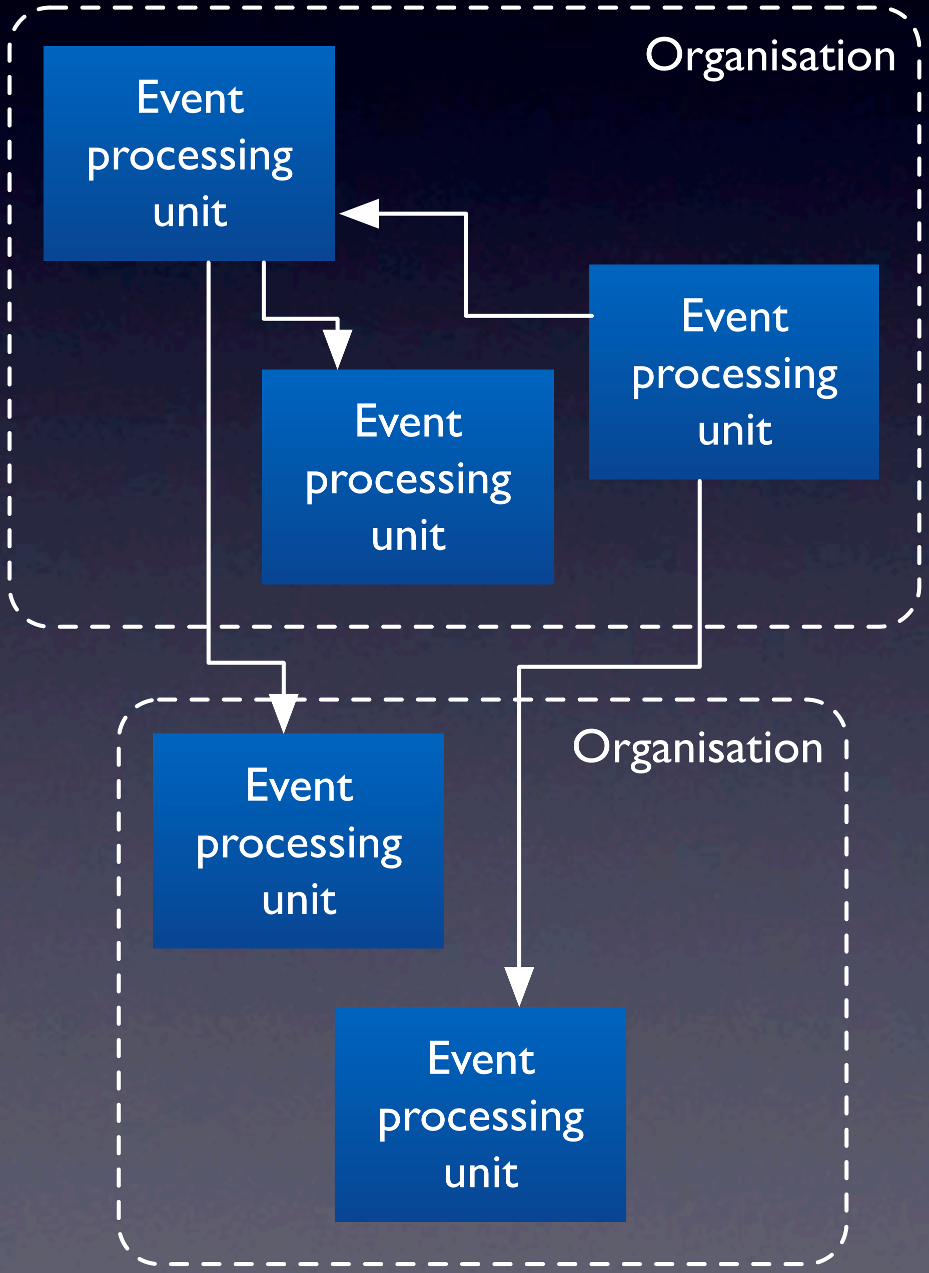
Distributed Decentralised Event Flow Control

David Evans

de239@cl.cam.ac.uk

The scene

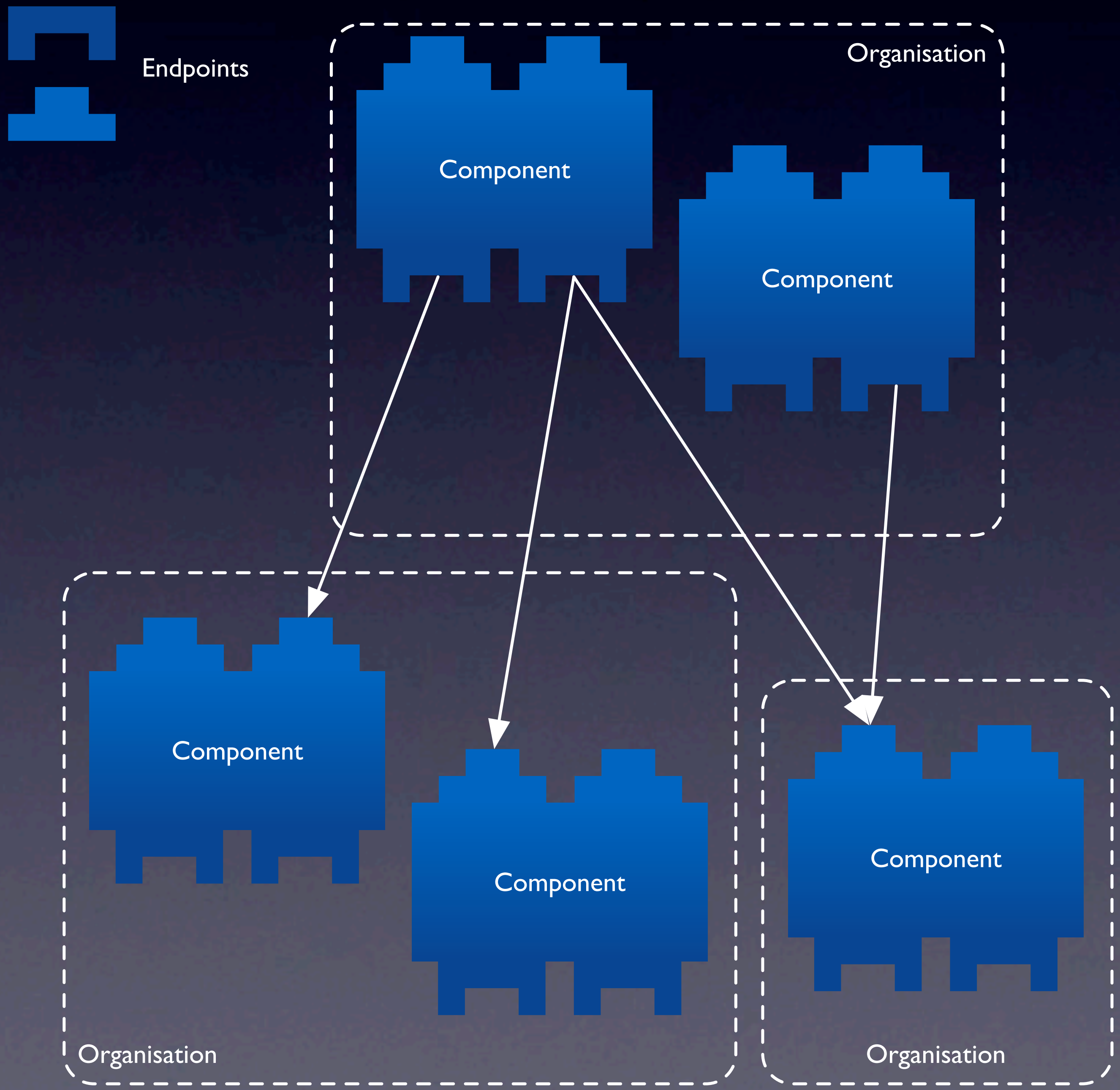
Multiple organisations exchange data



Key aspects

- Events typically contain data for multiple receivers
- There is no over-arching administrative authority
- Publishers don’t know events’ recipients
- Some recipients might be in a different organisation!

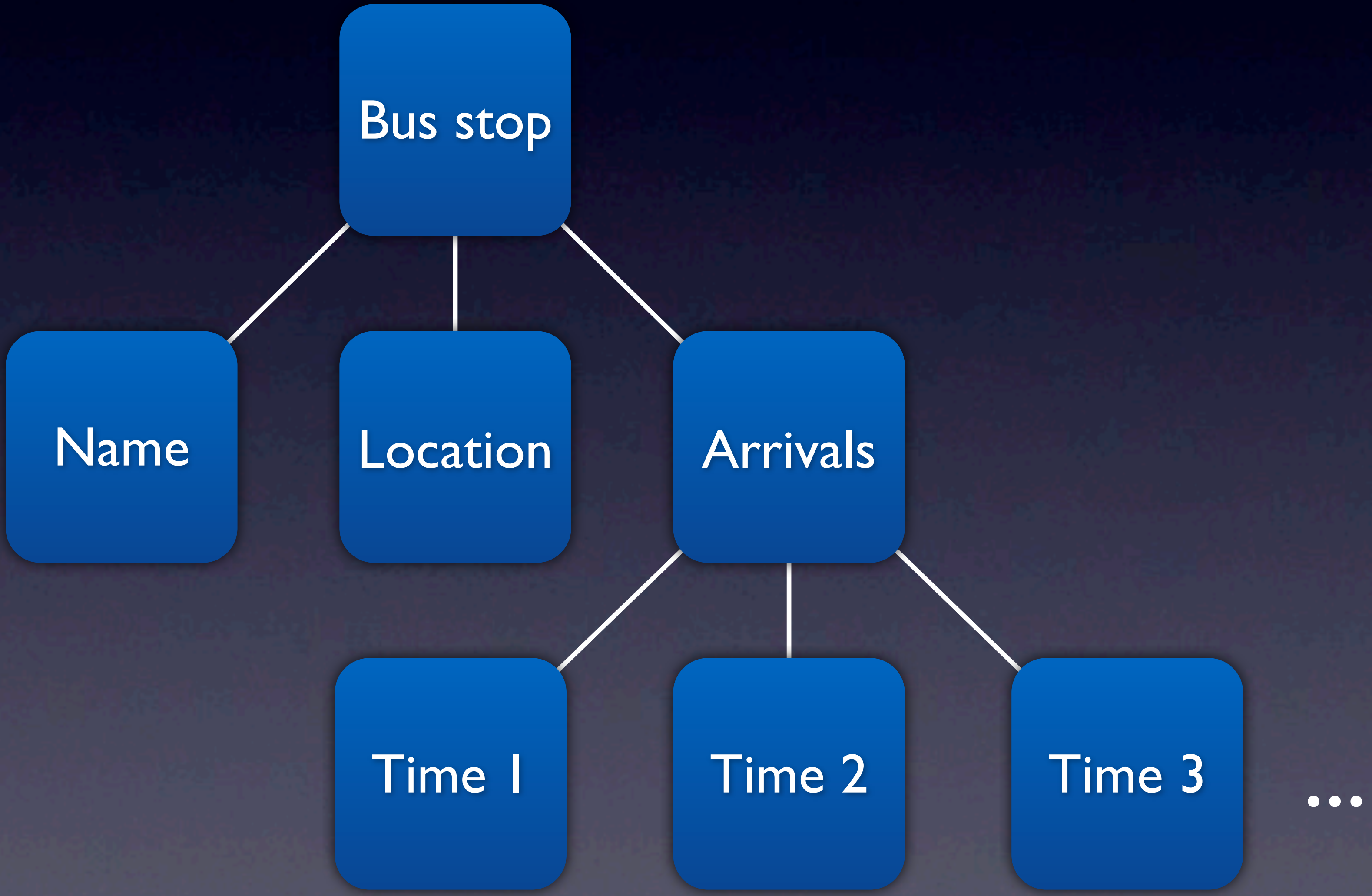
Components and endpoints (in the SBus world)



Event type system

- Each event has a type
- Events emitted or accepted by an endpoint all have the same type (the “type of the endpoint”)
- Only type-compatible endpoints can be connected

Events are trees


Bus stop

Name

Location

Arrivals

Time 1

Time 2

Time 3

...

Tags and labels

- A label has a set of *confidentiality* and *integrity* tags
- Blah blah blah...you saw this last week, remember?

Labels and nodes

- A label is assigned to each node

name	data	confidentiality tags	integrity tags
Name	data_X	$\varnothing$	$\{i_1\}$
Location	...	$\{c_1\}$	$\{i_1\}$
Arrivals	data_Y	$\{c_1, c_2\}$	$\{i_1\}$

Transporting event labels

- Labels are *not* part of the schema!

```
@tag bin

@label {
   ( confidentiality ^tag )
   ( integrity ^tag )
}

@nodelabel {
   nodename txt
   - ^label
}

labels ( - ^nodelabel )
```

Data use agreements

Deontic agreements

- Organisations form agreements describing data flow and attendant permissions and obligations (*deontic* concepts)
- Each maintains state describing the degree of compliance (the “deontic state”)
  - Events and fluents (in the Event Calculus sense)
- State affected by local concerns

From tags to agreements

Tags are local

- Per-organisation scope: get meaning by fiat
- Organisations must agree on deontic states anyway
- Map tags onto these states
- Use SBus event extraction interface to effect DEFCon-like access control

The meaning of a tag

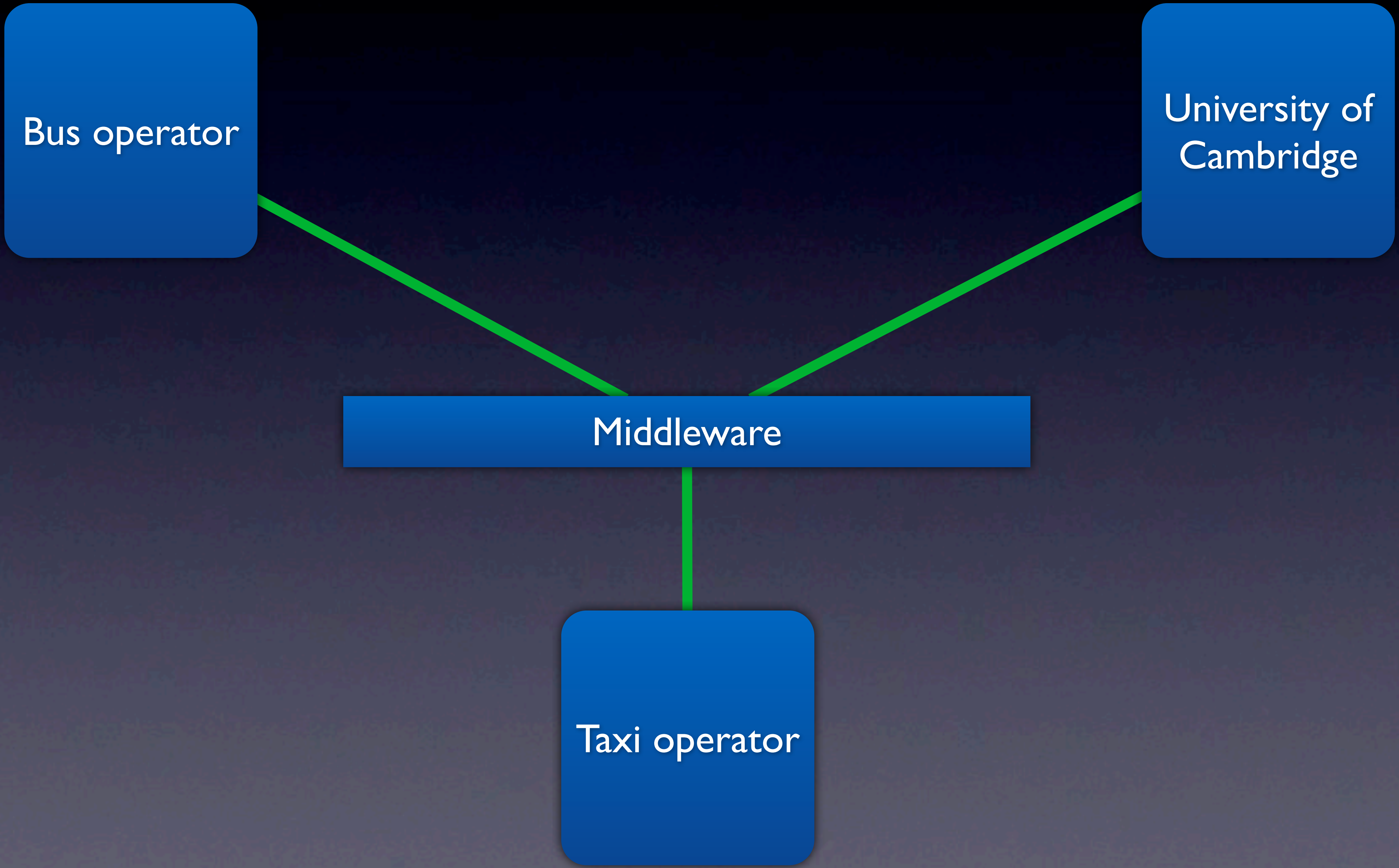
- A tag (and thus a label) has two meanings
  - It asserts that transmission of data tagged with it has a certain deontic meaning
  - The ability to assign it to data reflects the privilege of being able to effect deontic state changes in others who are party to the agreement

Agreements are expressions of trust

- An organisation trusts others to vet interaction with data according to their labels

Example

The players



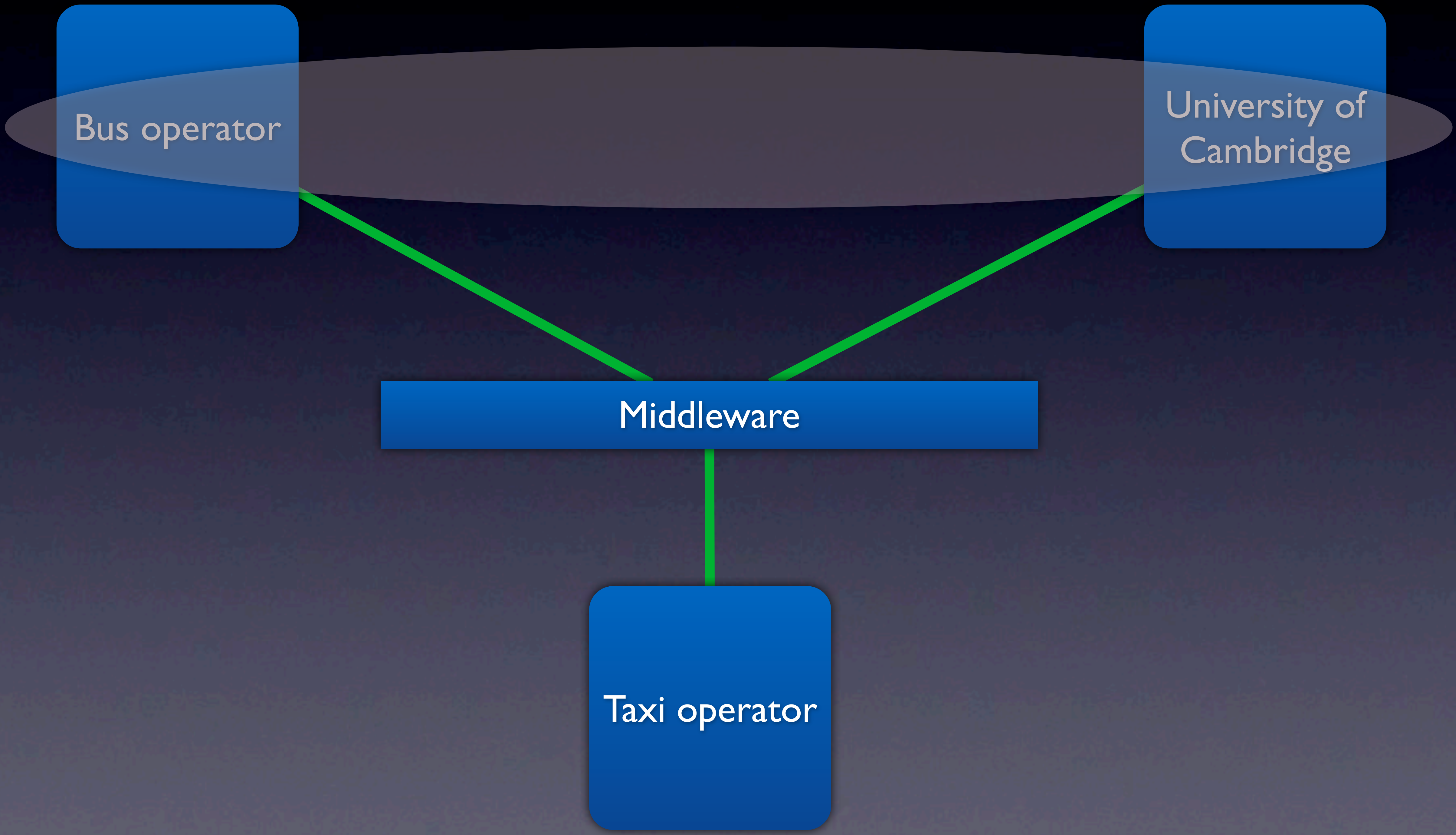
Bus operator

University of Cambridge

Middleware

Taxi operator

Agreements



Bus operator
University of Cambridge
Middleware
Taxi operator

Tags and fluents

- Tags
    - PROPRIETARY-VEHICLE-POSITION
- Fluents
    - KNOWS-BUS-LOCATION
    - BUS LOCATION
    - KNOWS-TAXI-LOCATION
    - TAXI LOCATION
    - TAXI-NEAR-BUS
    - VIOLATION-SUSPECTED

An event

```
<labels>
    <nodelabel>
    <nodename>bus</nodename>
        <label>
            <confidentiality>
                proprietary-vehicle-position
            </confidentiality>
            <integrity/>
        </label>
    </nodelabel>
</labels>
<bus>
    <name>3186</name>
    <when>17/02/2010,13:22:30</when>
    <coordinates>
        52.21138,0.102654
    </coordinates>
</bus>
```

Conclusions

Contributions

- Unified intra- and inter-organisation IFC
- Incorporation of security tag agreement into a larger, legally-backed framework
- Publishers don’t need to know whether event recipients are inside or outside their organisation

Future work

- What is the cost in terns of performance?
  - Enforcement is on the critical path
  - Efficient tag checking
- Tag allocation
  - Federated tag regestries?