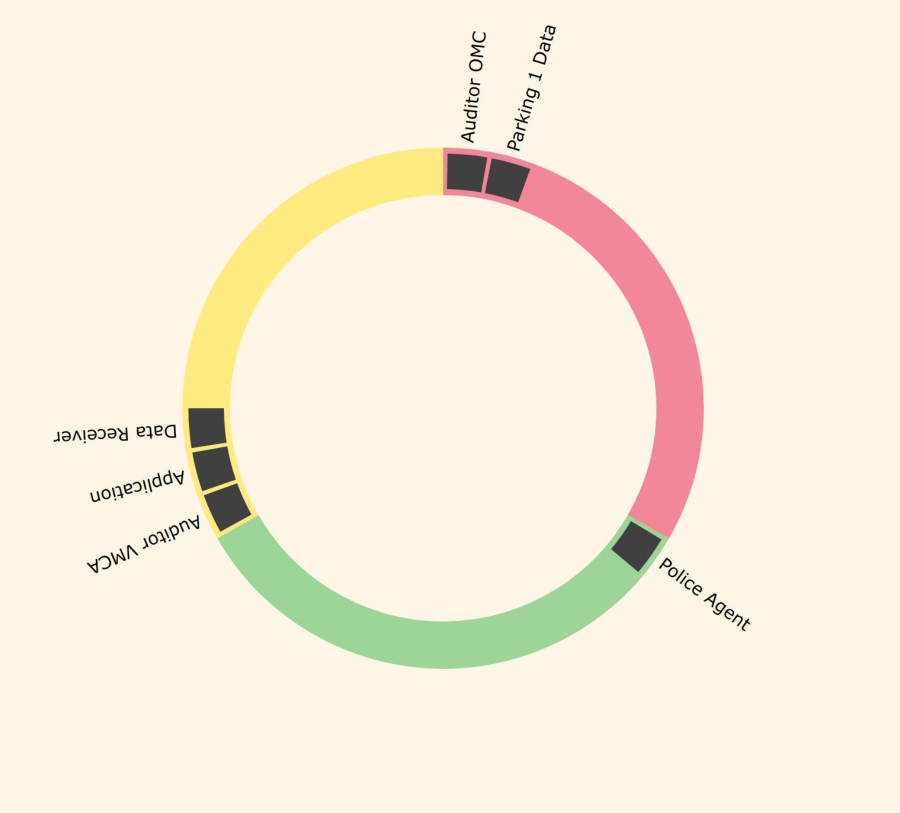
Plan A	Actions
	A1: Domain1-transfer-Domain3
	A2: Domain2-transfer-Domain3
	A3: Domain3-compute
	......

ArenA case context

- During the outflow of 7000 visitors, a fatal accident happened at a pedestrian when someone fell down from it.
- The traffic department VMCA needed parking lot data of ArenA Operational Mobility Center(OMC) to divert traffic
- **Policy enforcement**

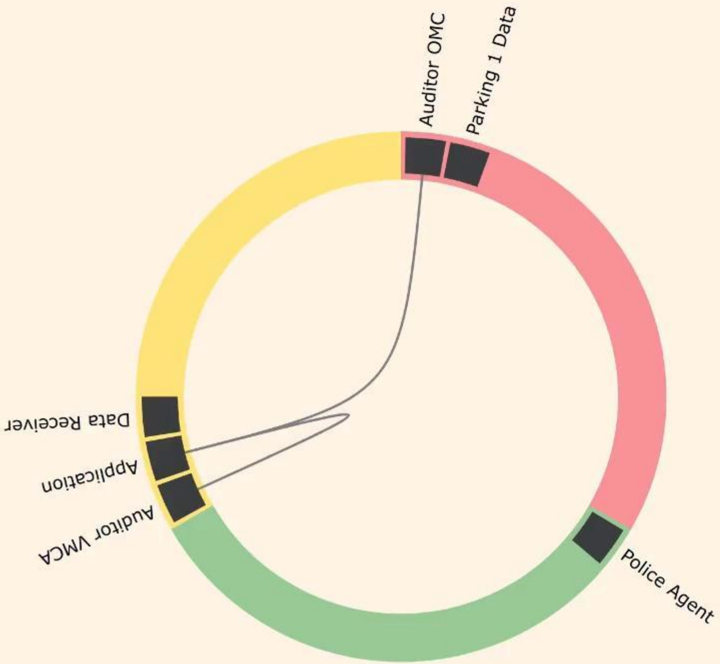


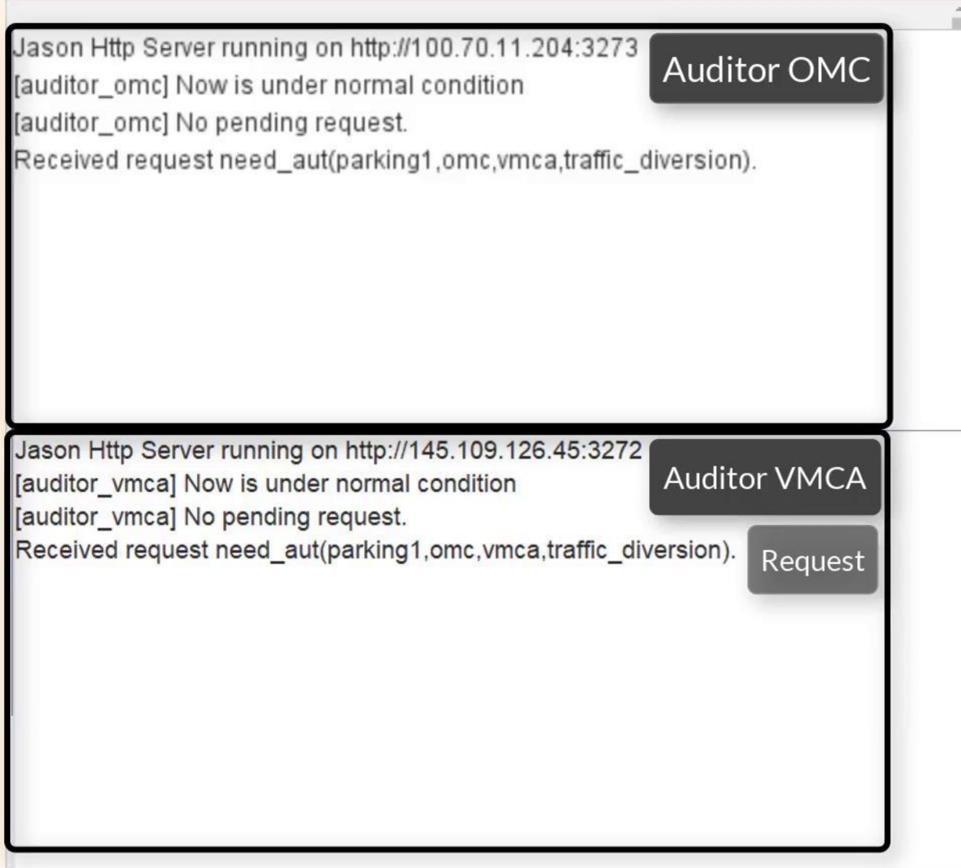
Intro to the demo



- Multi-domain overlay network
  - Signaling over message queue
- 3 domains
  - OMC (Stadium)
  - VMCA (Traffic)
  - Police (Authority)
- 6 Actors
  - 2 Auditors
  - 1 Application
  - 1 Sensor (Police Agent)
  - 1 Data sender
  - 1 Data receiver
- 2 Scenarios
  - **Normal condition** ✗
  - **Emergency condition** ✓

Scenario 1





```
Jason Http Server running on http://100.70.11.204:3273
[auditor_omc] Now is under normal condition
[auditor_omc] No pending request.
Received request need_aut(parking1,omc,vmca,traffic_diversion).
```

```
Jason Http Server running on http://145.109.126.45:3272
[auditor_vmca] Now is under normal condition
[auditor_vmca] No pending request.
Received request need_aut(parking1,omc,vmca,traffic_diversion).
```

Conclusions

- In a multi-domain scenario, auditing, authorization and access are not straight forward
    - Each domain is independent and has its own policies
    - Applications need to coordinate between multiple policies
- Future work
    - Cater for more complex policies such as the notion of obligation
    - Integrate further into SC19 demo
    - Secure compute

Questions?

- SC19 demo
    - http://shorturl.at/ijnuE
- More information at the project's website
    - https://www.dl4ld.net
    - https://dl4ld.nl
- More information on the data sharing research
    - https://mns-research.nl
    - https://cci-research.nl
- Demo based on paper

Xin Zhou, Reggie Cushing, Ralph Koning, Adam Belloum, Paola Grosso, Sander Klous, Tom van Engers, Cees de Laat, "**Policy Enforcement for Secure and Trustworthy Data Sharing in Multi-domain Infrastructures**" (The 14th IEEE International Conference on Big Data Science and Engineering, accepted）