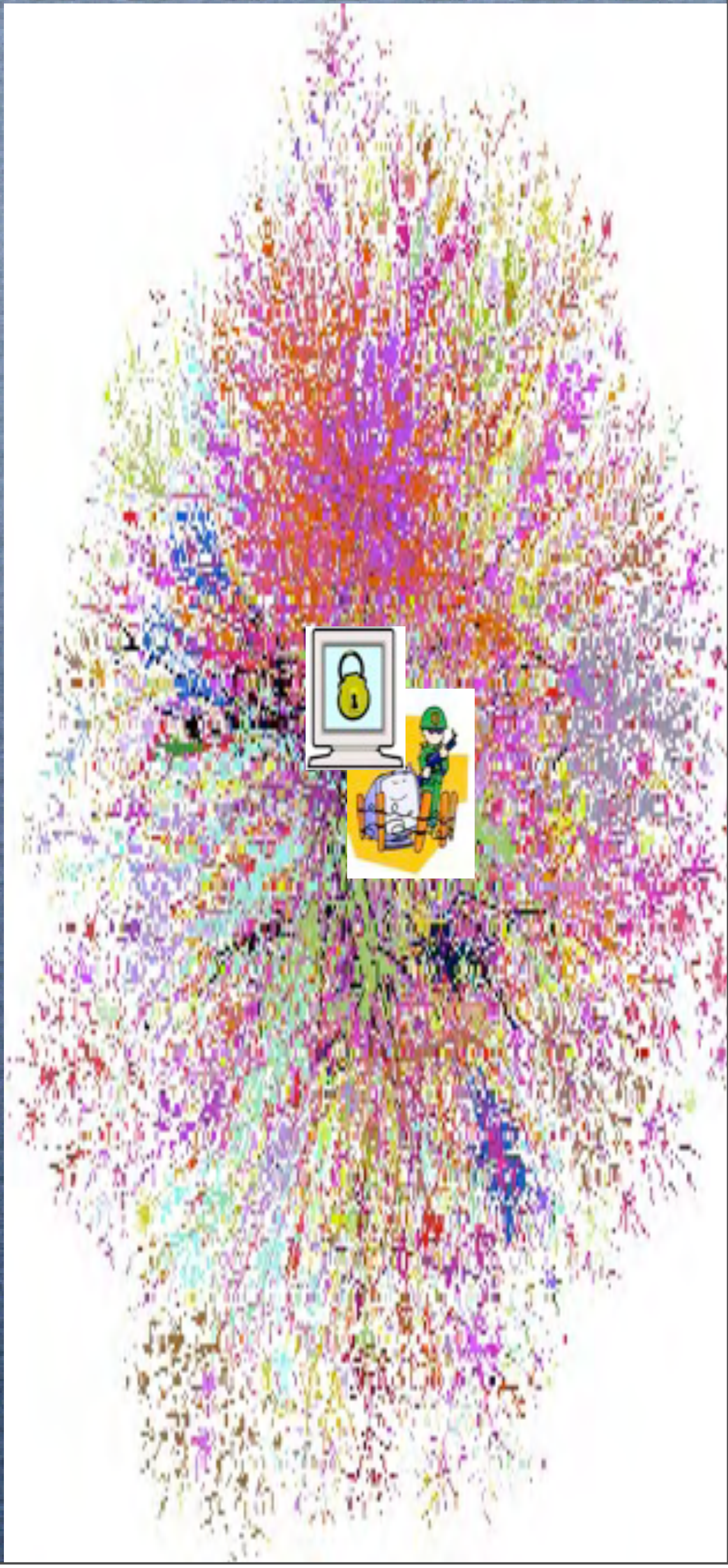
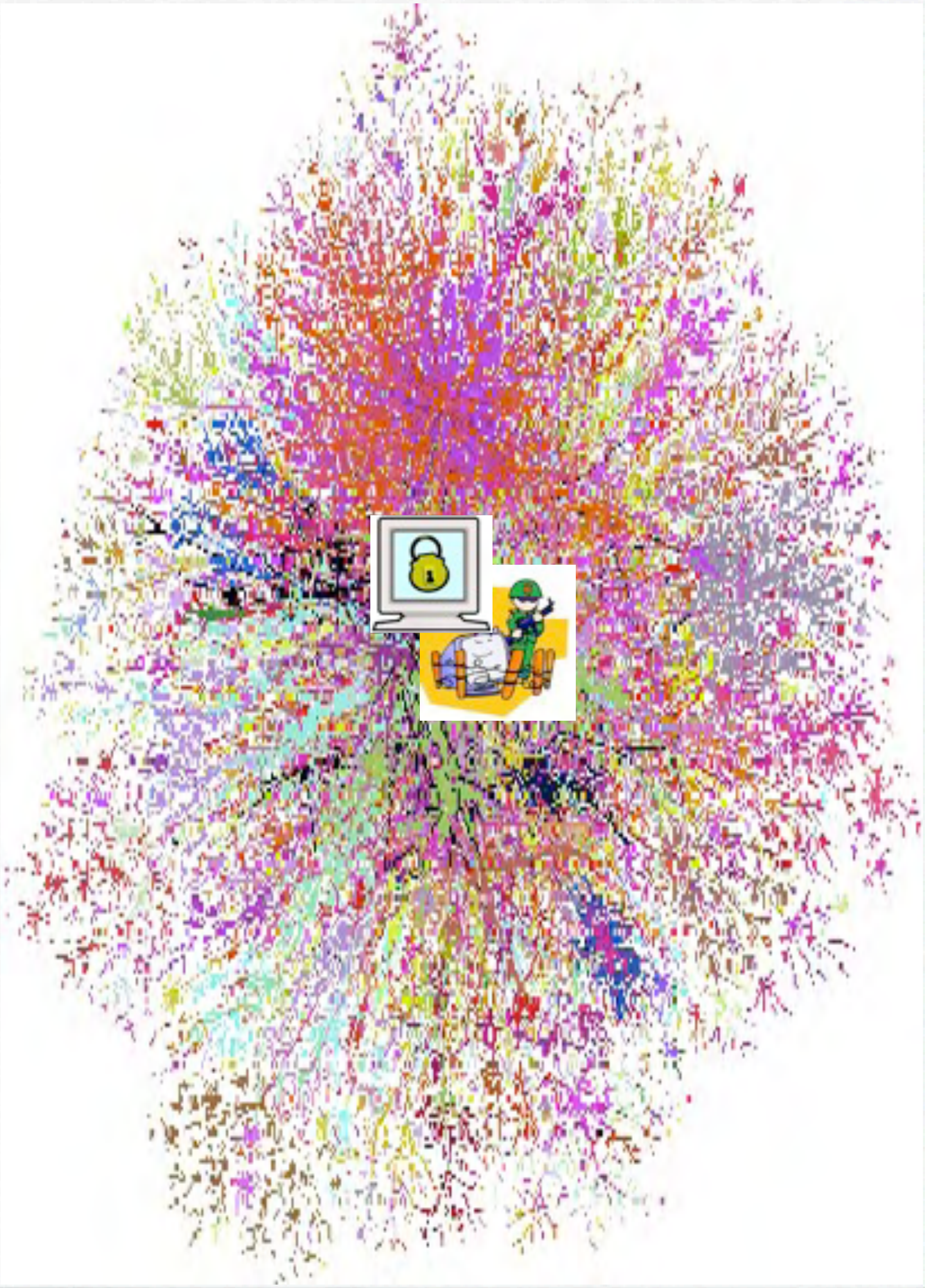
Applicability of Semantic Technologies in Security, Privacy and Trust

Mohammad M. R. Chowdhury
Senior Researcher
UNIK-University Graduate Center, Norway
mushfiq@ieee.org
http://www.unik.no/personer/mushfiq/



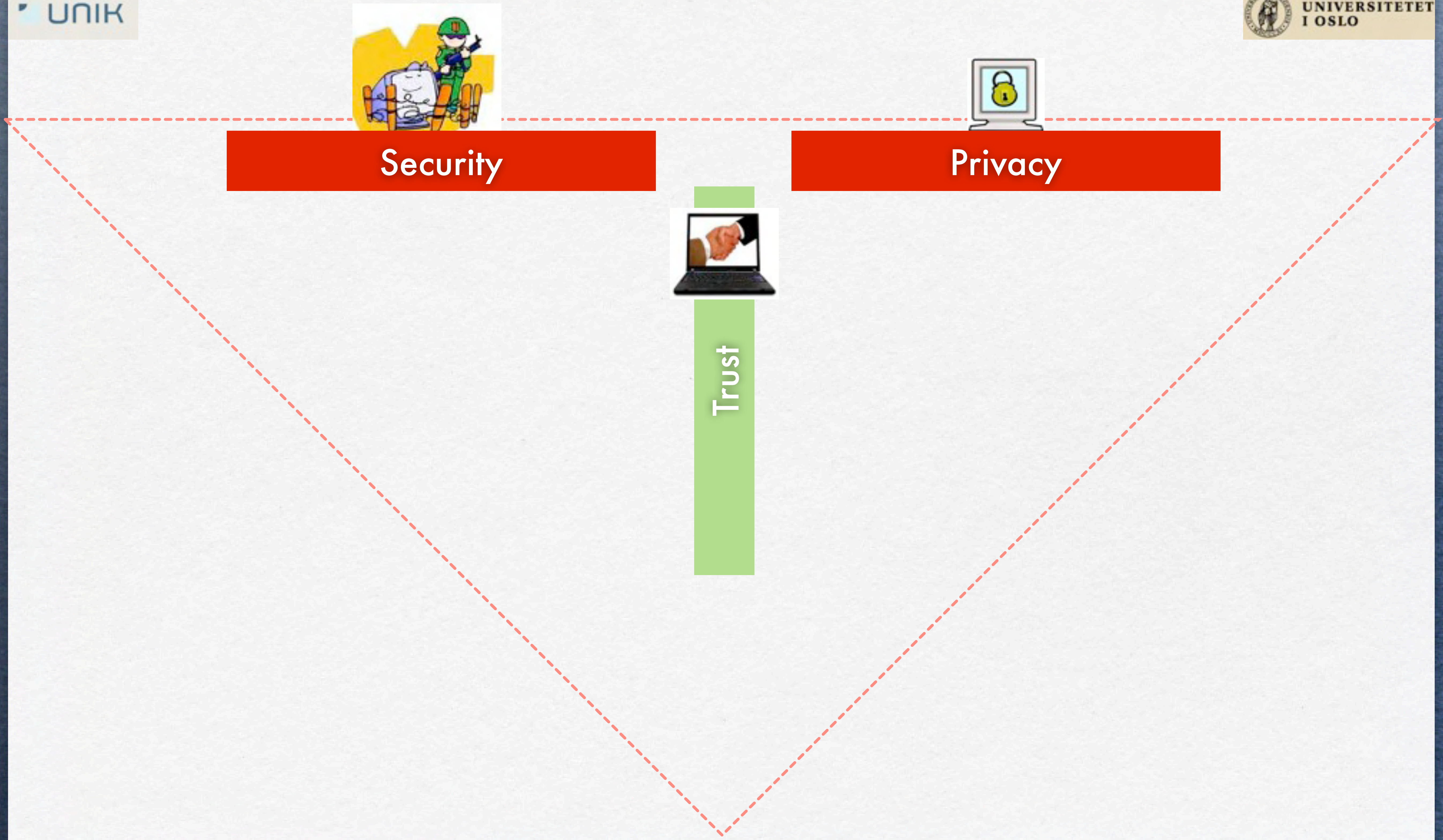
Agenda

- ☐ Intro: security, privacy & trust
- ☐ Motivation: why Semantics in Security and Privacy!
- ☐ Overview of the applicability
- ☐ Challenges & limitatipons



Security

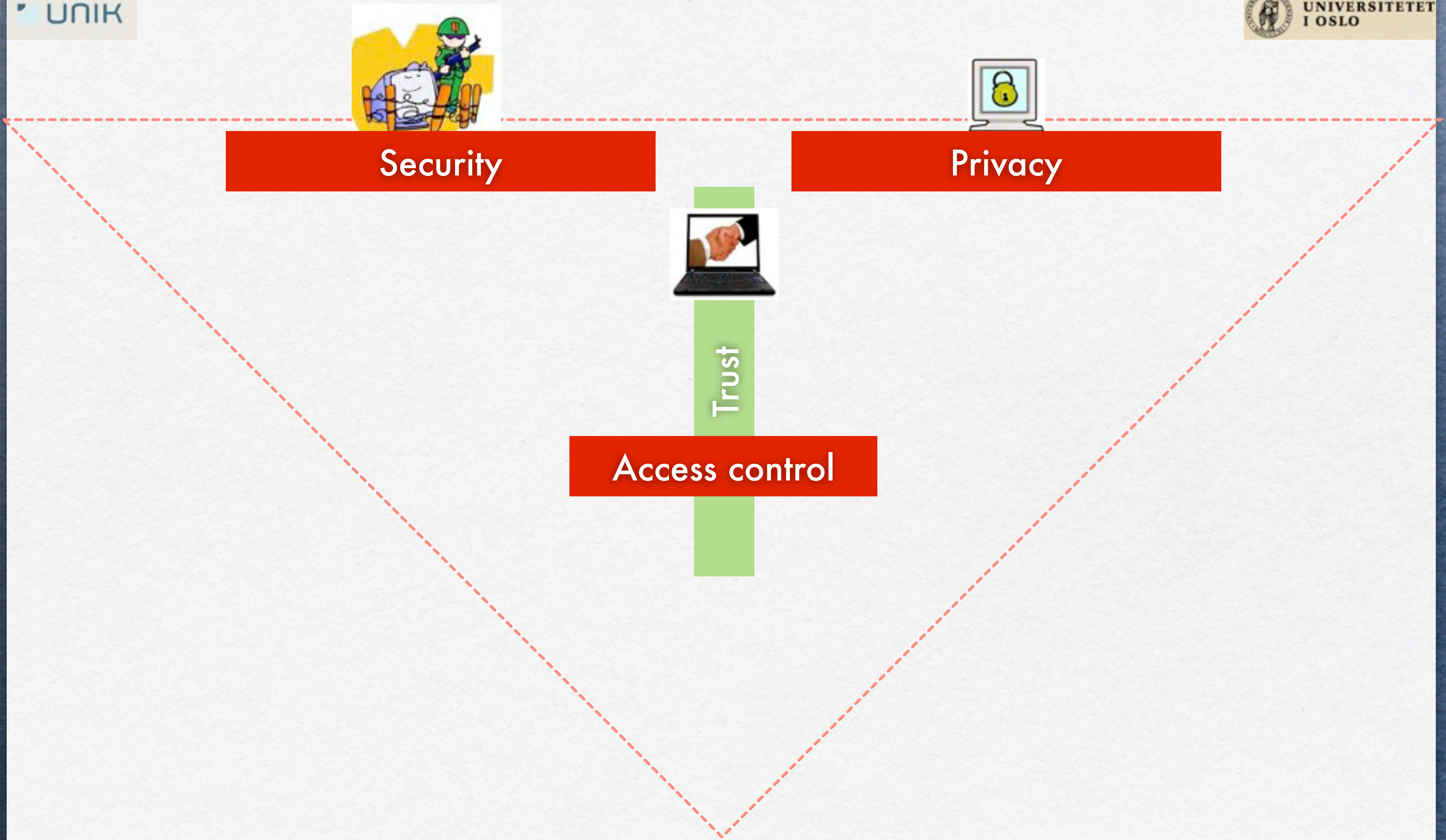
Privacy



Security

Privacy

Trust

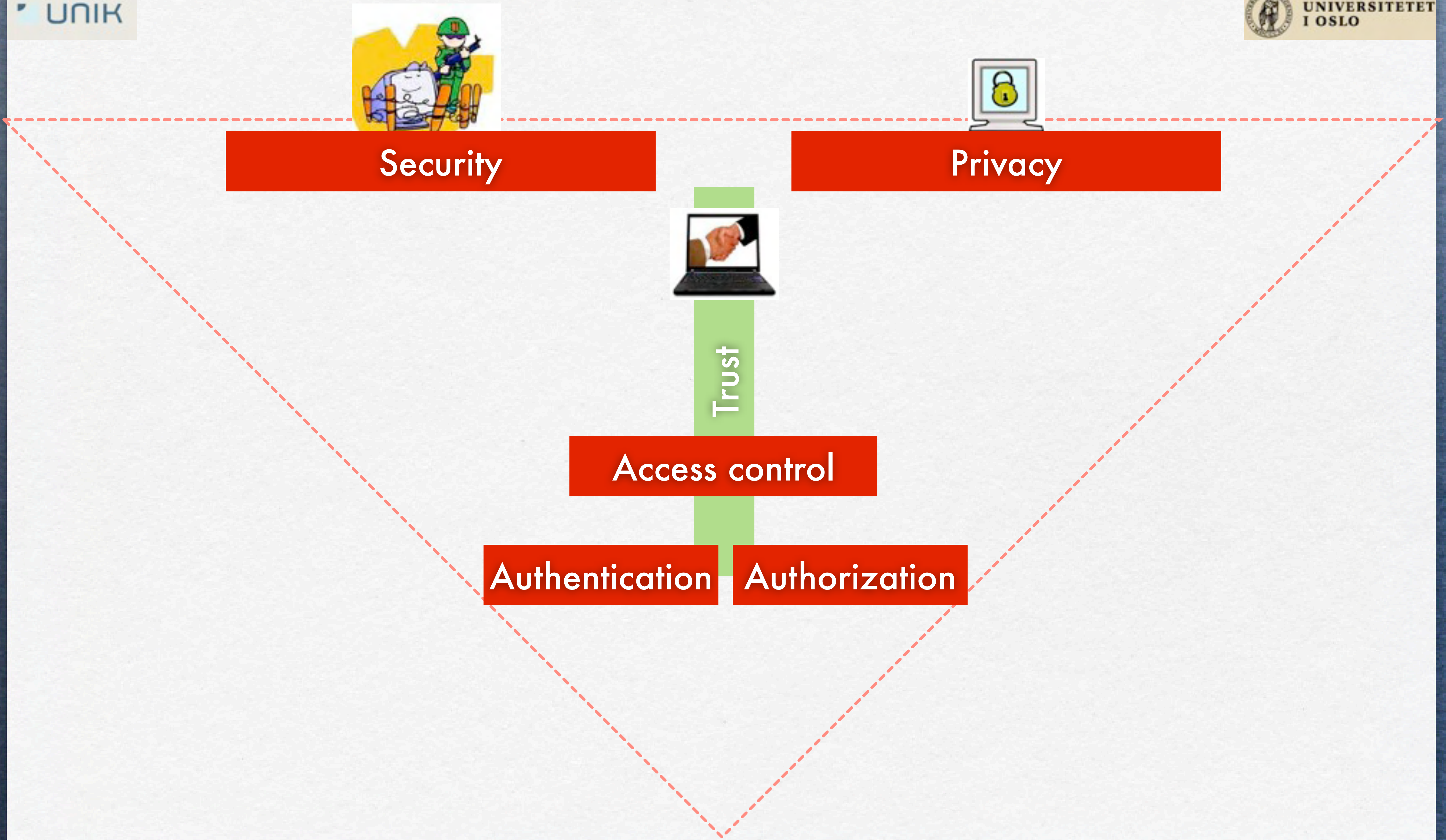


Security

Privacy

Trust

Access control



Security

Privacy

Trust

Access control

Authentication

Authorization

Why Semantics in security & privacy?

Semantics and Syntax

```
&lt;policy&gt;
&lt;xacl&gt;
  &lt;object href="id(contents)"/&gt;
  &lt;rule id="rule1"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Alice&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
      &lt;privilege type="write" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule2"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Bob&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule3"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="-"/&gt;
      &lt;privilege type="write" sign="-"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
&lt;/xacl&gt;
&lt;/policy&gt;

&lt;/document&gt;
```

Why Semantics in security & privacy?

Semantics and Syntax

```
&lt;policy&gt;
&lt;xacl&gt;
  &lt;object href="id(contents)"/&gt;
  &lt;rule id="rule1"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Alice&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
      &lt;privilege type="write" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule2"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Bob&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule3"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="-"/&gt;
      &lt;privilege type="write" sign="-"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
&lt;/xacl&gt;
&lt;/policy&gt;

&lt;/document&gt;
```

Meaning?:

> Alice has Read Write Privilege on content elements

> Bob has only Read Privilege on content elements

> By default, other users have no privilege on content elements

Why Semantics in security & privacy?

Semantics and Syntax

Why Dave has no access to the contents?

Why Alice has different privilege than Bob?

```
&lt;policy&gt;
&lt;xacl&gt;
  &lt;object href="id(contents)"/&gt;
  &lt;rule id="rule1"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Alice&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
      &lt;privilege type="write" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule2"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Bob&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule3"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="-"/&gt;
      &lt;privilege type="write" sign="-"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
&lt;/xacl&gt;
&lt;/policy&gt;

&lt;/document&gt;
```

Meaning?:

> Alice has Read Write Privilege on content elements

> Bob has only Read Privilege on content elements

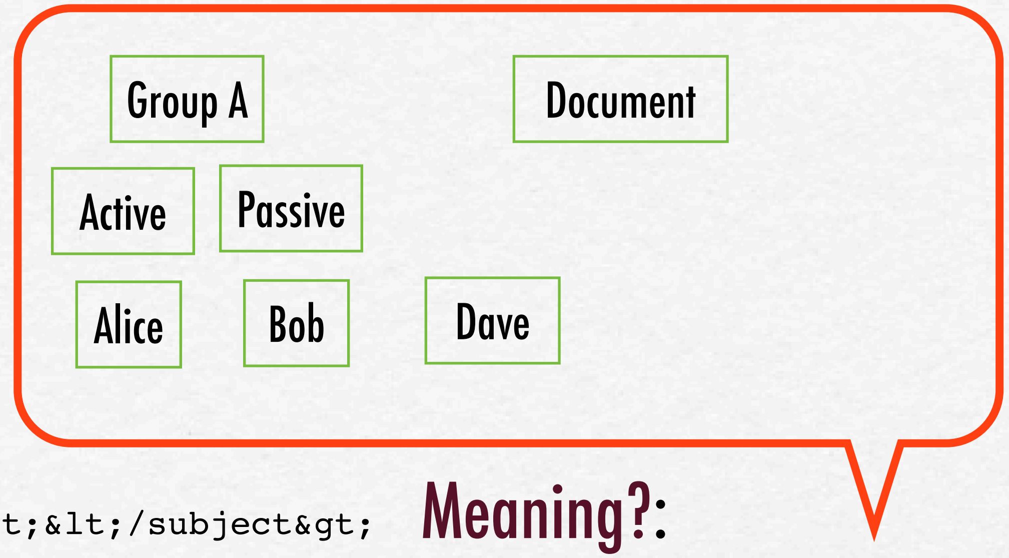
> By default, other users have no privilege on content elements

Why Semantics in security & privacy?

Semantics and Syntax

```
&lt;policy&gt;
&lt;xacl&gt;
  &lt;object href="id(contents)"/&gt;
  &lt;rule id="rule1"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Alice&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
      &lt;privilege type="write" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule2"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;uid&gt;Bob&lt;/uid&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="+"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
  &lt;rule id="rule3"&gt;
    &lt;acl&gt;
      &lt;subject&gt;&lt;/subject&gt;
      &lt;privilege type="read" sign="-"/&gt;
      &lt;privilege type="write" sign="-"/&gt;
    &lt;/acl&gt;
  &lt;/rule&gt;
&lt;/xacl&gt;
&lt;/policy&gt;

&lt;/document&gt;
```



Why Dave has no access to the contents?

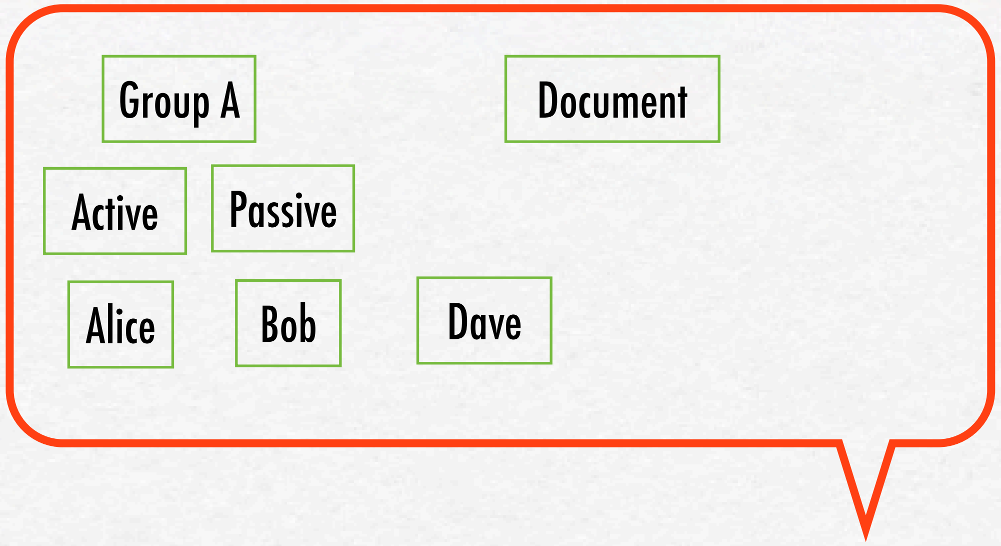
Why Alice has different privilege than Bob?

Meaning?:

> Alice has Read Write Privilege on content elements

> Bob has only Read Privilege on content elements

> By default, other users have no privilege on content elements



Group A

Document

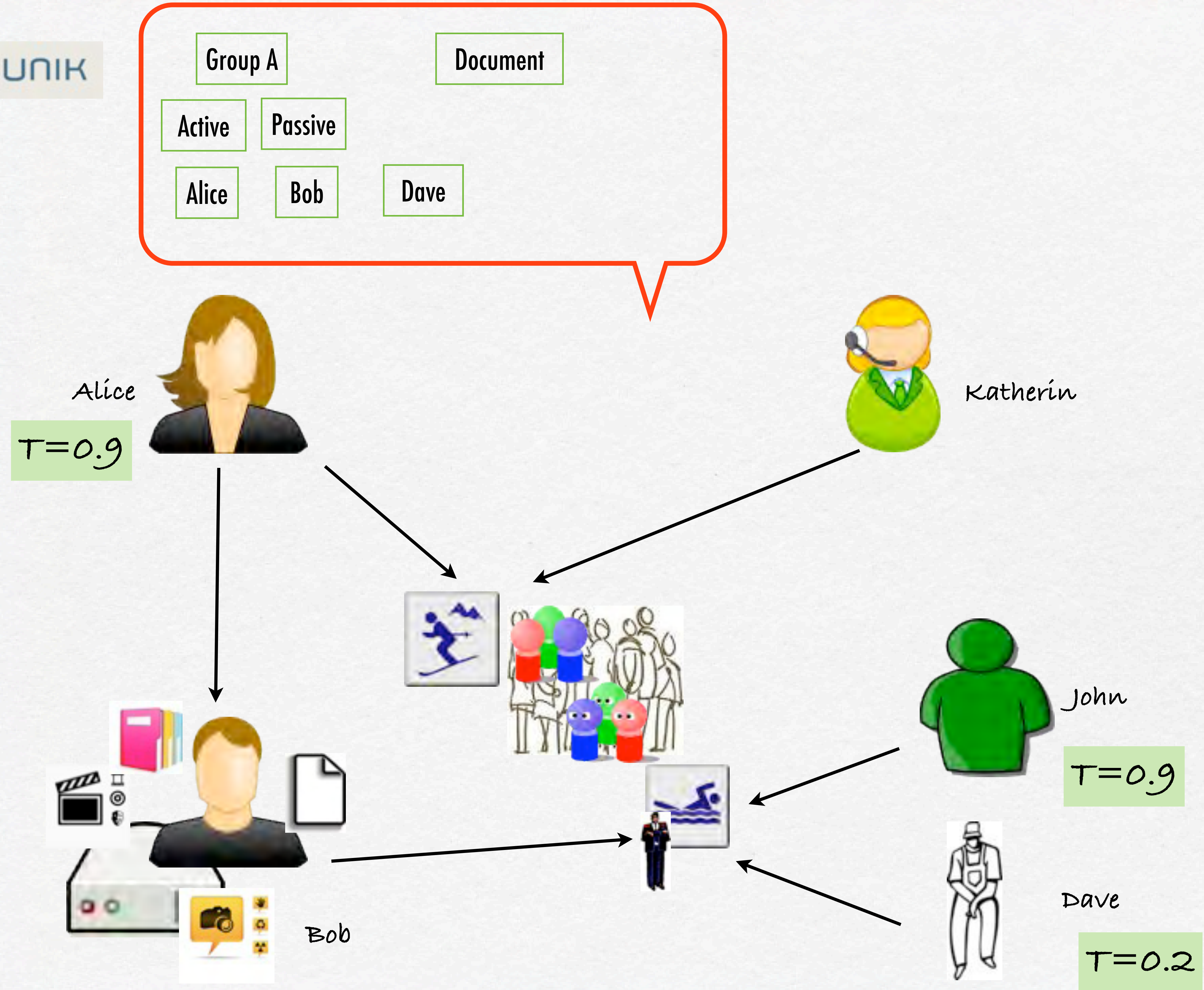
Active

Passive

Alice

Bob

Dave



Group A

Document

Active

Passive

Alice

Bob

Dave

Alice

T=0.9

Katherin

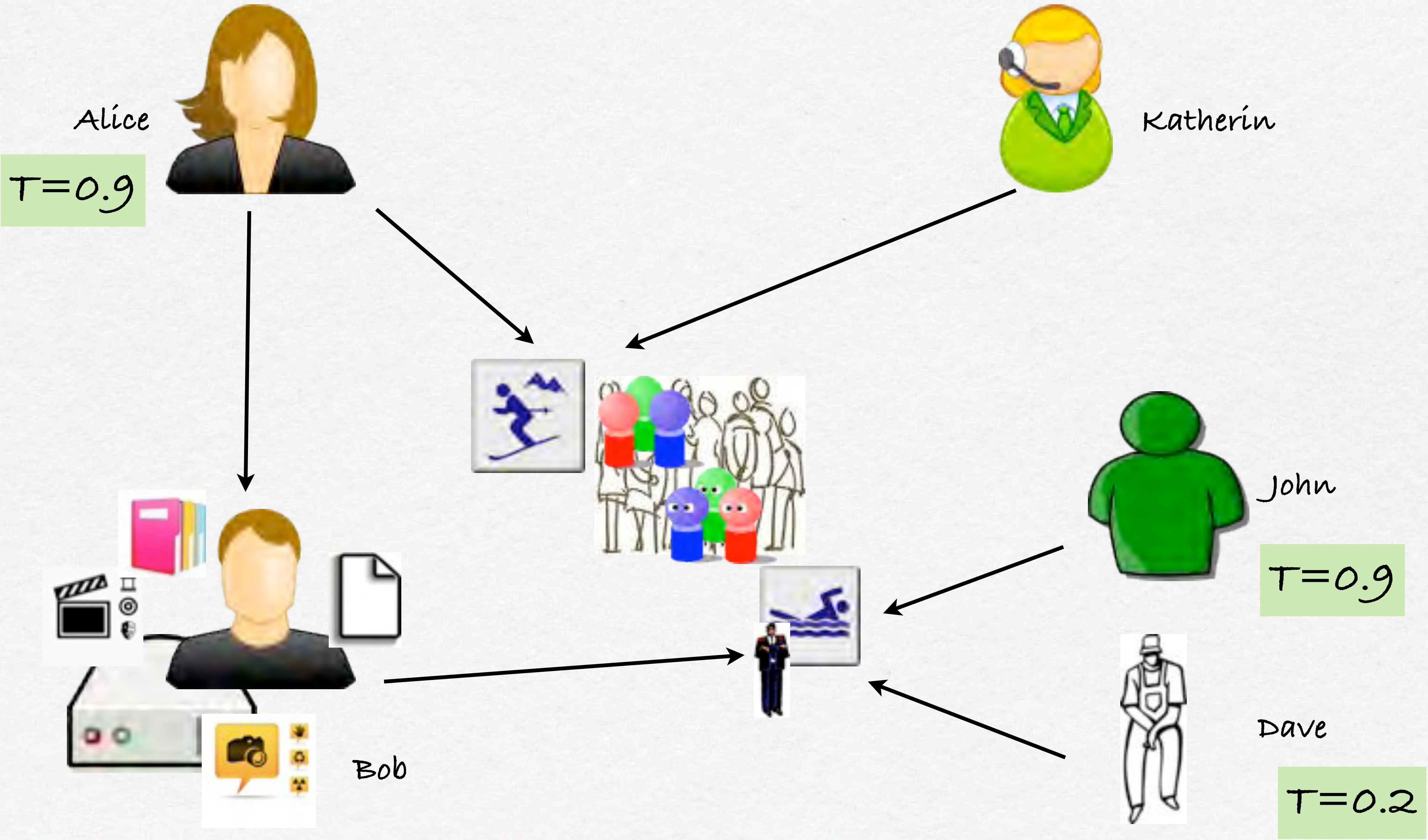
John

T=0.9

Dave

T=0.2

Bob



Alice

T=0.9

Katherin

John

T=0.9

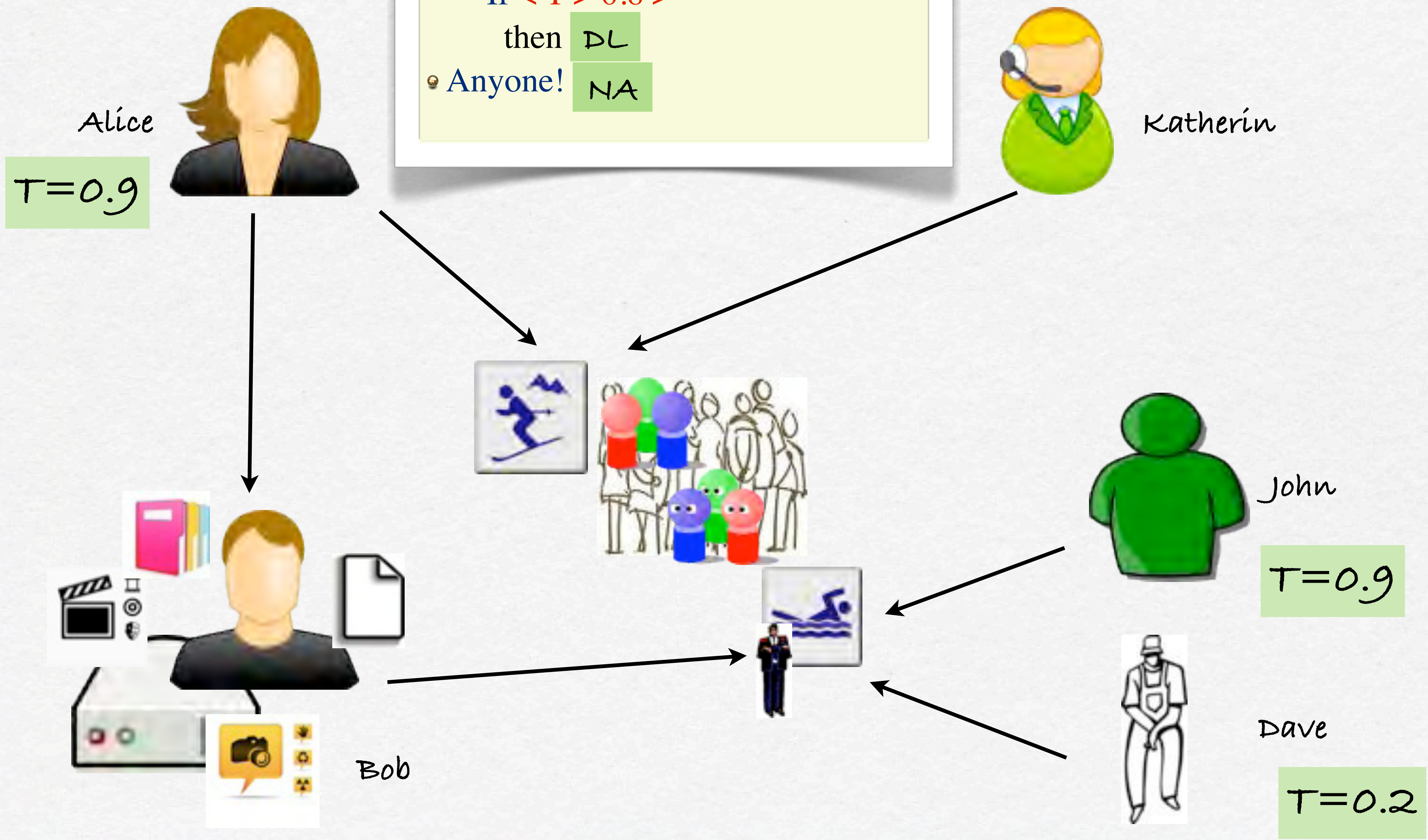
Dave

T=0.2

Bob

Security => Bob´s contents

```
If <Group>
   If < T < 0.8 >
      then View
If <Ski>
   If <Friend>
      If < T > 0.8 >
         then DL
Anyone! NA
```

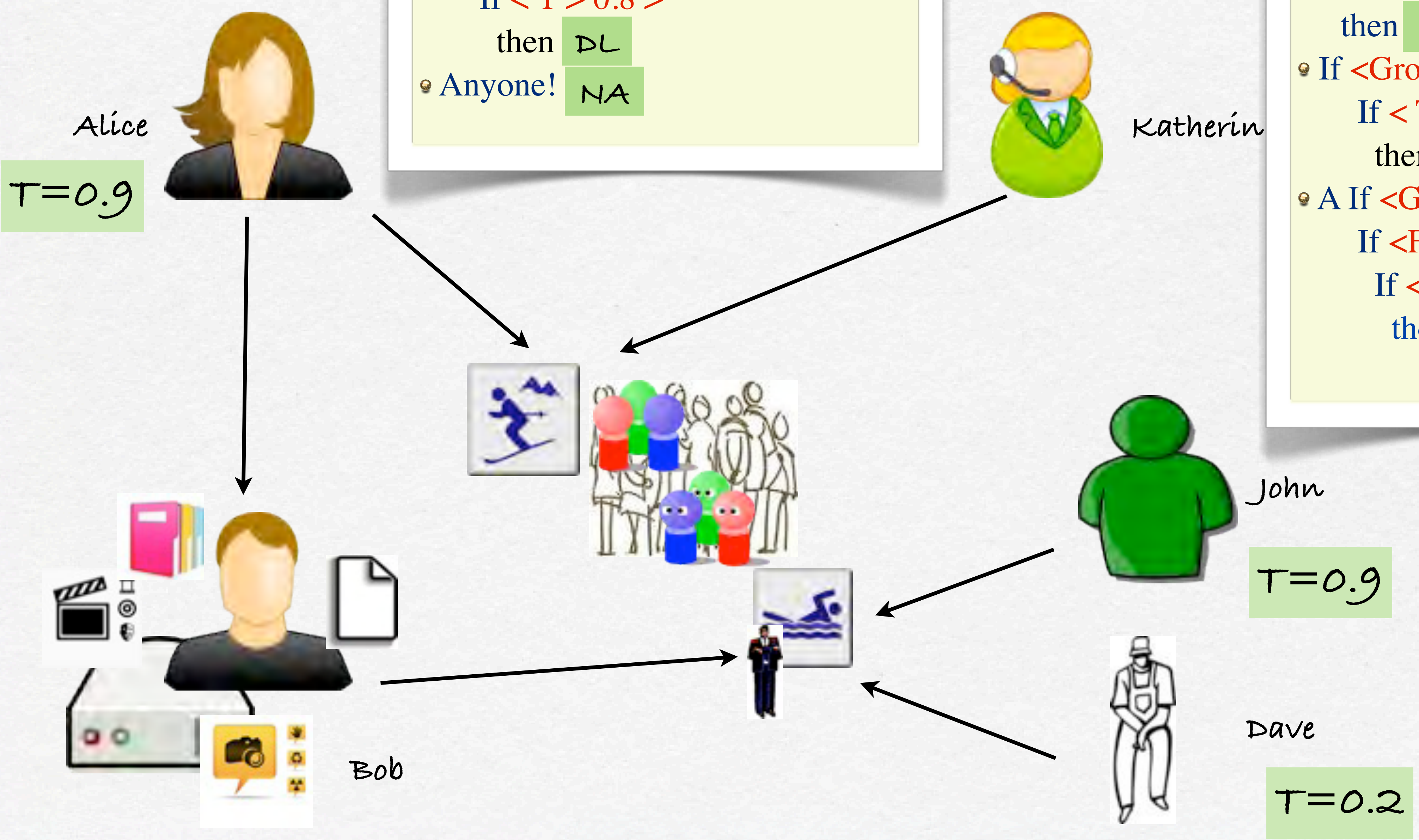


Security => Bob ´s contents

- If <Group>
  - If < T < 0.8 >
    - then View
- If <Ski>
  - If <Friend>
    - If < T > 0.8 >
      - then DL
- Anyone! NA

Privacy => Bob ´s profile

- If <Group>
  - then email
- If <Group>
  - If < T > 0.8 >
    - then phone
- A If <Group>
  - If <Friend>
    - If < T > 0.8 >
      - then location



Constraints!

- Group
- Role
- Relation
- Attributes
- Context

Constraints!

- Group
- Role
- Relation
- Attributes
- Context

Requirements!

Constraints!

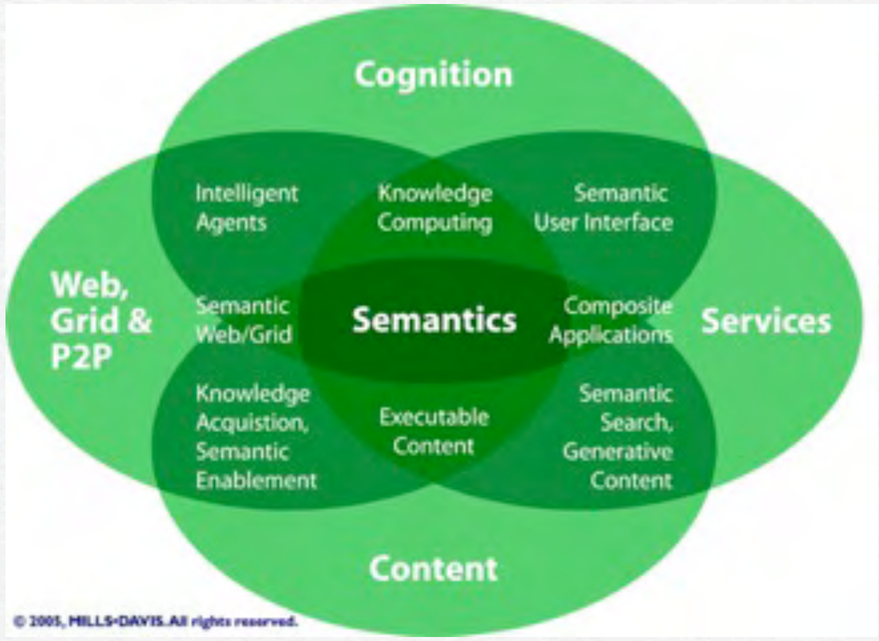
- Group
- Role
- Relation
- Attributes
- Context

Requirements!

□ Flexibility & expressivity
□ Personalization
□ Granularity
□ Manageability and maintainability
□ Scalability

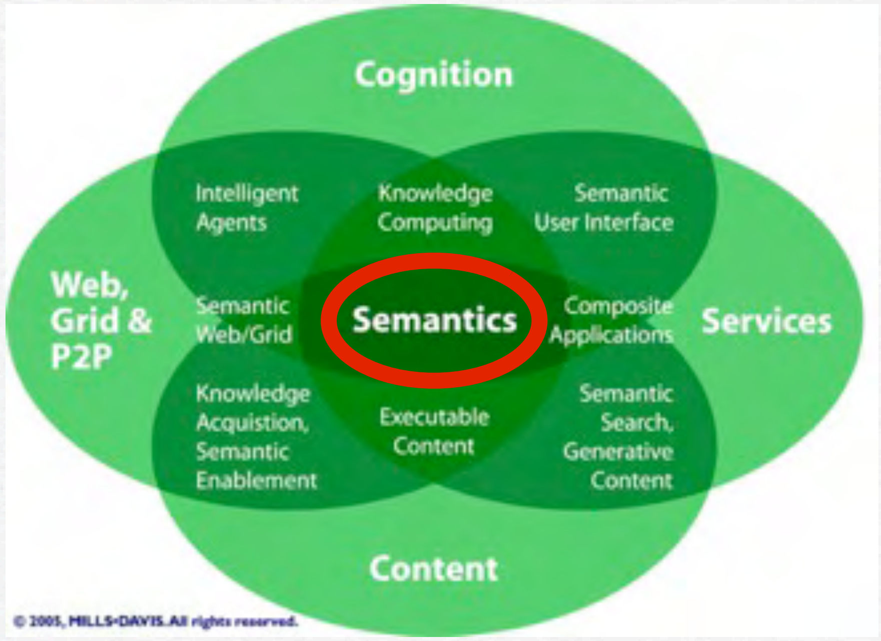
Motivation: Semantic Technologies

Application of Semantic technologies



Motivation: Semantic Technologies

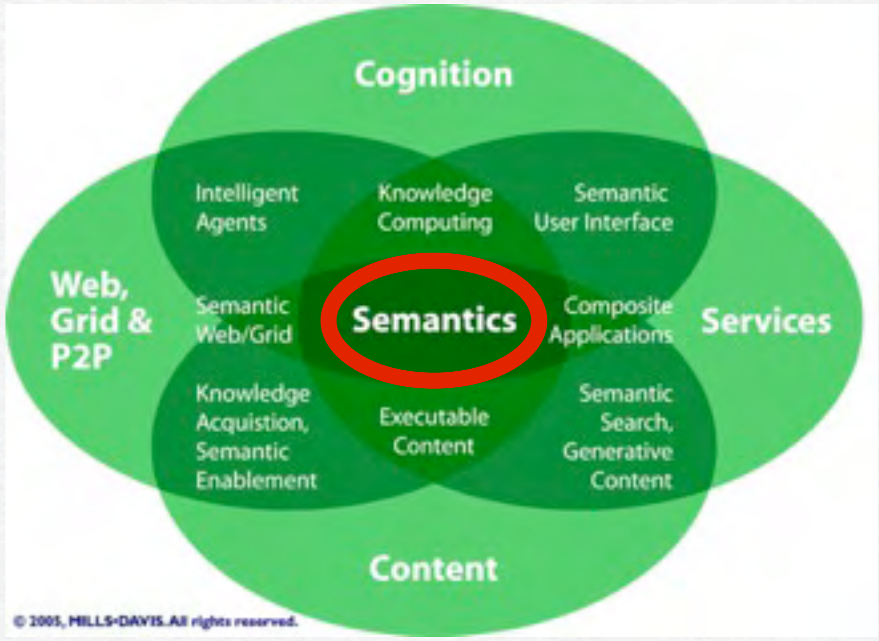
Application of Semantic technologies



© 2005, MILLS•DAVIS. All rights reserved.

Motivation: Semantic Technologies

Application of Semantic technologies



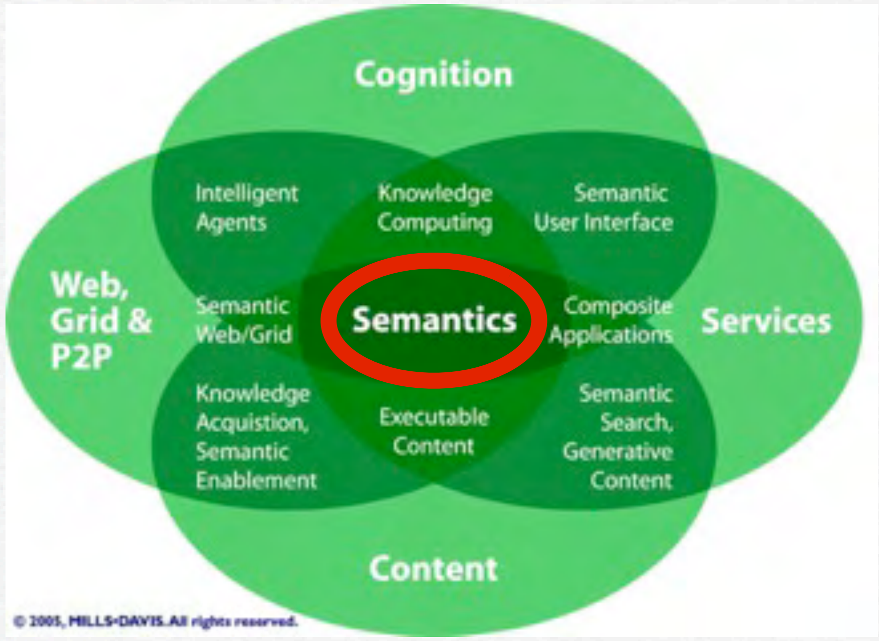
- access decisions: granting access requires deriving new facts based on existing facts - a potential areas of Semantic Technology due to its reasoning capabilities

UNIK

Motivation: Semantic Technologies

UNIVERSITETET I OSLO

Application of Semantic technologies

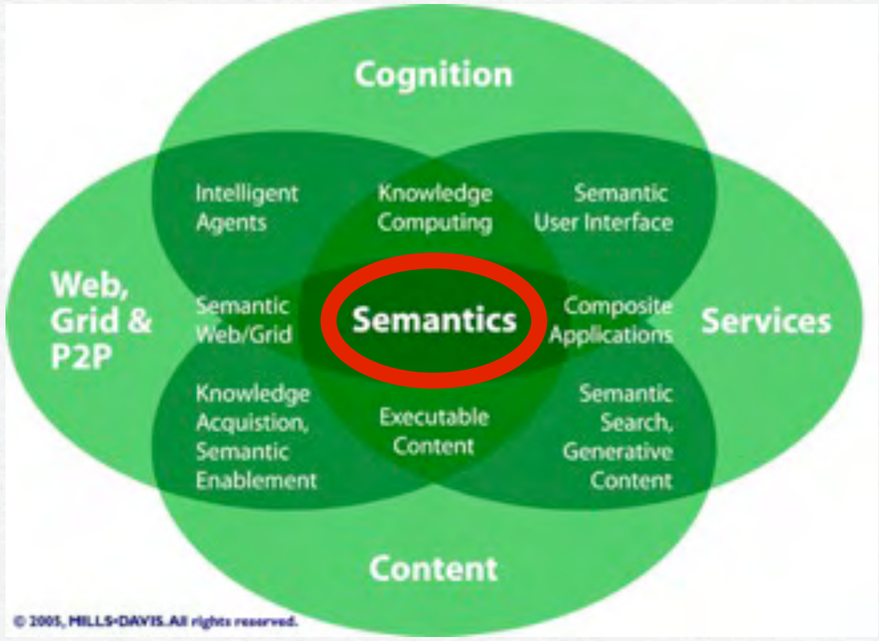


- access decisions: granting access requires deriving new facts based on existing facts - a potential areas of Semantic Technology due to its reasoning capabilities

Non-semantic (e.g. ACL) | Semantically Enhanced

Motivation: Semantic Technologies

Application of Semantic technologies



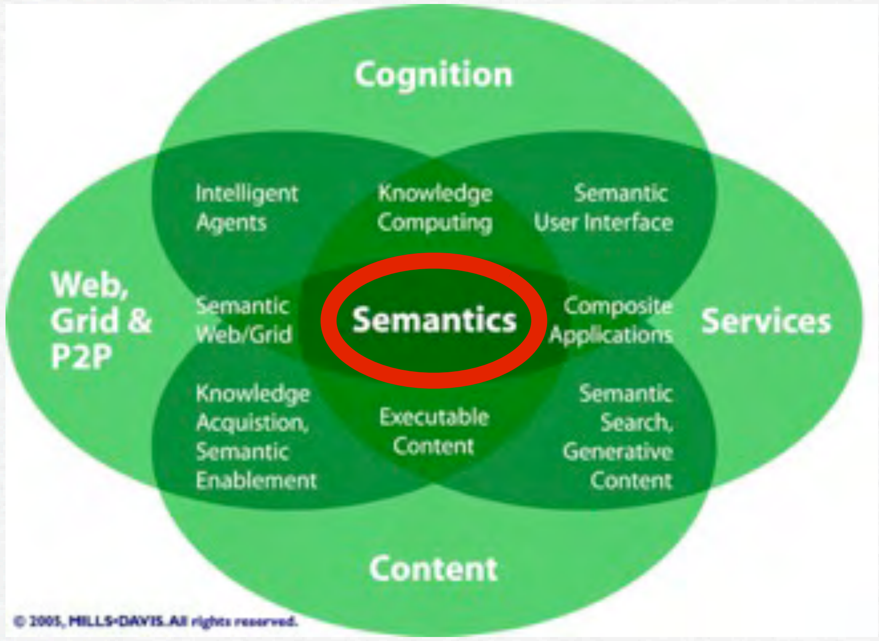
© 2005, MILLS-DAVIS. All rights reserved.

- access decisions: granting access requires deriving new facts based on existing facts - a potential areas of Semantic Technology due to its reasoning capabilities

	Non-semantic (e.g. ACL)	Semantically Enhanced
Complexity in constraints		
Maintenance & modification		
Easiness		

Motivation: Semantic Technologies

Application of Semantic technologies

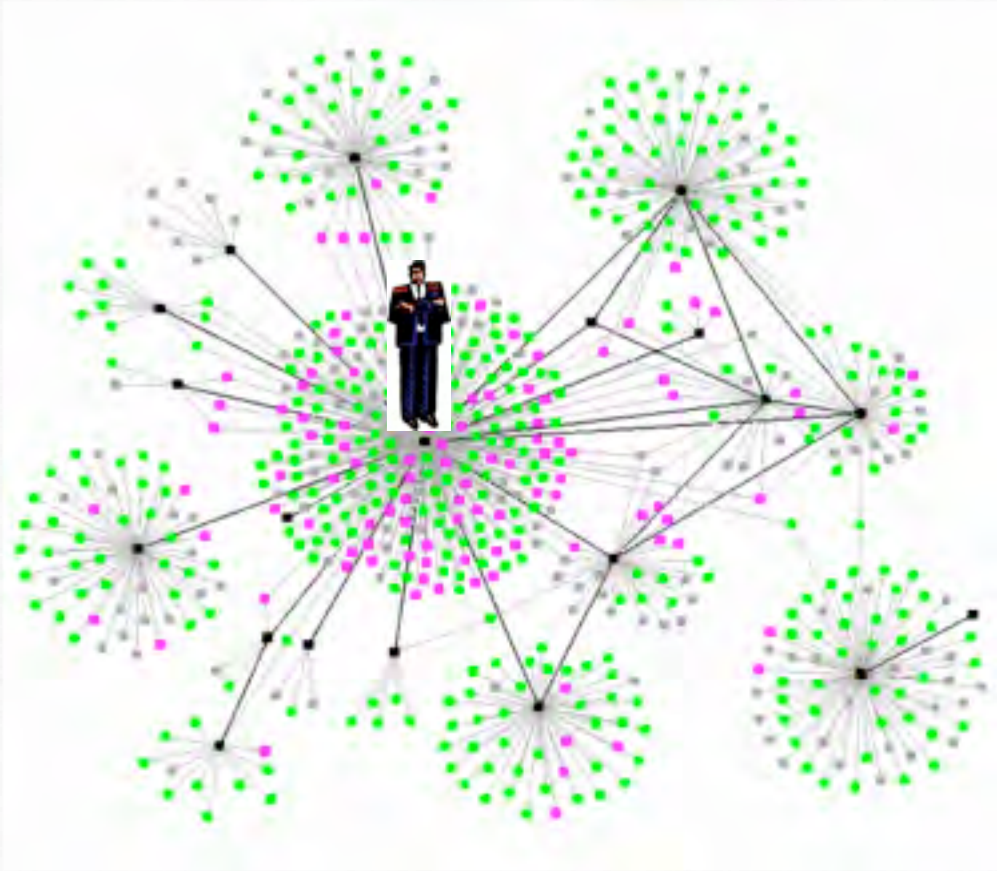


- access decisions: granting access requires deriving new facts based on existing facts - a potential areas of Semantic Technology due to its reasoning capabilities

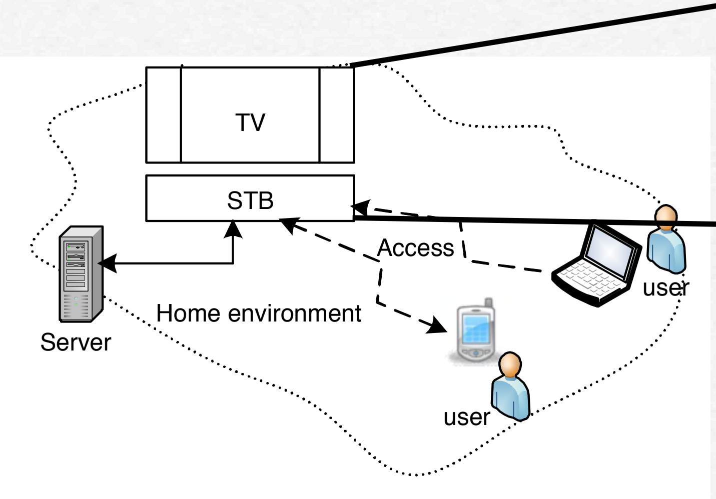
	Non-semantic (e.g. ACL)	Semantically Enhanced
Complexity in constraints		+
Maintenance & modification		+
Easiness	+	

Applicability - use cases scenario

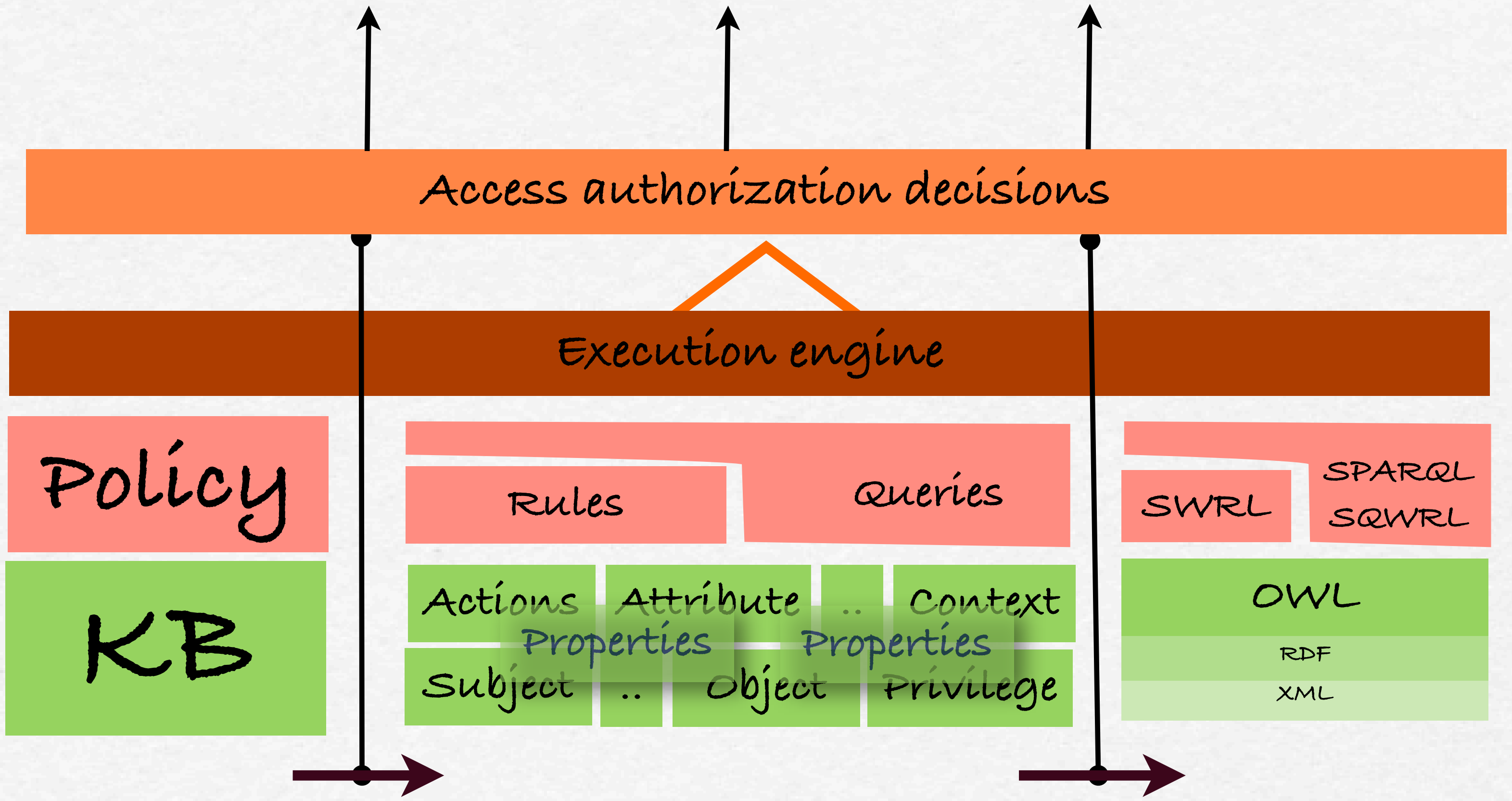
- □ On the Web: Social Network



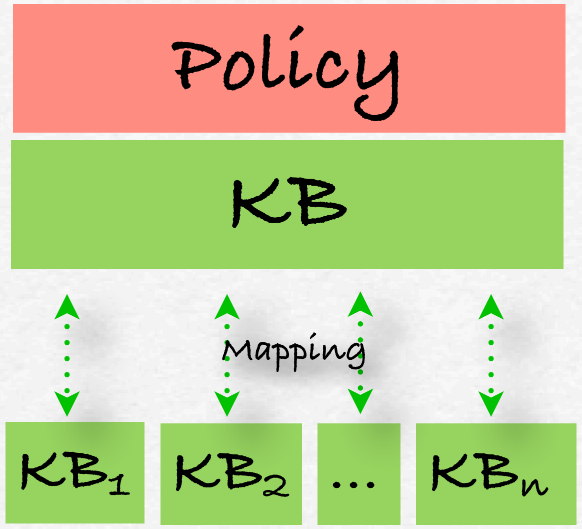
- □ On the Device: Home Network



Semantic technologies



Decentralization



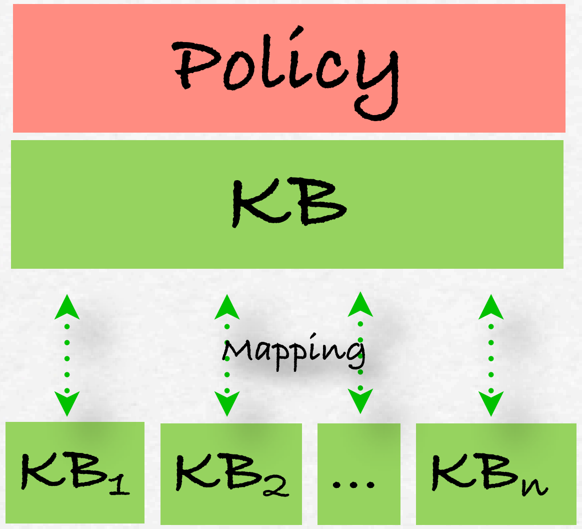
Motivation:

Privacy, user-centric + enhanced control

Better management and maintenance

Portable social graph to virtual community networks

Decentralization



Policy

KB

Mapping

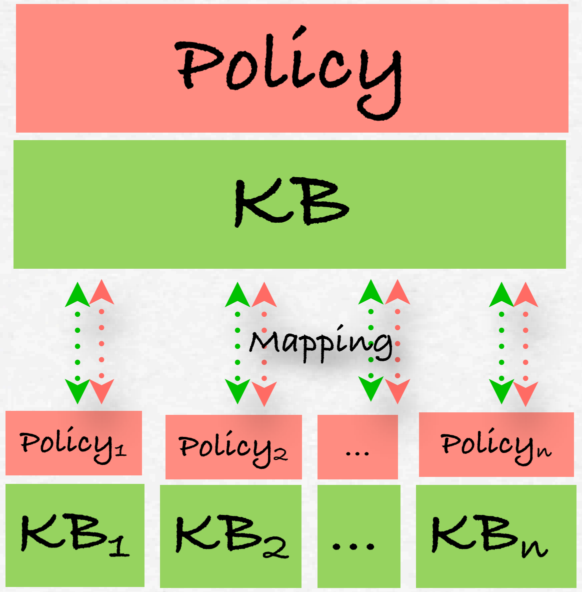
KB_1 KB_2 ... KB_n

Motivation:

Privacy, user-centric + enhanced control

Better management and maintenance

Portable social graph to virtual community networks



Policy

KB

Mapping

$Policy_1$ $Policy_2$ ... $Policy_n$

KB_1 KB_2 ... KB_n

Portable social graph + policy

Challenges!

- Expressivity Vs. complexity!

Challenges!

Rule 1:

$$Identity(?ID)\wedge hasRole(?ID,?R)\wedge Family(?R)\wedge$$
$$has\Pr ivilege(?R,?Y)\wedge Contents(?Z)\wedge need\Pr ivilege(?Z,?Y)$$
$$\rightarrow hasAccessTo(?ID,?Z)$$

Rule 2:

$$Identity(?ID)\wedge hasRole(?ID,?R)\wedge Family(?R)\wedge$$
$$hasAge(?ID,?y)\wedge swrlb:greaterThan(?y,15)\wedge$$
$$has\Pr ivilege(?R,?Y)\wedge Contents(?Z)\wedge need\Pr ivilege(?Z,?Y)$$
$$\rightarrow hasAccessTo(?ID,?Z)$$

Rule 3:

$$Identity(?ID)\wedge hasRole(?ID,?R)\wedge Family(?R)\wedge$$
$$hasAge(?ID,?y)\wedge swrlb:greaterThan(?y,15)\wedge$$
$$hasTrustlevel(?ID,?x)\wedge swrlb:lessThan(?x,0.7)\wedge$$
$$has\Pr ivilege(?R,?Y)\wedge Contents(?Z)\wedge need\Pr ivilege(?Z,?Y)$$
$$\rightarrow hasAccessTo(?ID,?Z)$$

- Expressivity Vs. complexity!

Challenges!

- Expressivity Vs. complexity!

Rule 1:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$has\Pr ivilege(?R,?Y) \wedge Contents(?Z) \wedge need\Pr ivilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$

Rule 2:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$\boxed{hasAge(?ID,?y) \wedge swrlb : greaterThan(?y,15) \wedge}$

$has\Pr ivilege(?R,?Y) \wedge Contents(?Z) \wedge need\Pr ivilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$

Rule 3:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$\boxed{hasAge(?ID,?y) \wedge swrlb : greaterThan(?y,15) \wedge}$

$\boxed{hasTrustlevel(?ID,?x) \wedge swrlb : lessThan(?x,0.7) \wedge}$

$has\Pr ivilege(?R,?Y) \wedge Contents(?Z) \wedge need\Pr ivilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$

Challenges!

- Expressivity Vs. complexity!

Rule 1:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$has\,Privilege(?R,?Y) \wedge Contents(?Z) \wedge need\,Privilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$

Rule 2:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$\boxed{hasAge(?ID,?y) \wedge swrlb:greaterThan(?y,15) \wedge}$

$has\,Privilege(?R,?Y) \wedge Contents(?Z) \wedge need\,Privilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$

Rule 3:

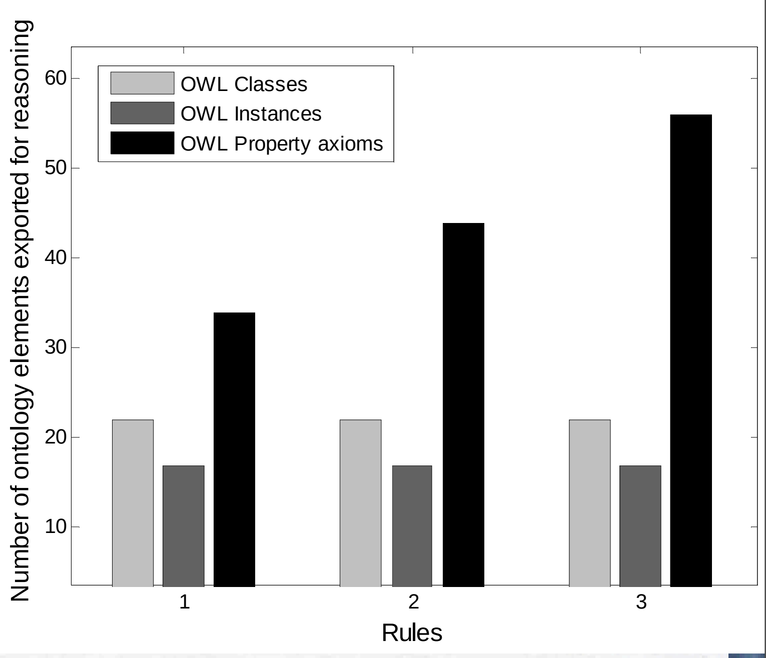
$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$

$\boxed{hasAge(?ID,?y) \wedge swrlb:greaterThan(?y,15) \wedge}$

$\boxed{hasTrustlevel(?ID,?x) \wedge swrlb:lessThan(?x,0.7) \wedge}$

$has\,Privilege(?R,?Y) \wedge Contents(?Z) \wedge need\,Privilege(?Z,?Y)$

$\rightarrow hasAccessTo(?ID,?Z)$



Challenges!

Rule 1:

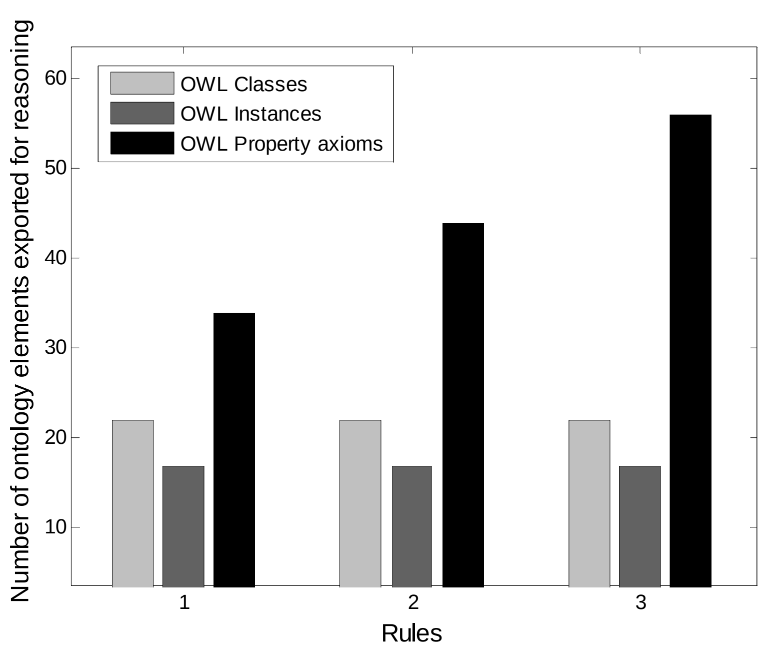
$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$
$hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y)$
$\rightarrow hasAccessTo(?ID,?Z)$

Rule 2:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$
$\boxed{hasAge(?ID,?y) \wedge swrlb: greaterThan(?y,15) \wedge}$
$hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y)$
$\rightarrow hasAccessTo(?ID,?Z)$

Rule 3:

$Identity(?ID) \wedge hasRole(?ID,?R) \wedge \boxed{Family(?R) \wedge}$
$\boxed{hasAge(?ID,?y) \wedge swrlb: greaterThan(?y,15) \wedge}$
$\boxed{hasTrustlevel(?ID,?x) \wedge swrlb: lessThan(?x,0.7) \wedge}$
$hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y)$
$\rightarrow hasAccessTo(?ID,?Z)$



- □ Expressivity Vs. complexity!
- □ Realtime reasoning over complex constraints

UNIK

Challenges!

Rule 1:

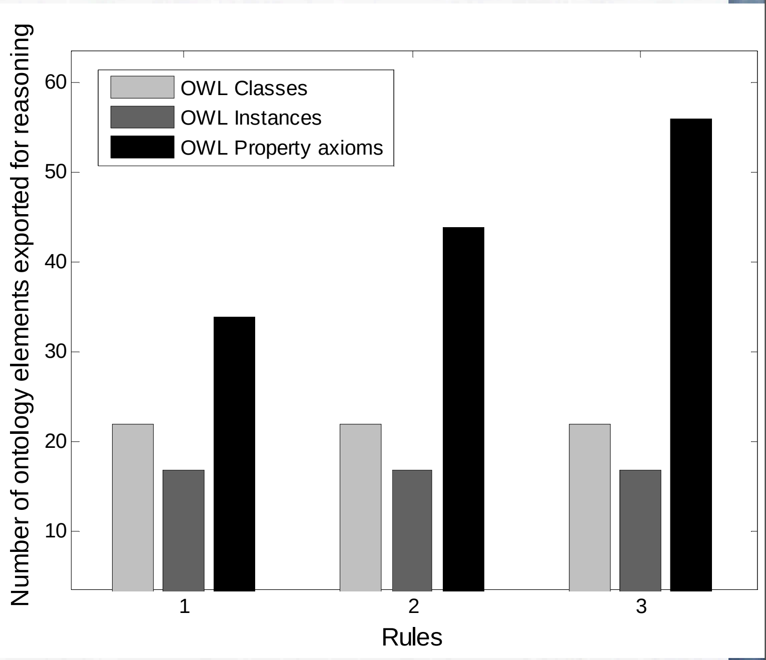
$$Identity(?ID) \wedge hasRole(?ID,?R) \wedge Family(?R) \wedge hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y) \rightarrow hasAccessTo(?ID,?Z)$$

Rule 2:

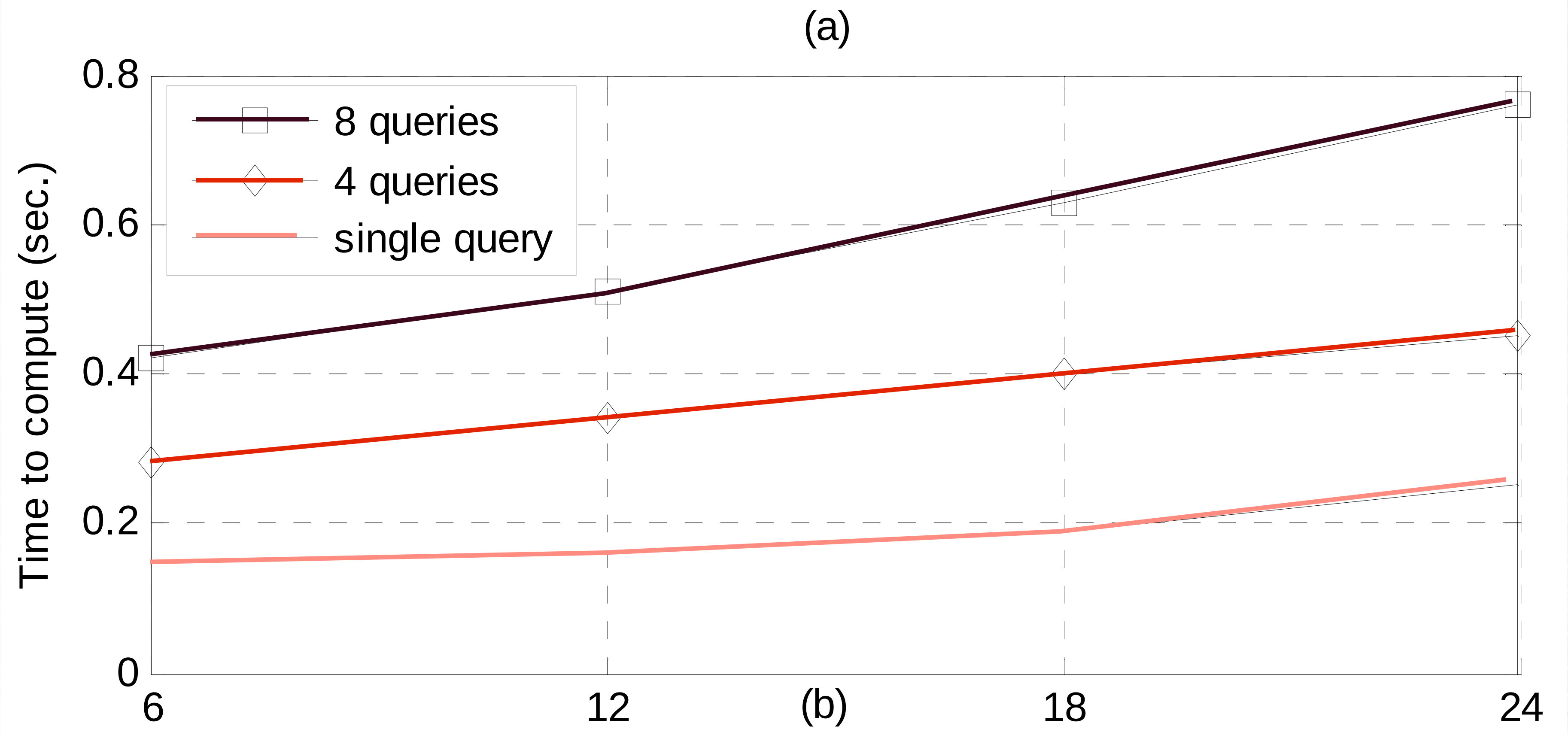
$$Identity(?ID) \wedge hasRole(?ID,?R) \wedge Family(?R) \wedge hasAge(?ID,?y) \wedge swrlb: greaterThan(?y,15) \wedge hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y) \rightarrow hasAccessTo(?ID,?Z)$$

Rule 3:

$$Identity(?ID) \wedge hasRole(?ID,?R) \wedge Family(?R) \wedge hasAge(?ID,?y) \wedge swrlb: greaterThan(?y,15) \wedge hasTrustlevel(?ID,?x) \wedge swrlb: lessThan(?x,0.7) \wedge hasPrivilege(?R,?Y) \wedge Contents(?Z) \wedge needPrivilege(?Z,?Y) \rightarrow hasAccessTo(?ID,?Z)$$



- □ Expressivity Vs. complexity!
- □ Realtime reasoning over complex constraints



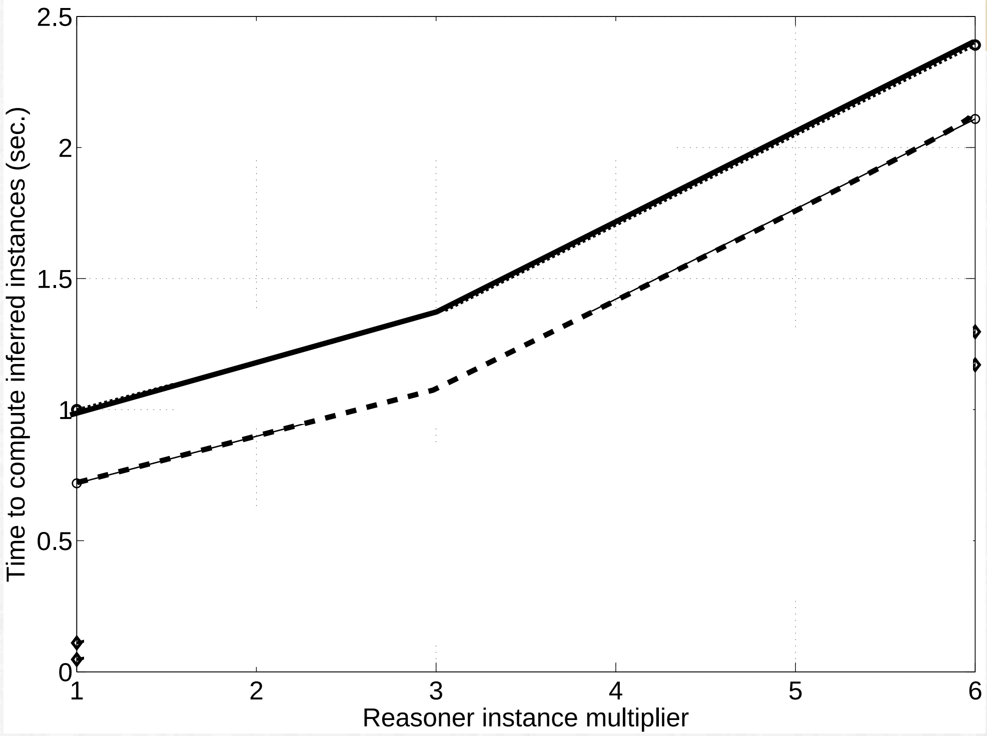
Challenges!

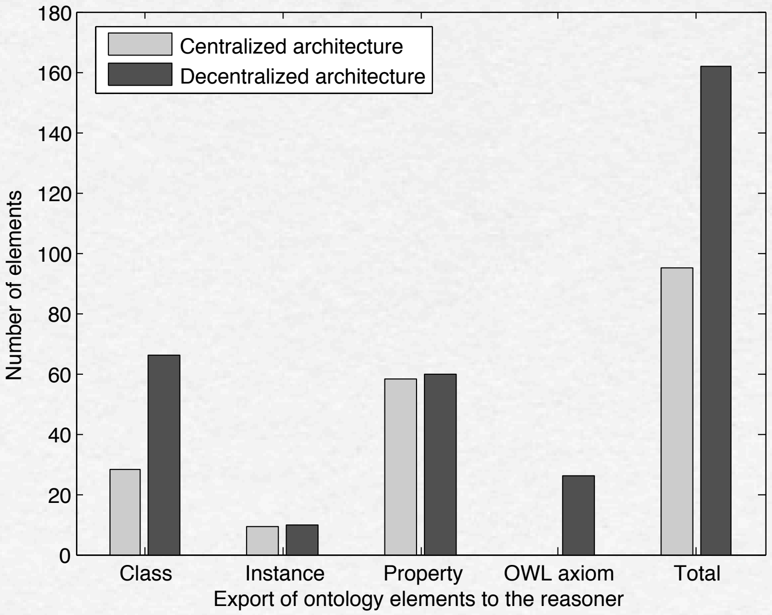
- Decentralization & computational complexity

Challenges!

Penalty?

- □ Decentralization & computational complexity

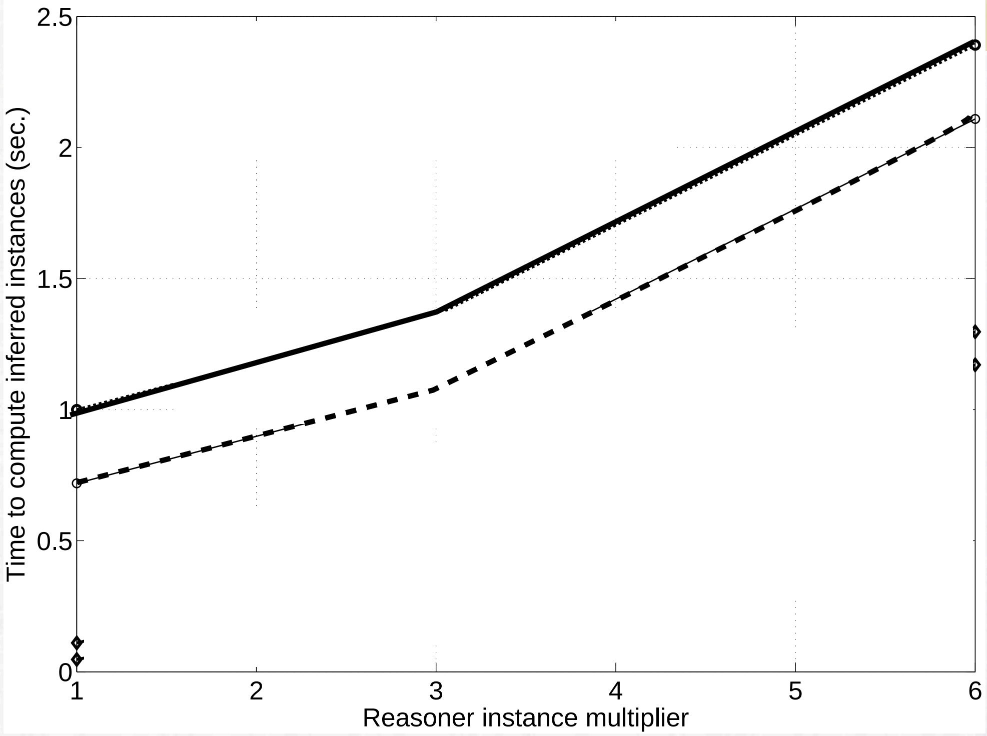


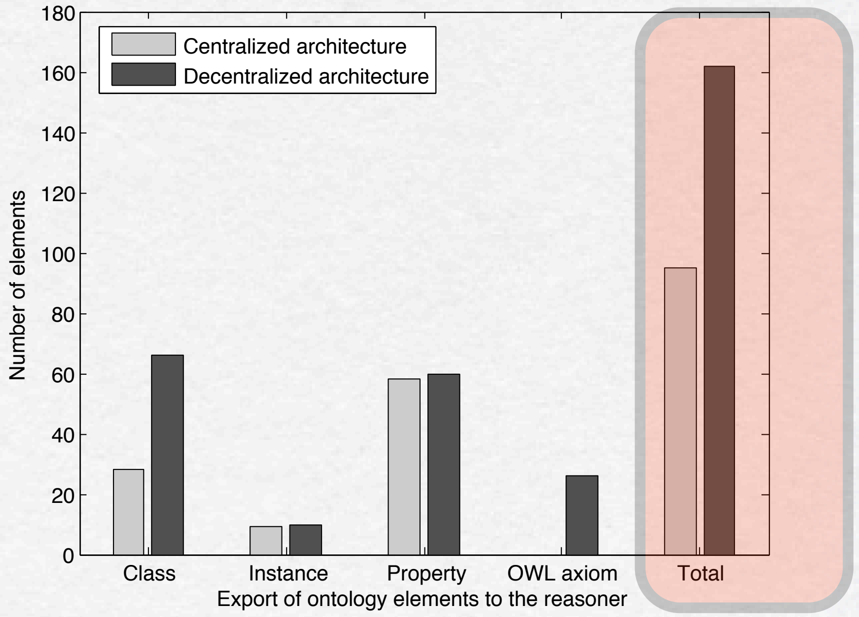


Challenges!

- □ Decentralization & computational complexity

Penalty?





Challenges!

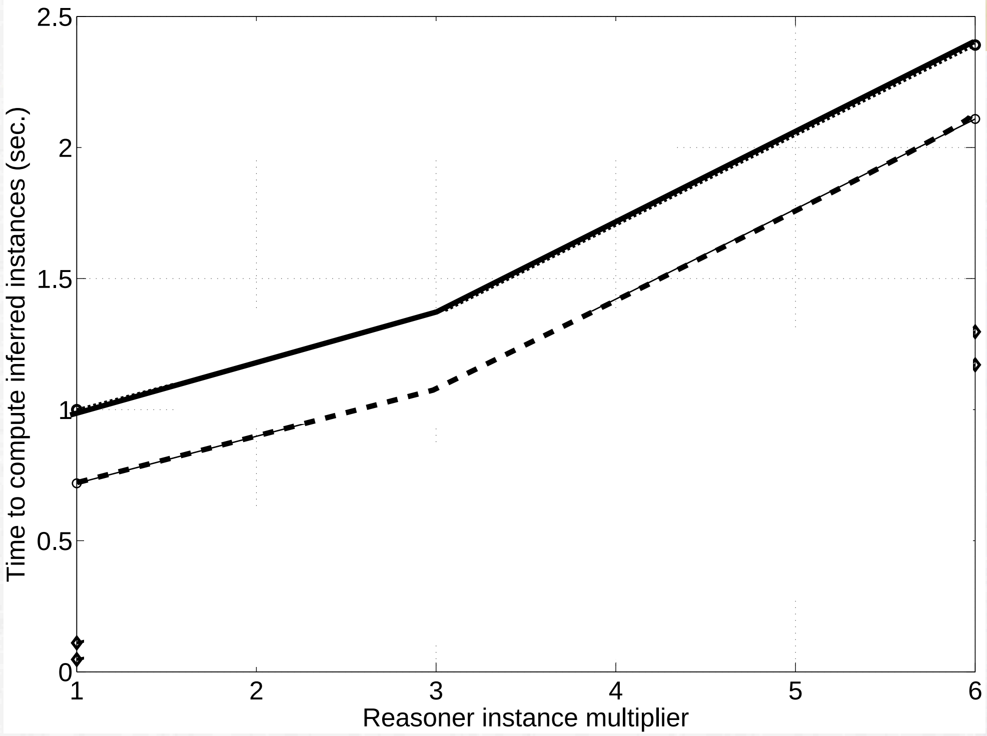
- □ Decentralization & computational complexity

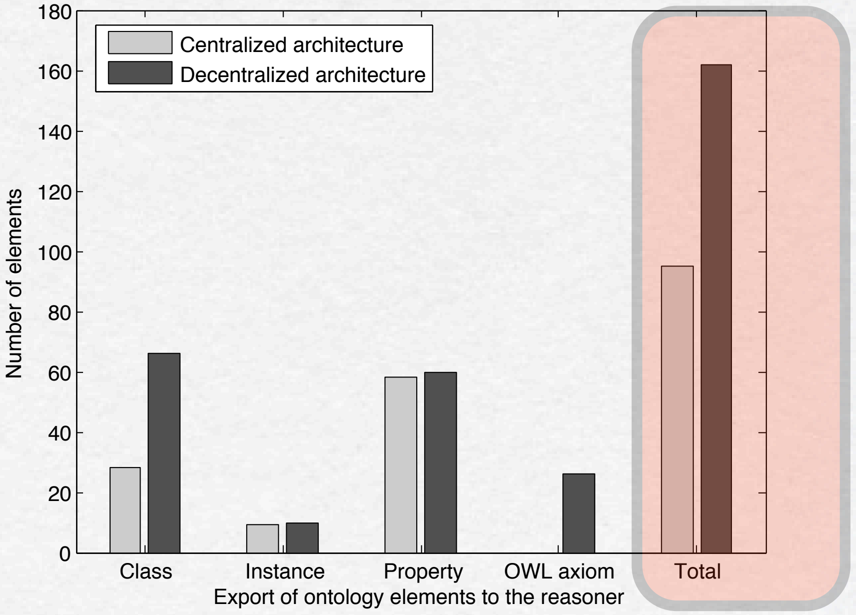
Other issues!

Efficient mapping

Privacy preserving ontology mapping

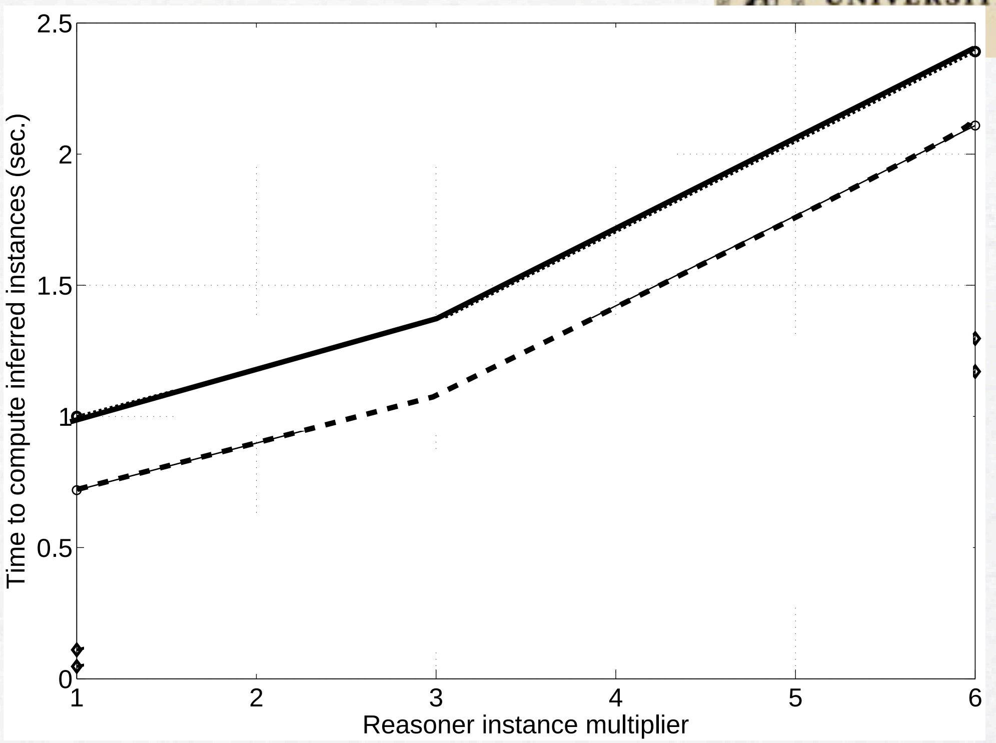
Penalty?





Challenges!

Penalty?

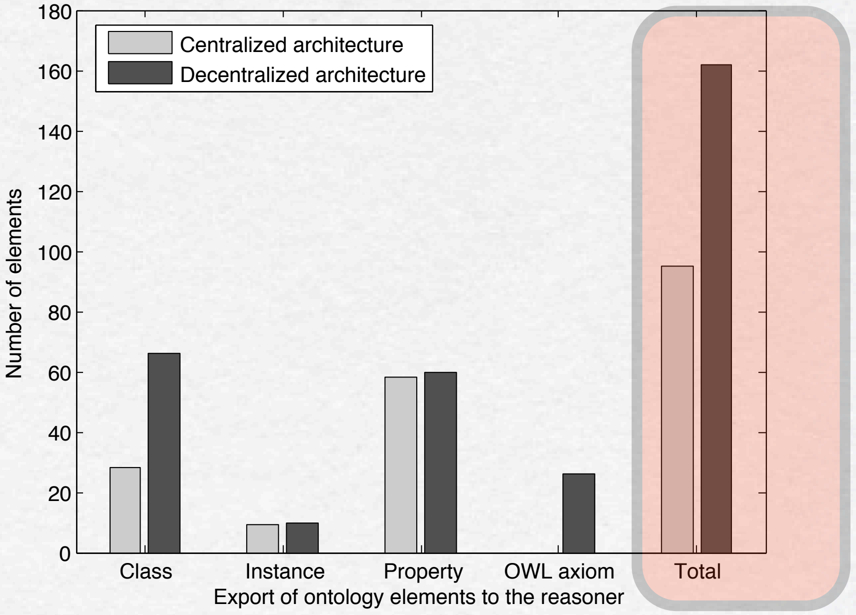


- □ Decentralization & computational complexity

Other issues!

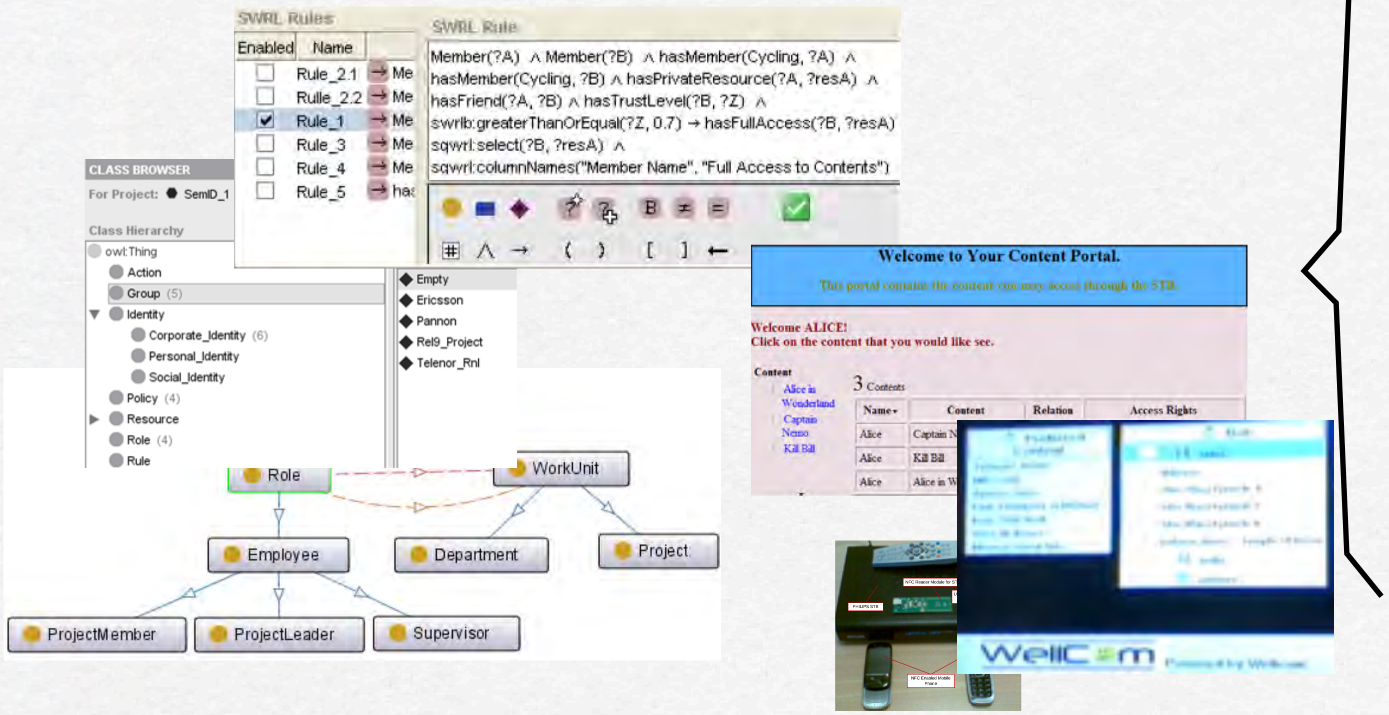
Efficient mapping

Privacy preserving ontology mapping



- □ Limitation of tools!

Alternative to real time reasoning!



SWRL Rules

Enabled	Name	
□	Rule_2.1	→ Me
□	Rulle_2.2	→ Me
☑	Rule_1	→ Me
□	Rule_3	→ Me
□	Rule_4	→ Me
□	Rule_5	→ has

SWRL Rule

```
Member(?A) ∧ Member(?B) ∧ hasMember(Cycling, ?A) ∧
hasMember(Cycling, ?B) ∧ hasPrivateResource(?A, ?resA) ∧
hasFriend(?A, ?B) ∧ hasTrustLevel(?B, ?Z) ∧
swrlb:greaterThanOrEqual(?Z, 0.7) → hasFullAccess(?B, ?resA)
sqwrl:select(?B, ?resA) ∧
sqwrl:columnNames("Member Name", "Full Access to Contents")
```

CLASS BROWSER

For Project: ● SemID_1

Class Hierarchy

- owl:Thing
  - Action
  - Group (5)
  - Identity
    - Corporate_Identity (6)
    - Personal_Identity
    - Social_Identity
  - Policy (4)
  - Resource
  - Role (4)
  - Rule

◆ Empty
◆ Ericsson
◆ Pannon
◆ Rel9_Project
◆ Telenor_Rnl

Welcome to Your Content Portal.

This portal contains the content you may access through the STB.

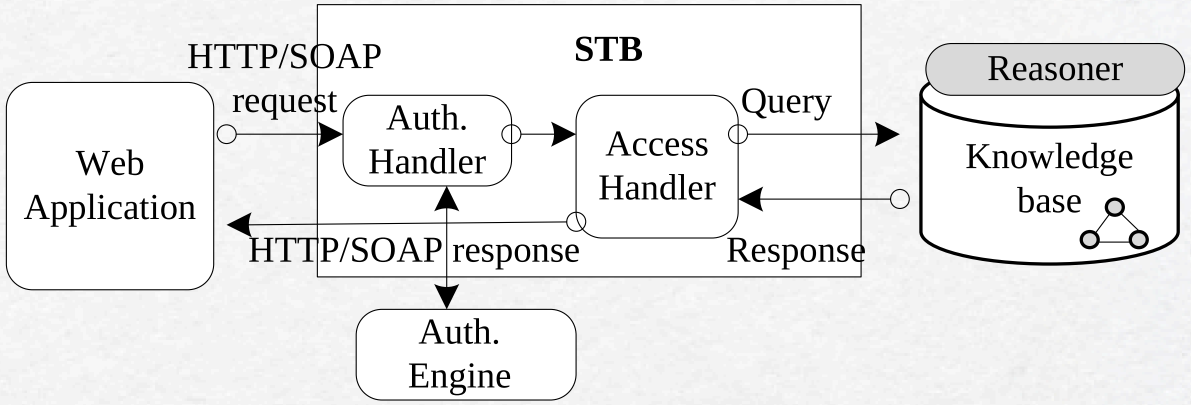
Welcome ALICE!
Click on the content that you would like see.

Content

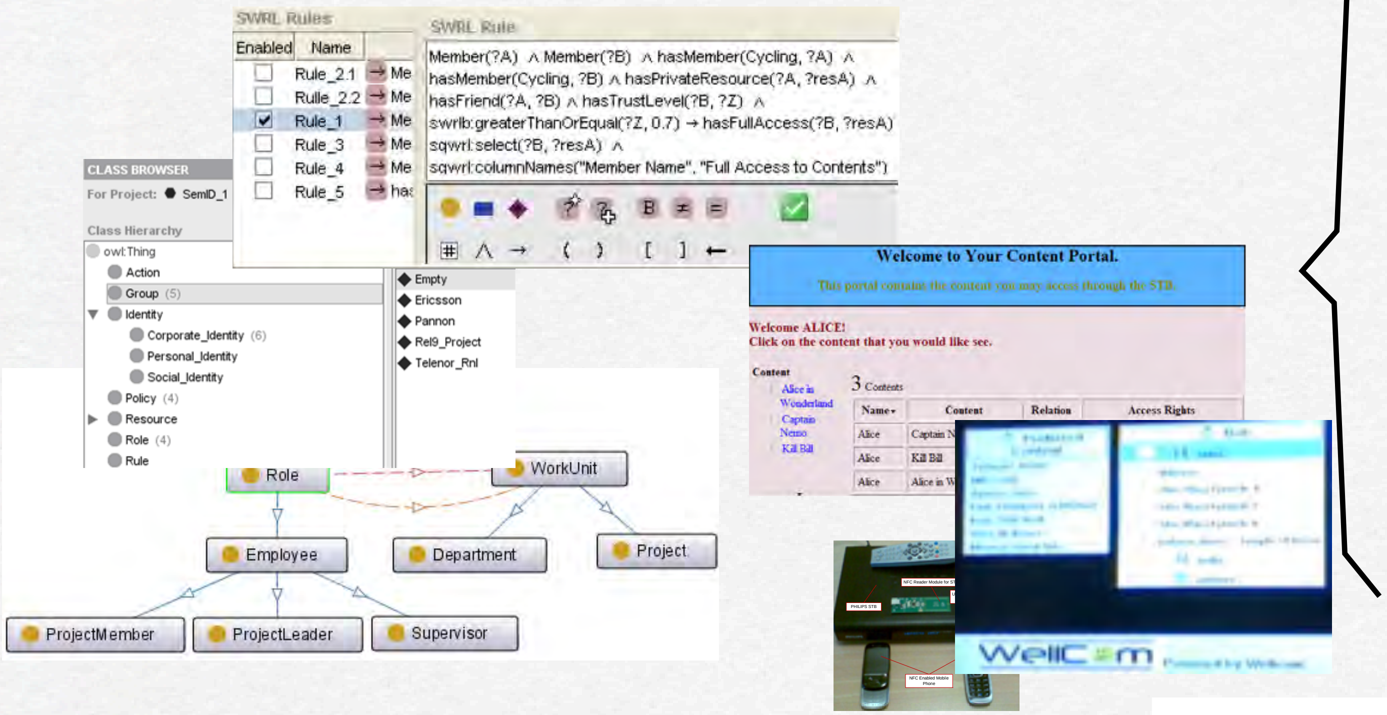
- Alice in Wonderland
- Captain Nemo
- Kill Bill

3 Contents

Name	Content	Relation	Access Rights
Alice	Captain N		
Alice	Kill Bill		
Alice	Alice in W		



Alternative to real time reasoning!



SWRL Rules

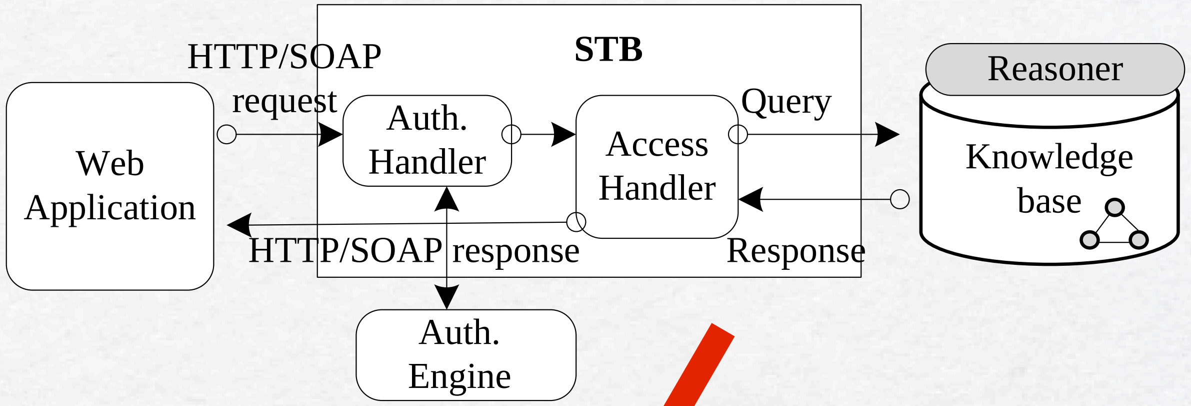
Enabled	Name
□	Rule_2.1
□	Rule_2.2
☑	Rule_1
□	Rule_3
□	Rule_4
□	Rule_5

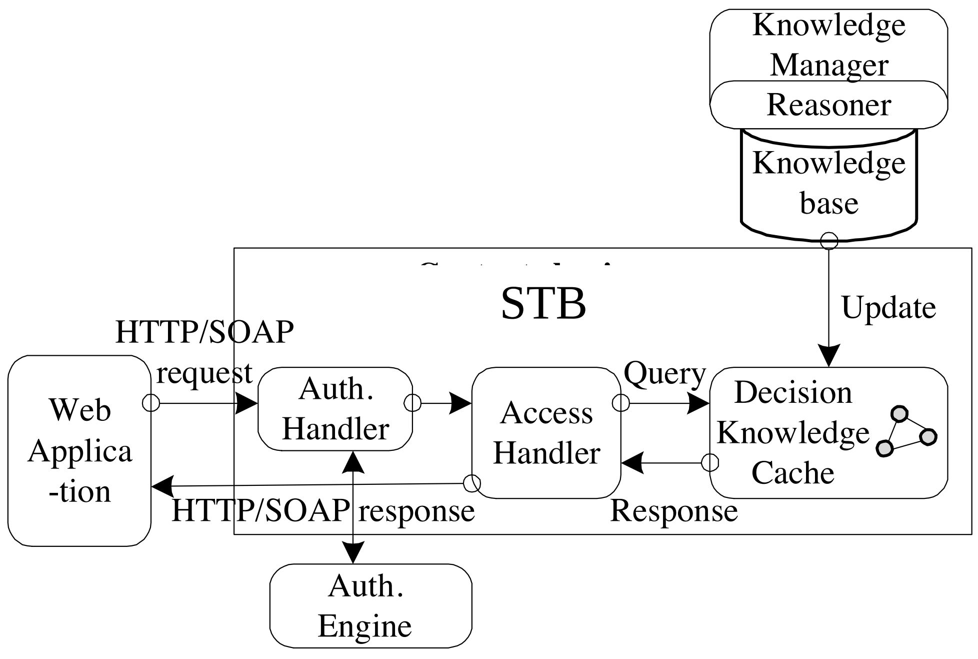
SWRL Rule

```
Member(?A) ∧ Member(?B) ∧ hasMember(Cycling, ?A) ∧
hasMember(Cycling, ?B) ∧ hasPrivateResource(?A, ?resA) ∧
hasFriend(?A, ?B) ∧ hasTrustLevel(?B, ?Z) ∧
swrlb:greaterThanOrEqual(?Z, 0.7) → hasFullAccess(?B, ?resA)
sqwrl:select(?B, ?resA) ∧
sqwrl:columnNames("Member Name", "Full Access to Contents")
```

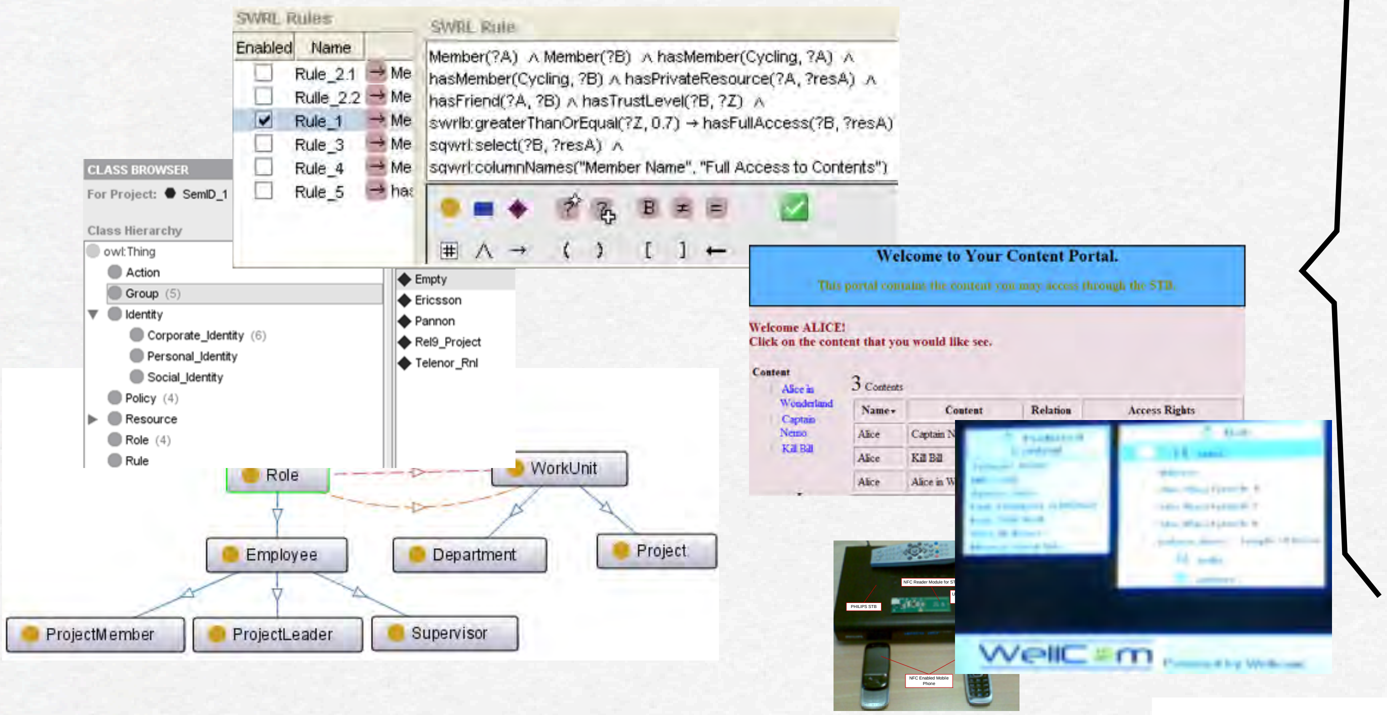
Welcome to Your Content Portal.

Welcome ALICE!
Click on the content that you would like see.





Alternative to real time reasoning!



SWRL Rules

Enabled	Name
□	Rule_2.1
□	Rulle_2.2
☑	Rule_1
□	Rule_3
□	Rule_4
□	Rule_5

SWRL Rule

```
Member(?A) ∧ Member(?B) ∧ hasMember(Cycling, ?A) ∧
hasMember(Cycling, ?B) ∧ hasPrivateResource(?A, ?resA) ∧
hasFriend(?A, ?B) ∧ hasTrustLevel(?B, ?Z) ∧
swrlb:greaterThanOrEqual(?Z, 0.7) → hasFullAccess(?B, ?resA)
sqwrl:select(?B, ?resA) ∧
sqwrl:columnNames("Member Name", "Full Access to Contents")
```

CLASS BROWSER

For Project: ● SemID_1

Class Hierarchy

Welcome to Your Content Portal.

This portal contains the content you may access through the STB.

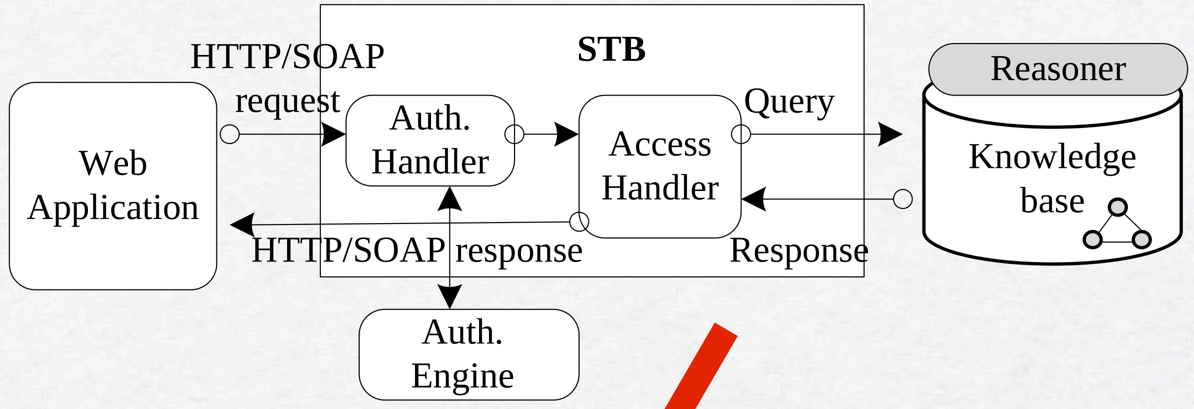
Welcome ALICE!
Click on the content that you would like see.

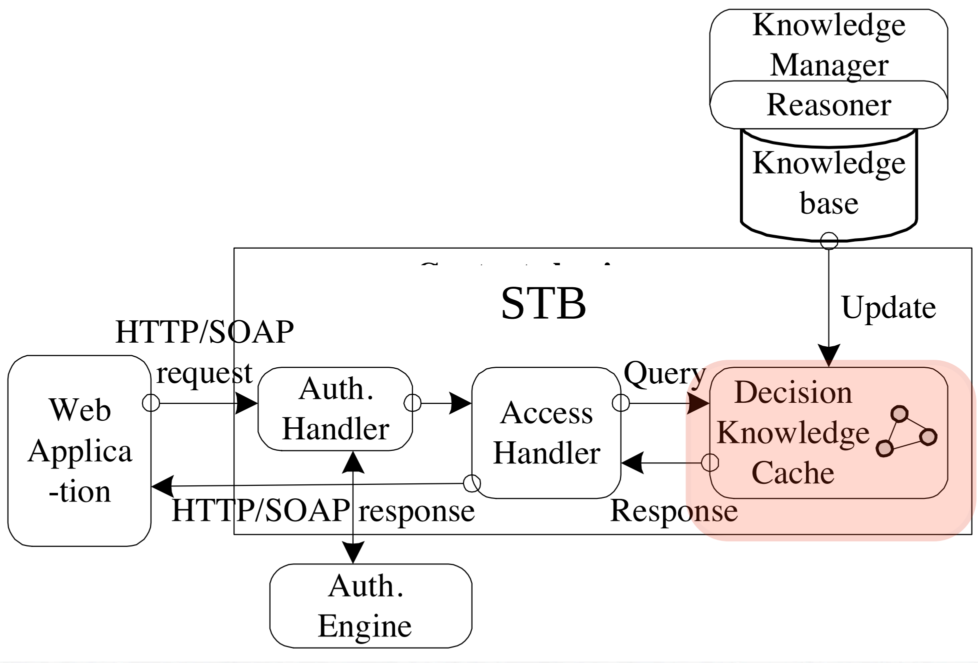
Content

- Alice in Wonderland
- Captain Nemo
- Kill Bill

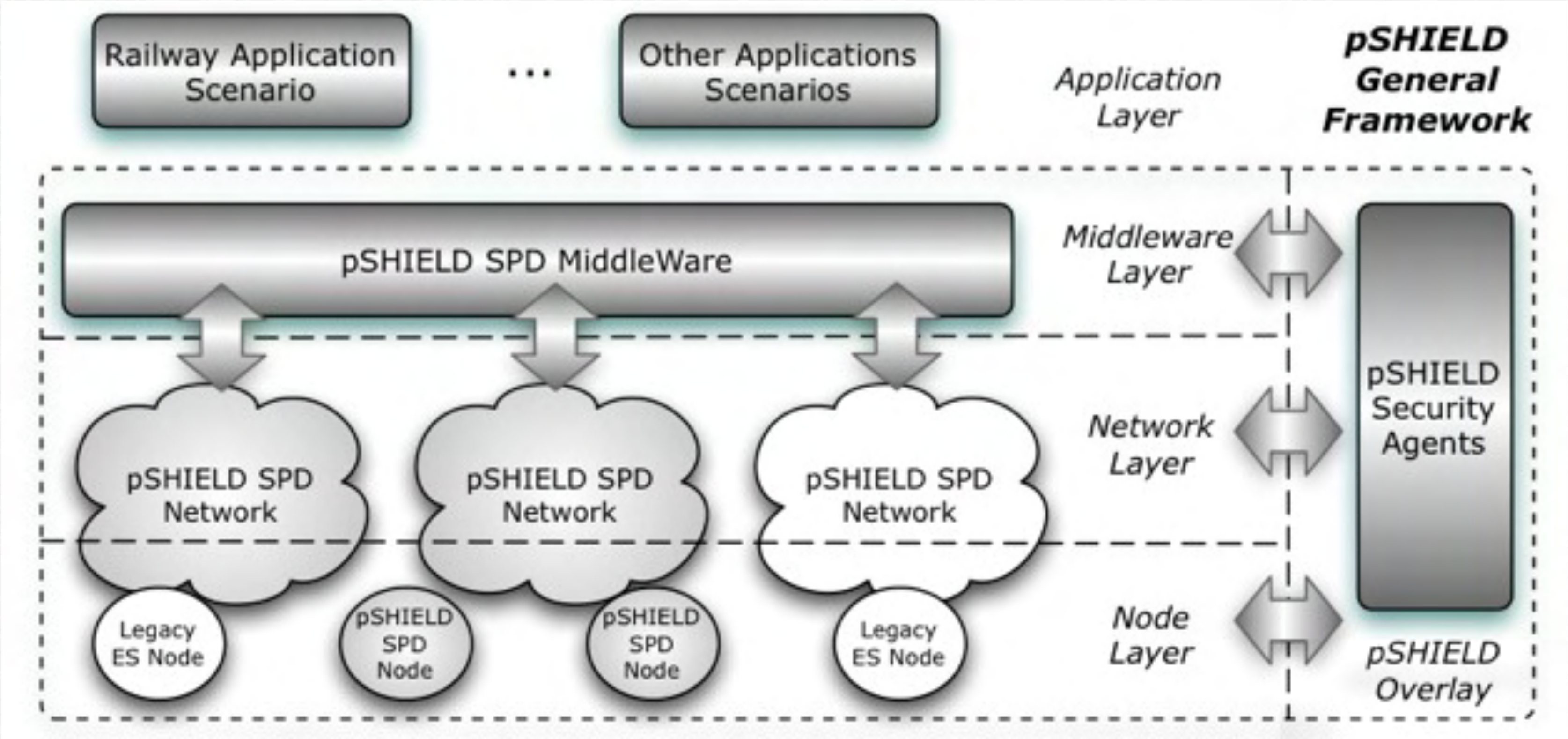
3 Contents

Name	Content	Relation	Access Rights
Alice	Captain N		
Alice	Kill Bill		
Alice	Alice in W		

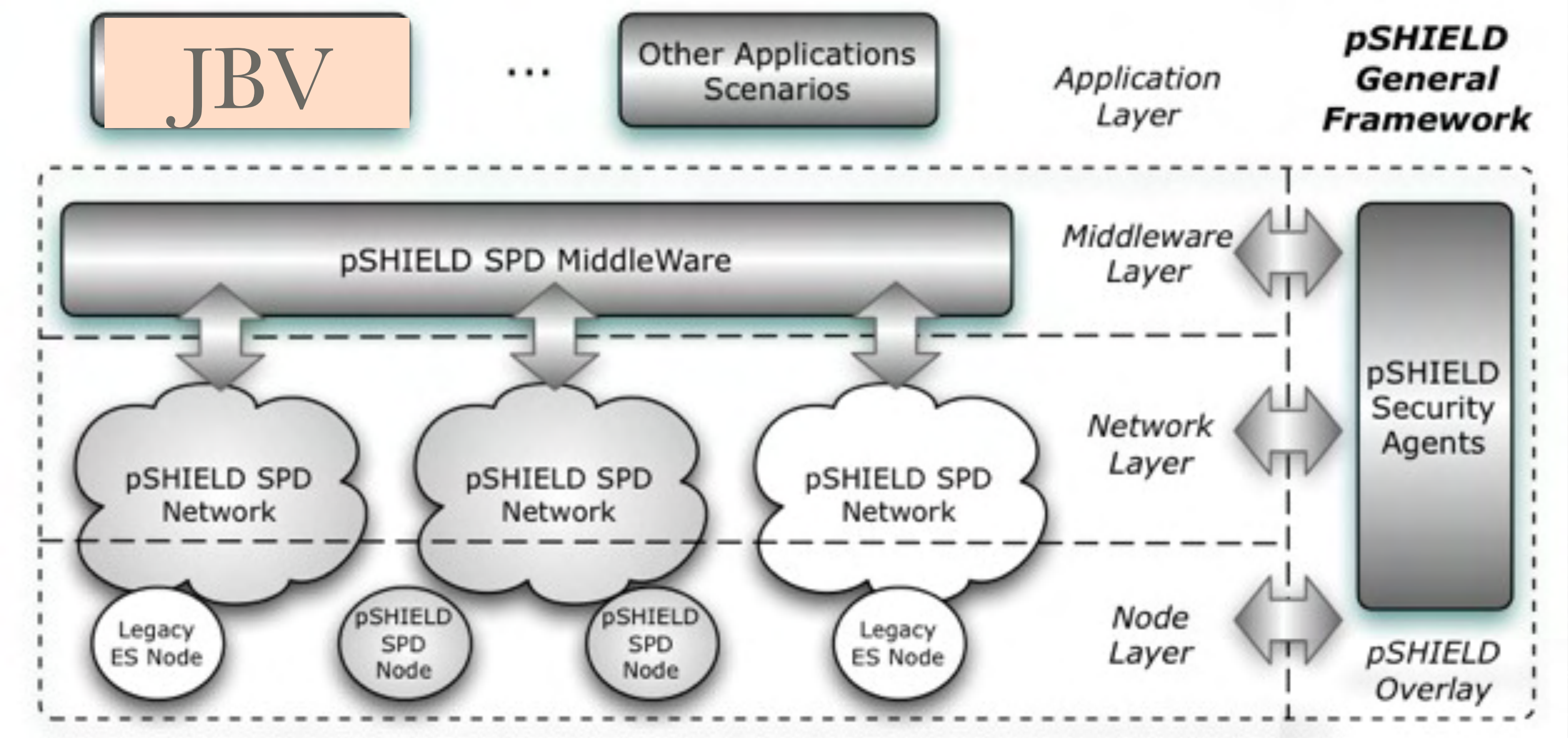




Another use case



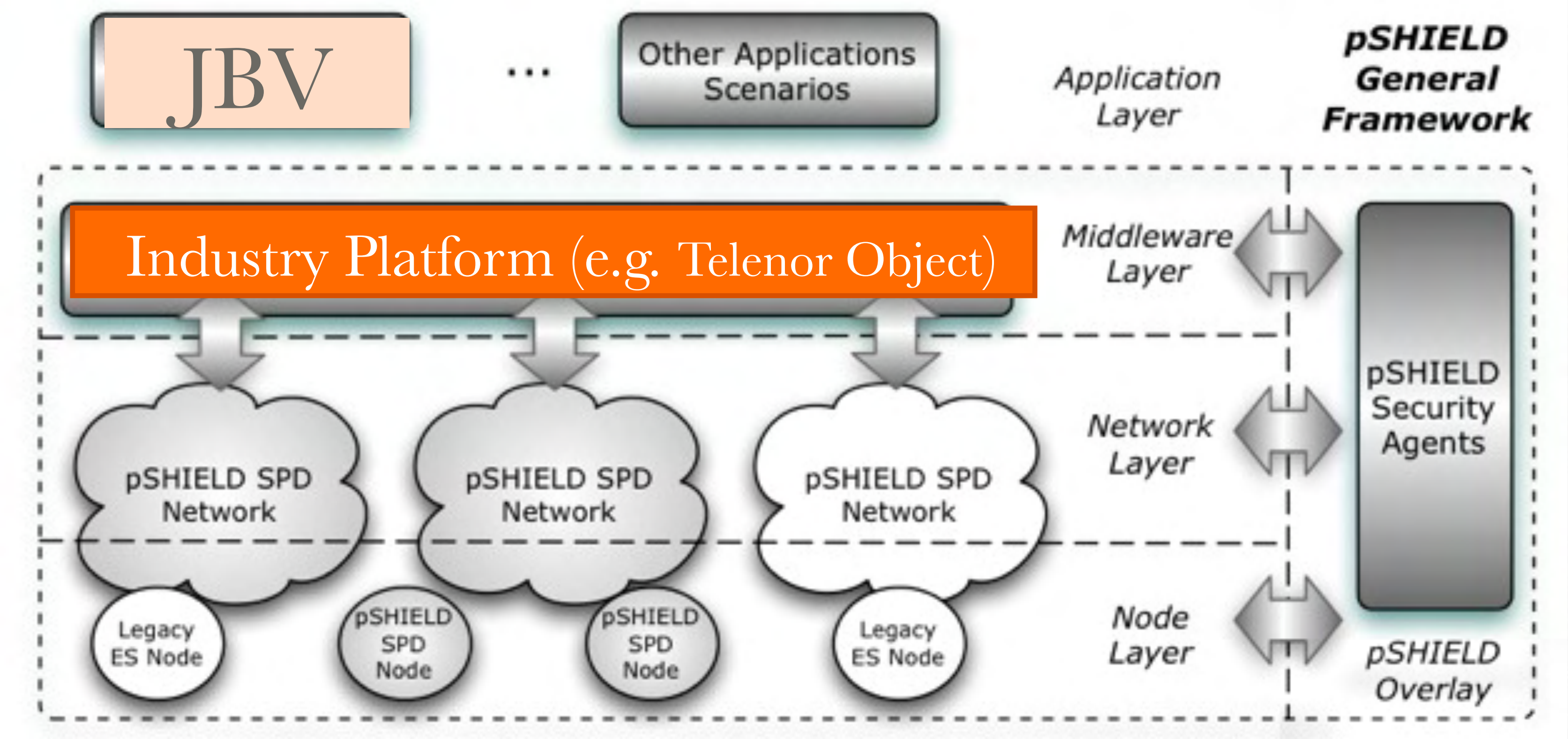
Another use case



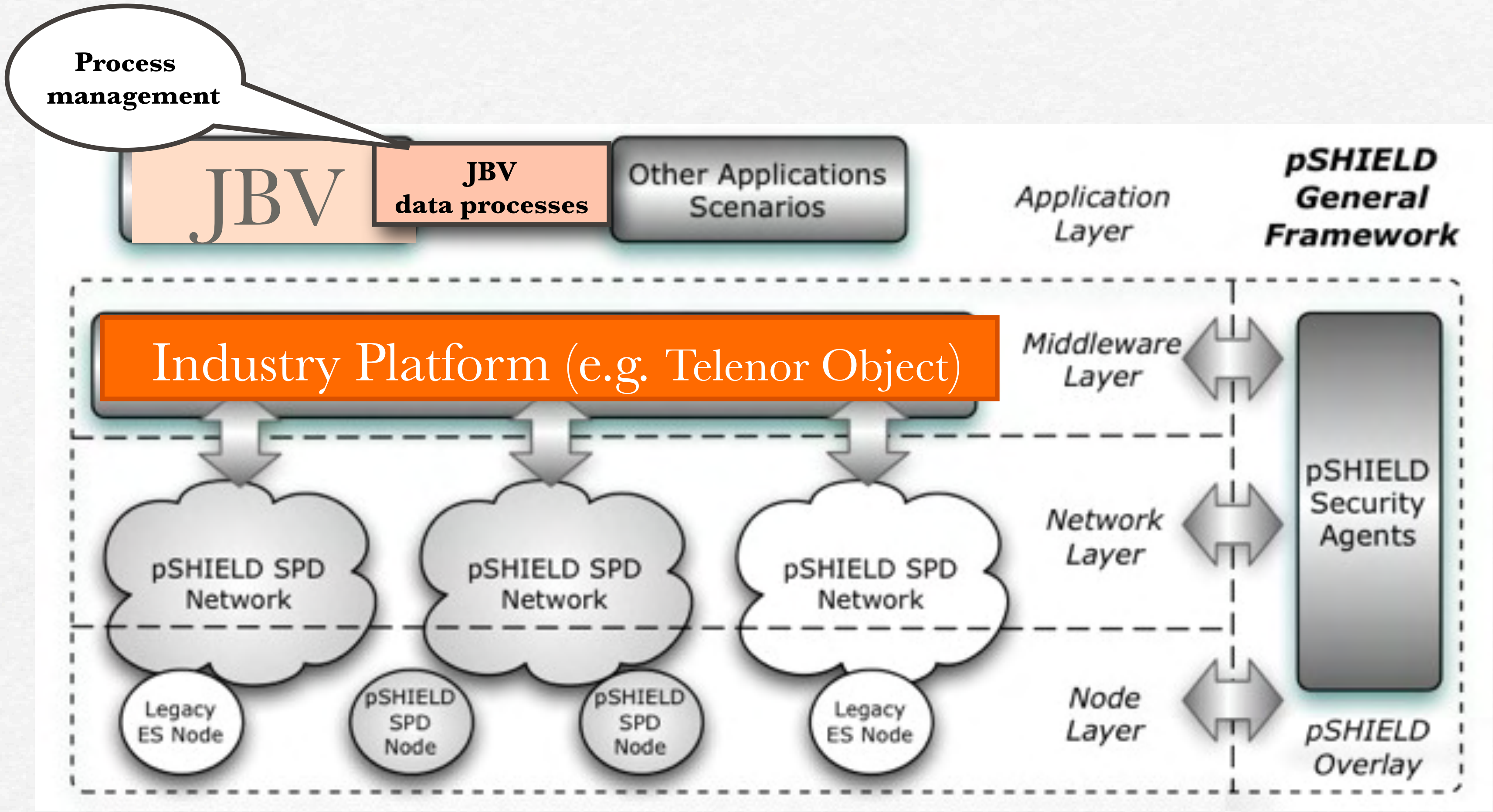
UNIK

Another use case

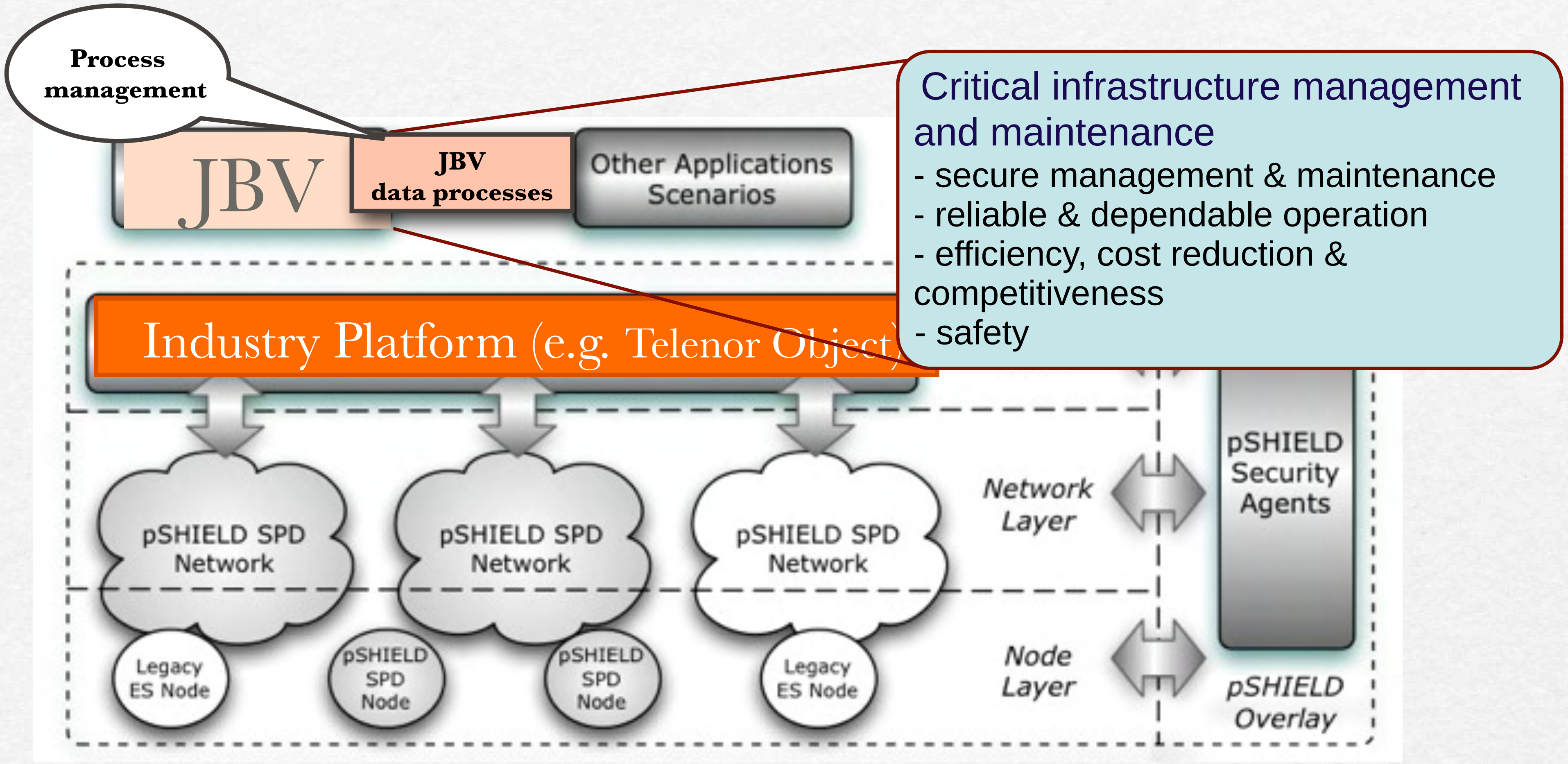
UNIVERSITETET I OSLO



Another use case



Another use case



Critical infrastructure management and maintenance

- secure management & maintenance
- reliable & dependable operation
- efficiency, cost reduction & competitiveness
- safety

State of the art

Approach: Access control models; Policy based access

State of the art

Approach: Access control models; Policy based access

Access control

□ ACL

□ RBAC

□ ABAC

□ CWAC

Policy

□ XACML

□ KAOS

□ Rei

□ WSPL

State of the art

Approach: Access control models; Policy based access

Access control

- □ ACL
- □ RBAC
- □ ABAC
- □ CWAC

Policy

- □ XACML
- □ KAOS
- □ Rei
- □ WSPL

Access control models	Generic	Expressivity	Varying levels of granularity	Scalability	High level specification of constraints	Ability to delegate	Ability to revoke
ACL	Yes	No	No	No	No	No	Yes
RBAC	No	Yes	Yes	No	Yes	Yes	Yes
ABAC	Yes	Yes	Yes	No	Yes	No	No
CWAC	Yes	Yes	Yes	No	Yes	No	No

Policy languages	Well-defined semantics	Monotonicity	Expressiveness of condition	Execution of action	Ability to delegate	Extensibility
EPAL	+	-	+	+	-	+
KAoS	++	+	++	-	-	+
Protune	+	+	+	+	+	+
Ponder	-	-	+	+	+	+
Rei	+	+	++	-	+	+
XACML	-	-	+	+	-	+
WSPL	-	-	+	+	-	-

State of the art

Approach: Access control models; Policy based access

Access control

- □ ACL
- □ RBAC
- □ ABAC
- □ CWAC

Policy

- □ XACML
- □ KAOS
- □ Rei
- □ WSPL

Access control models	Generic	Expressivity	Varying levels of granularity	Scalability	High level specification of constraints	Ability to delegate	Ability to revoke
ACL	Yes	No	No	No	No	No	Yes
RBAC	No	Yes	Yes	No	Yes	Yes	Yes
ABAC	Yes	Yes	Yes	No	Yes	No	No
CWAC	Yes	Yes	Yes	No	Yes	No	No

Policy languages	Well-defined semantics	Monotonicity	Expressiveness of condition	Execution of action	Ability to delegate	Extensibility
EPAL	+	-	+	+	-	+
KAoS	++	+	++	-	-	+
Protune	+	+	+	+	+	+
Ponder	-	-	+	+	+	+
Rei	+	+	++	-	+	+
XACML	-	-	+	+	-	+
WSPL	-	-	+	+	-	-

Summary

- ❐ Semantic technologies can contribute to security and privacy
  - ❐ grant permission through reasoning
- ❐ Introduced some practical use cases
- ❐ Challenges remain
  - ❐ granularity vs complexity
  - ❐ real time reasoning and computation complexity