Semantics-Enabled Web Policies for Privacy Protection and Digital Rights Management: Current Status and Future Trends

Prof.(Dr.) Yuh-Jong Hu

Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan

March-11-2009

NRC IIT Colloquium

Part I

Research Goals

Long Term Research Goals

SemPIF Framework: PIF + Meta-PIF

- SemPIF: : Semantic PIF and Semantics-enabled meta-PIF
- Policy Interchange Format (PIF)
- Meta-PIF
- SemPIF for privacy protection
- SemPIF for DRM
- SemPIF for multiple domains
- SemPIF for policies legalized

Short Term Research Goals

Privacy Protection

Semantics-Enabled privacy protection policies

- Formal semantic model of P3P and EPAL
- Semantic enforcement of privacy protection policies
- Semantics-enabled privacy protection system on the Web

Current Status[15]

- *DL* + *log*-based ontology+rule on P3P
- Ontology-based privacy protection policies
- Rule-based privacy protection policies
- Semantics-enabled of privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL

Short Term Research Goals

Privacy Protection

Semantics-Enabled privacy protection policies

- Formal semantic model of P3P and EPAL
- Semantic enforcement of privacy protection policies
- Semantics-enabled privacy protection system on the Web

Current Status[15]

- *DL* + *log*-based ontology+rule on P3P
- Ontology-based privacy protection policies
- Rule-based privacy protection policies
- Semantics-enabled of privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL

Short Term Research Goals
Digital Rights Management (DRM)

Semantics-Enabled DRM policies

- Formal semantic model of ODRL/XrML
- Semantics-enable of DRM policies
- Semantic enforcement of DRM system on the Web

Current Status[14]

- SWRL-based ontology+rule on ODRL
- Ontology-based usage and delegation rights of DRM
- Rule-based usage and delegation rights of DRM
- DRM policies for fair use of Intellectual Property (IP)

Short Term Research Goals
Digital Rights Management (DRM)

Semantics-Enabled DRM policies

- Formal semantic model of ODRL/XrML
- Semantics-enable of DRM policies
- Semantic enforcement of DRM system on the Web

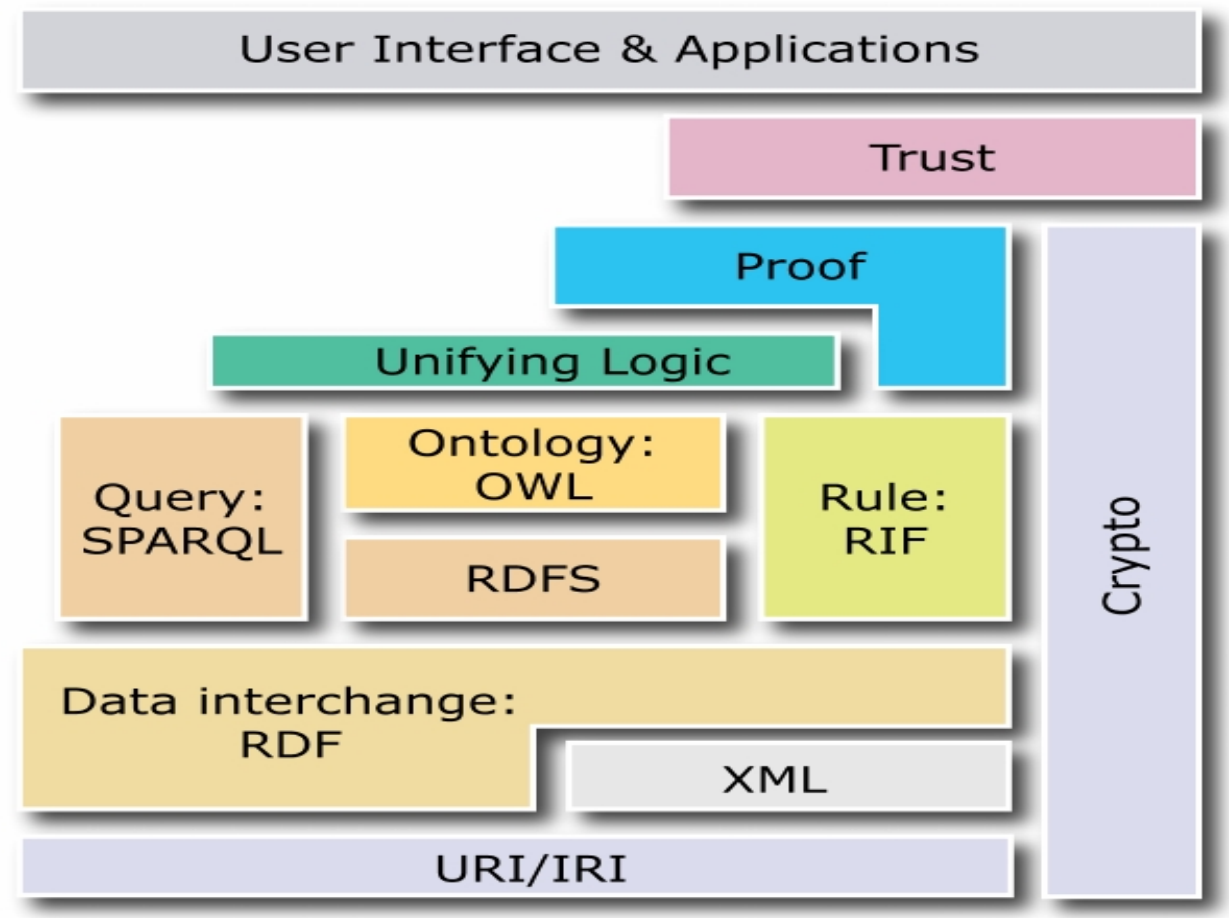
Current Status[14]

- SWRL-based ontology+rule on ODRL
- Ontology-based usage and delegation rights of DRM
- Rule-based usage and delegation rights of DRM
- DRM policies for fair use of Intellectual Property (IP)

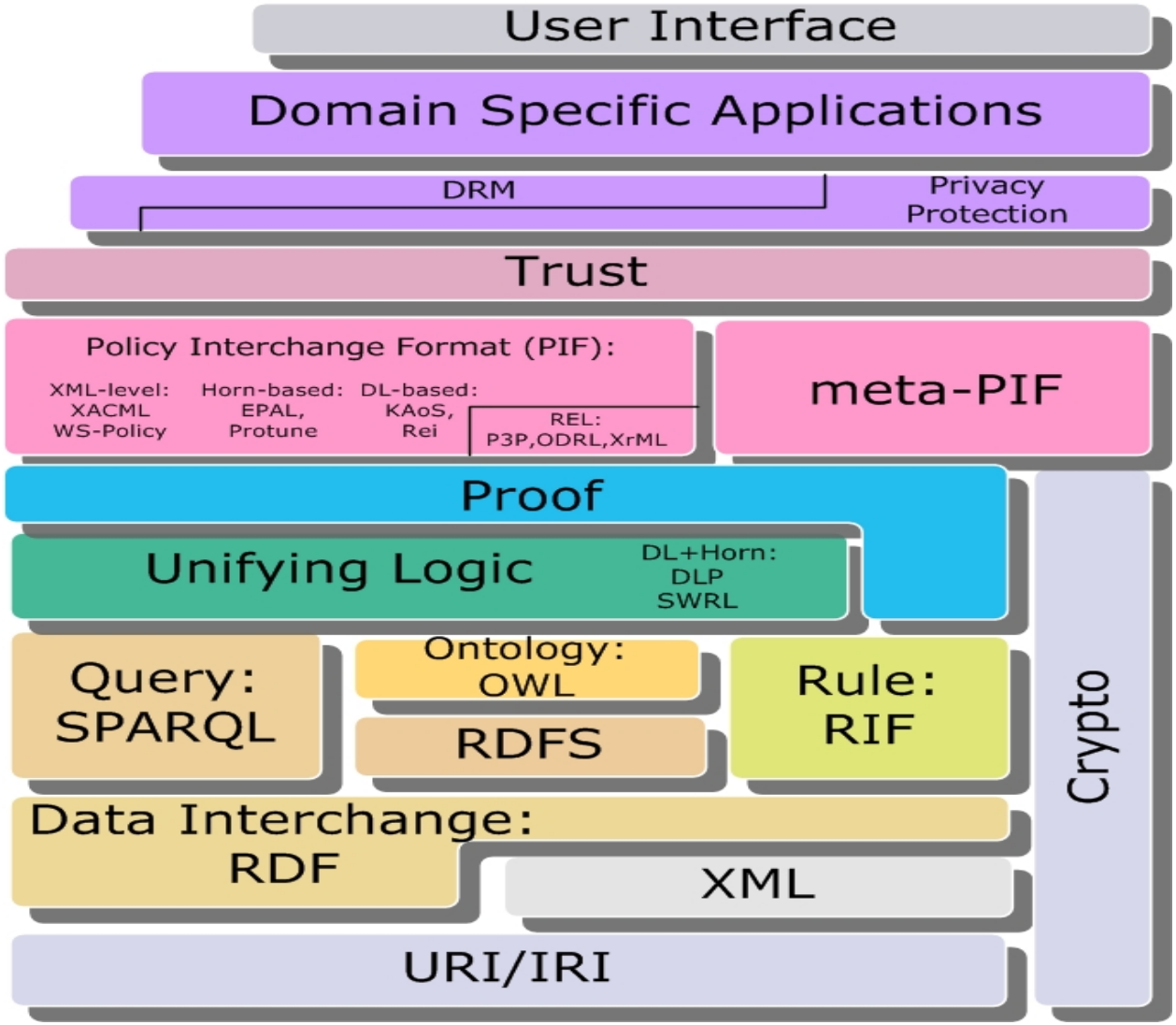
Part II

SemPIF: PIF + Meta-PIF

Well-Known Semantic Web Layer Cake(2007 Version)



SemPIF Extends Semantic Web



SemPIF's Related Work

Where Are Current Available Policy Frameworks?

- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- FP6 IST-ESTRELLA LKIF

What Is the Features of SemPIF

- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- Applying a combination of ontology+rule for PIF and meta-PIF
- SemPIF for various protection domains, e.g. privacy protection and DRM

SemPIF's Related Work

Where Are Current Available Policy Frameworks?

- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- FP6 IST-ESTRELLA LKIF

What Is the Features of SemPIF

- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- Applying a combination of ontology+rule for PIF and meta-PIF
- SemPIF for various protection domains, e.g. privacy protection and DRM

Part III

Semantics-Enabled Web Policies

What Do You Mean Policies?

- Declared as knowledge bases, i.e., ontologies or/and rules
- Reducing program coding to a minimum level
- Enabling automated documentation
- Framework supports policy interoperability
- Low deployment and maintenance cost
- Context of policy is machine understandable
- Maybe supports automatic negotiation between agents

Policy Specification, Enforcement, and Integration, WG I2, REWERSE FP6

What Do You Mean Meta-Policy?

- A policy about policies
- Providing a set of rules to enforce the adding and changing management services of multi-policies
- Setting up priority of polices to coordinate, enforce, and even negotiate multi-policies on the Web

Hosmer, H. H., Metapolicies I, ACM SIGSAC Review, 1992"

XML-based Policy Lacks Semantics

XML-based policies

- XrML [17] $\Leftarrow$ digital rights expression language
- ODRL [16] $\Leftarrow$ digital rights expression language
- P3P [5] $\Leftarrow$ privacy rights expression language
- EP3P(EPAL) [1] $\Leftarrow$ privacy rights expression language
- XACML [1] $\Leftarrow$ general policy language

Pure FOL-based Policy Is Not Web-Enabled

Formal semantics of DL ($\subset$ FOL) or LP for policies

- Semantic ODRL [26] $\Leftarrow$ FOL semantics
- Semantic XrML [10] $\Leftarrow$ FOL semantics
- Semantic P3P [33] $\Leftarrow$ relational semantics
- FAF [18] $\Leftarrow$ LP semantics
- Semantic E-P3P (or EPAL) [1] $\Leftarrow$ FAF semantics
- Rein, KAoS [31] $\Leftarrow$ DL-based FOL semantics
- Protune [3] $\Leftarrow$ LP semantics

Semantics-Enabled Web Policies

Web policies from semantic web languages

- Ontology Languages: RDF(S), OWL-DL, OWL2
- Rules Languages: N3, RuleML, RIF
- Ontology+Rule Language: SWRL, OWL2+RIF

Web policies from ontology+rule

- Policy vs. Regulation (or Law)
- Policy Language vs. Policies
- Semantics-enabled Policy Language
- Semantics-enabled Meta-PIF

Semantics-Enabled Web Policies

Web policies from semantic web languages

- Ontology Languages: RDF(S), OWL-DL, OWL2
- Rules Languages: N3, RuleML, RIF
- Ontology+Rule Language: SWRL, OWL2+RIF

Web policies from ontology+rule

- Policy vs. Regulation (or Law)
- Policy Language vs. Policies
- Semantics-enabled Policy Language
- Semantics-enabled Meta-PIF

Semantics-Enabled Web Policies (conti.)

Why use ontology+rule?

- Exploiting semantic web research
- Two major knowledge representations
- Automatic machine processing of policies
- Choosing which ontology+rule is not easy!

Why not use ontologies or rules alone?

- Policies might be DL-based semantics and LP-based semantics
- Power enhancement of policies from ontologies and rules
- Different knowledge integration, interchange, and interoperation
- Options to use ontologies, rules or both

Semantics-Enabled Web Policies (conti.)

Why use ontology+rule?

- Exploiting semantic web research
- Two major knowledge representations
- Automatic machine processing of policies
- Choosing which ontology+rule is not easy!

Why not use ontologies or rules alone?

- Policies might be DL-based semantics and LP-based semantics
- Power enhancement of policies from ontologies and rules
- Different knowledge integration, interchange, and interoperation
- Options to use ontologies, rules or both

Semantics-Enabled Web Policies (conti.)

Which ontology+rule combination for Web Policies?

- We do not know yet!
- Decidability of computation
- Expressive power of ontology+rule
- Semantics differences between DL and LP
- Uni-(or bi-)directional of knowledge flow
- Homogeneous of ontology+rule
- Heterogeneous (or Hybrid)) of ontology+rule

Semantics-Enabled Web policies

Homogeneous ontology+rule [29]

- CARIN [20] (limited expressive power)
- Description Logic Program (DLP) [8] (too restricted)
- Semantic Web Rule Language(SWRL) [12] (undecidable unless DL-safe rules)

Future Semantics-Enabled Web Policies (conti.)

Hybrid ontology+rule [29]

Positive Datalog rules

- (Disjunctive)AL-log [6] $\Leftarrow$ decidability of *ALC* plus positive, recursive DL-safe rules
- DL-safe rules [23] $\Leftarrow$ decidability of *SHOIN* plus positive, recursive DL-safe rules

Non-monotonic Datalog rules

- DL-log safe hybrid Knowledge Bases [27] $\Leftarrow$ decidability of DLs/FOL plus non-monotonic, recursive DL-safe rules
- DL+log [28] $\Leftarrow$ decidability of arbitrary DLs plus non-monotonic, recursive weakly DL-safe rules
- Hybrid MKNF Knowledge Bases [22] $\Leftarrow$ mixing OWA and CWA reasoning in DL-safe rules

Future Semantics-Enabled Web Policies (conti.)

Hybrid ontology+rule [29]

Positive Datalog rules

- (Disjunctive)AL-log [6] $\Leftarrow$ decidability of *ALC* plus positive, recursive DL-safe rules
- DL-safe rules [23] $\Leftarrow$ decidability of *SHOIN* plus positive, recursive DL-safe rules

Non-monotonic Datalog rules

- DL-log safe hybrid Knowledge Bases [27] $\Leftarrow$ decidability of DLs/FOL plus non-monotonic, recursive DL-safe rules
- DL+log [28] $\Leftarrow$ decidability of arbitrary DLs plus non-monotonic, recursive weakly DL-safe rules
- Hybrid MKNF Knowledge Bases [22] $\Leftarrow$ mixing OWA and CWA reasoning in DL-safe rules

Part IV

Privacy Protection

Privacy Protection on the Web

Privacy Protection on Web 1.0

- Privacy protection policies representation through natural language
- Static personal profile and digital traces
- Information disclosure policies and mechanisms are embedded together
- Does the website comply the policies announcement is unknown!

Privacy Protection on Web 2.0

- APPEL/P3P provides information disclosure's opt-in/opt-out and negotiation mechanisms
- More challenging to protect a variety of dynamic digital traces
- Does the website comply the policies announcement is still unknown!

Privacy Protection on the Web

Privacy Protection on Web 1.0

- Privacy protection policies representation through natural language
- Static personal profile and digital traces
- Information disclosure policies and mechanisms are embedded together
- Does the website comply the policies announcement is unknown!

Privacy Protection on Web 2.0

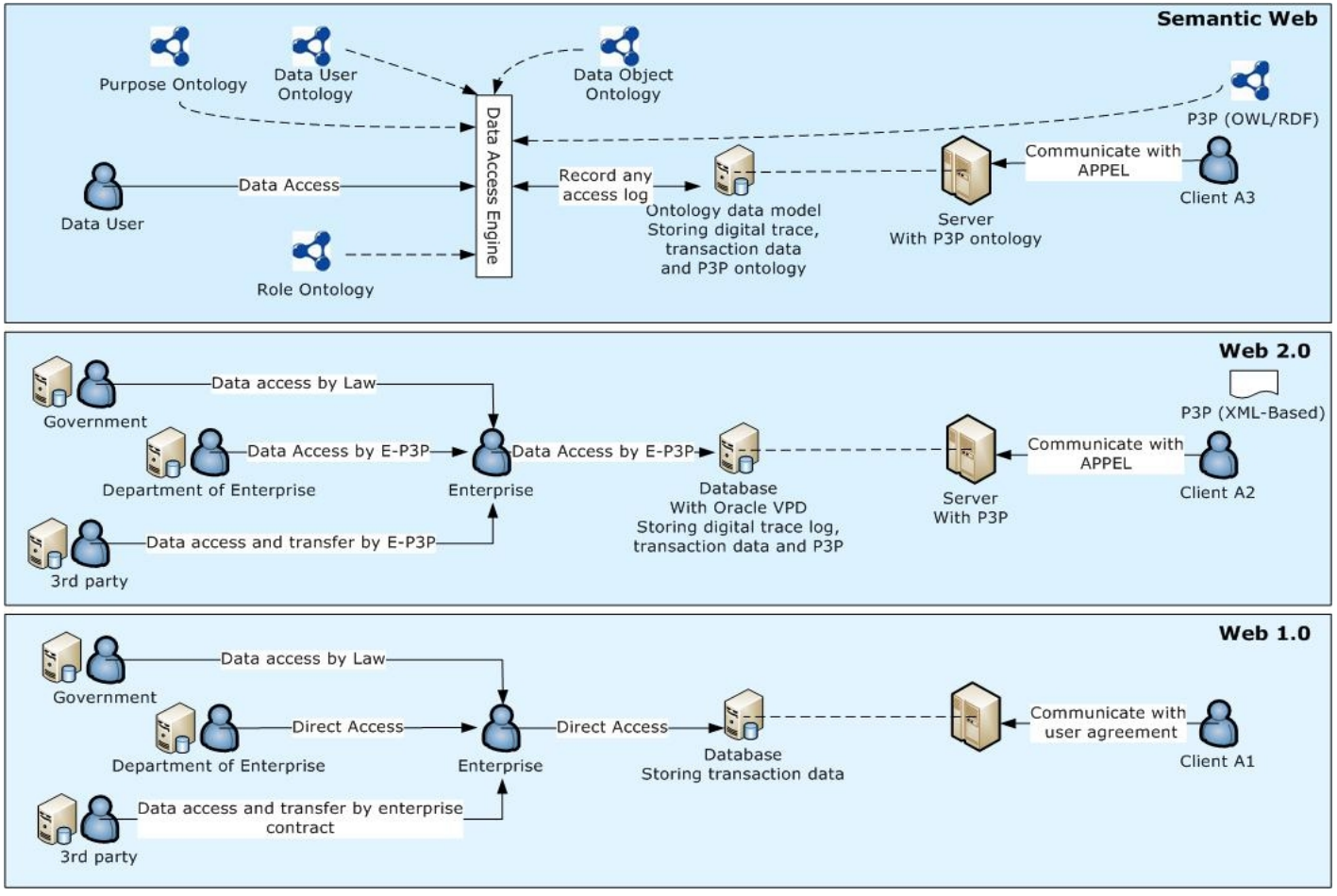
- APPEL/P3P provides information disclosure's opt-in/opt-out and negotiation mechanisms
- More challenging to protect a variety of dynamic digital traces
- Does the website comply the policies announcement is still unknown!

Privacy Protection on the Web

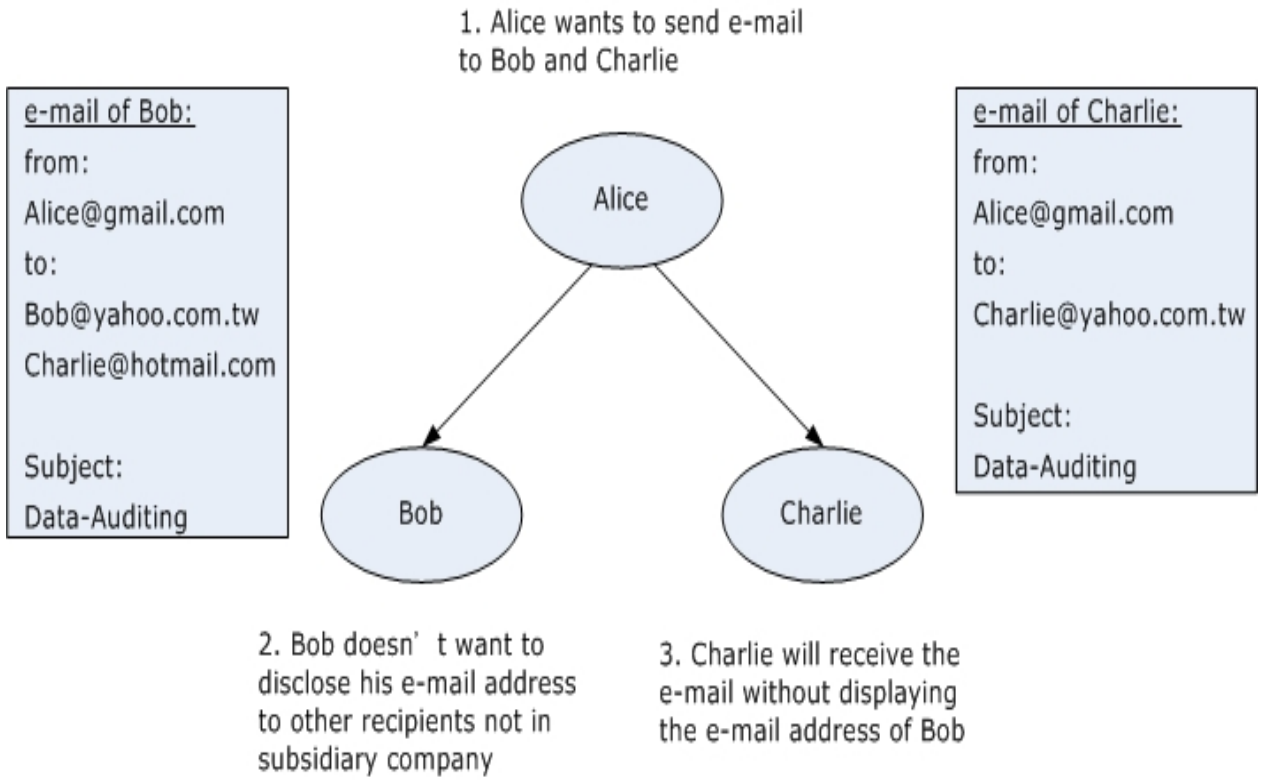
Privacy Protection on Web 3.0

- We have a separation of privacy protection protection policies and mechanisms.
- Personal profile and digital traces are semantics-enabled data model.
- Automatic enforcement of the semantics-enabled privacy protection policies
- Auditing and verifying the compliance of privacy policies to the laws
- Do we need Sound and complete semantics-enabled policies from the legal privacy laws?

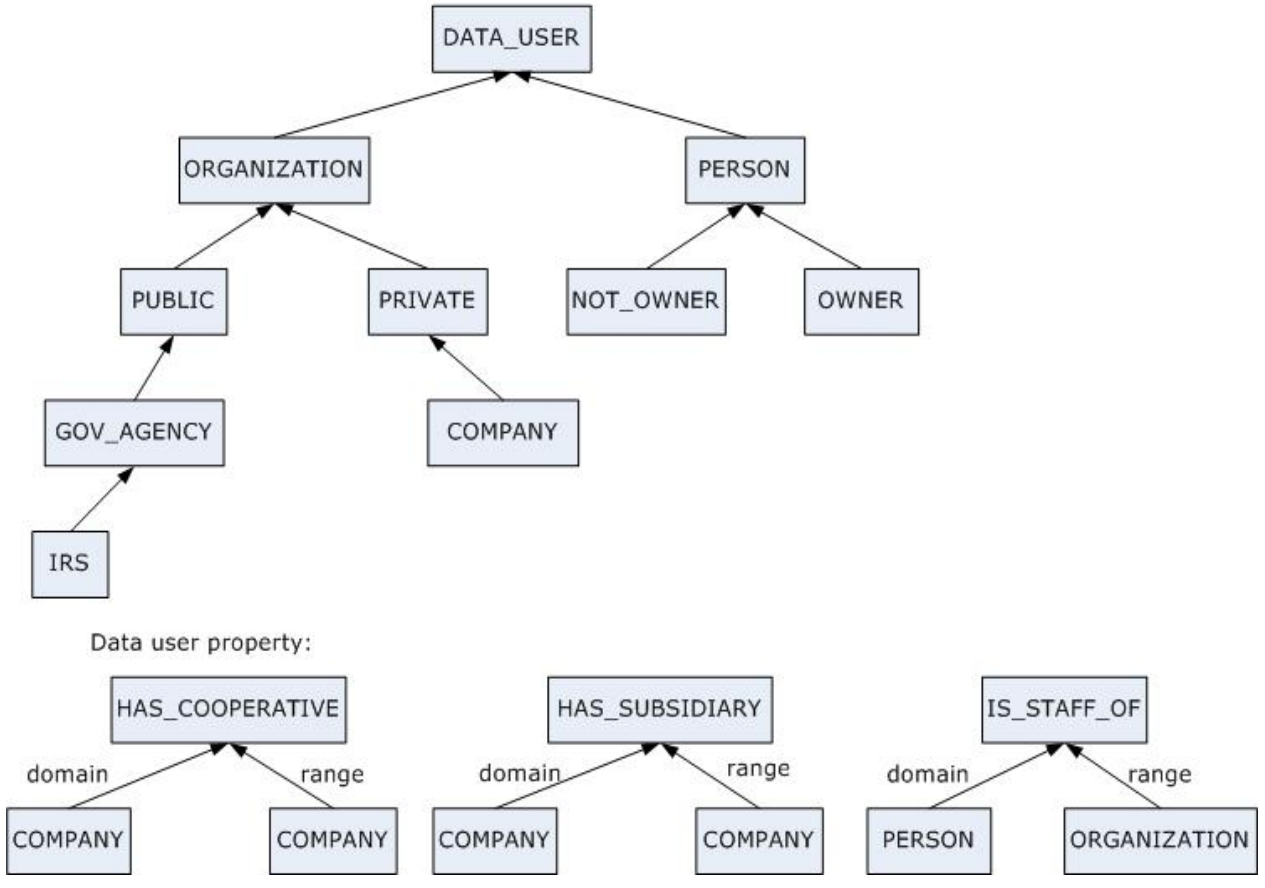
Privacy Protection on Different Web Generations



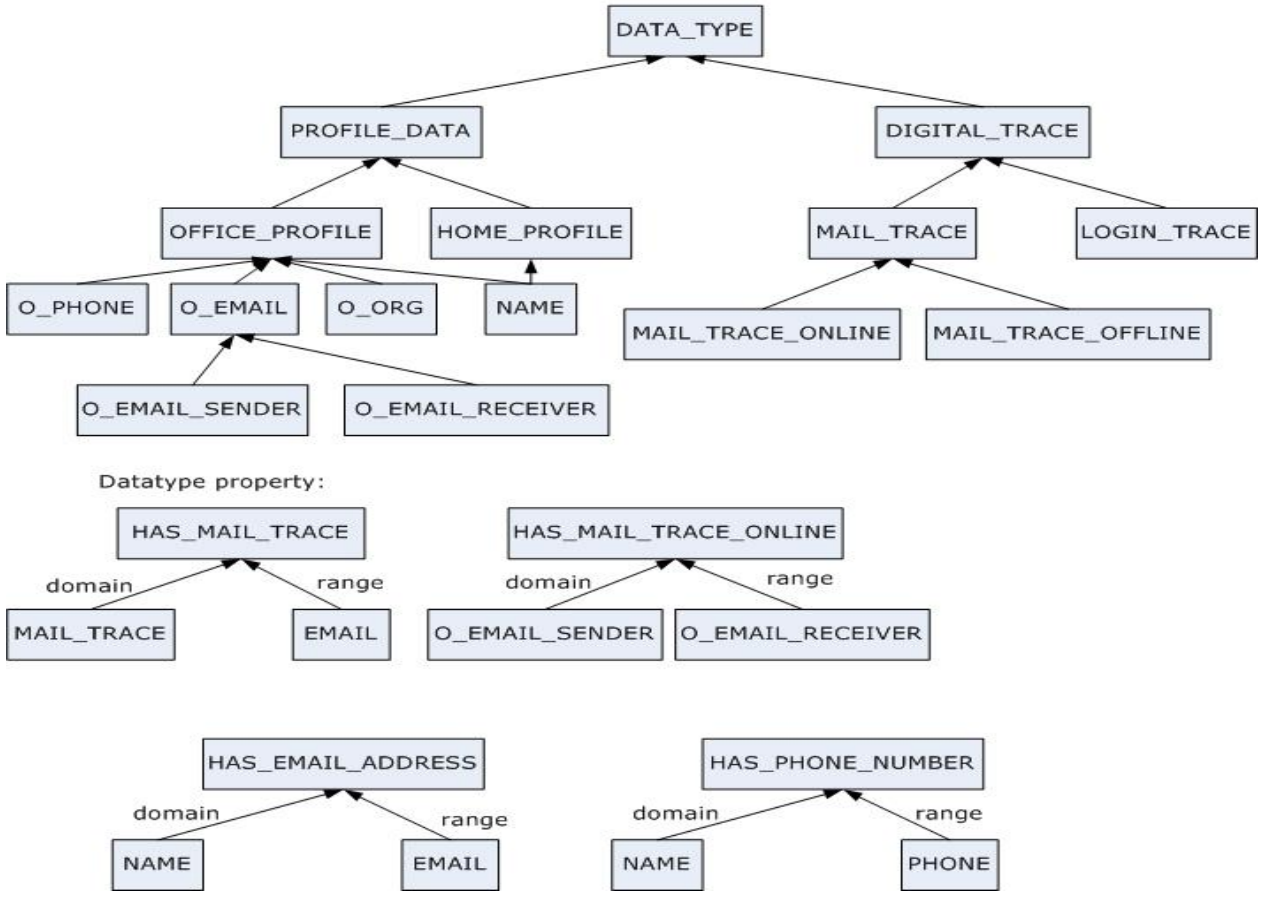
Non-disclosure of recipient's email address



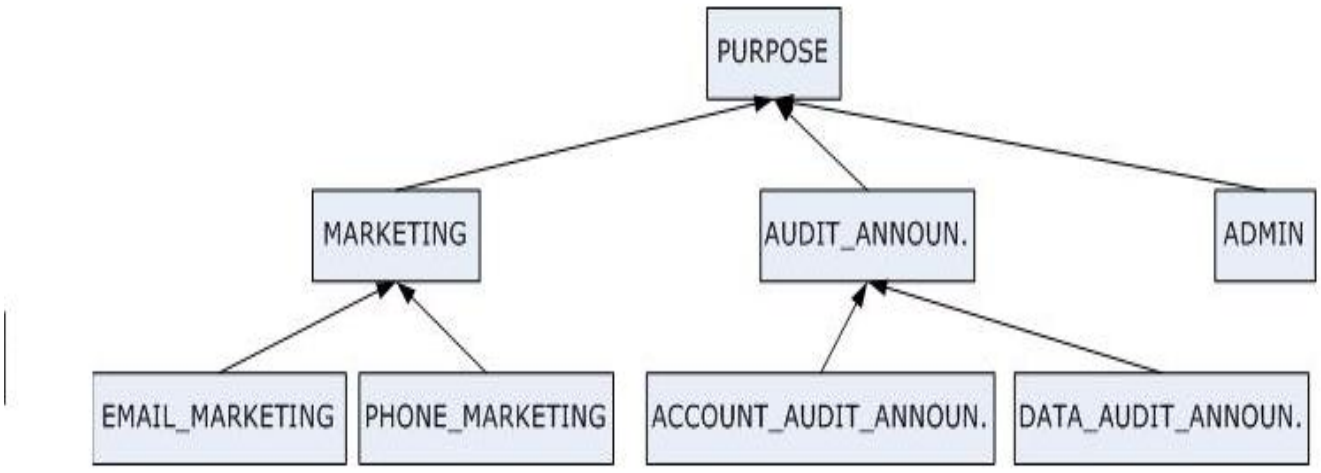
Data User Ontologies (conti.)



Data Type Ontologies (conti.)



Purpose Ontology (conti.)



Ontology Module

Example (Ontology Module's Axiom)

- $COMPANY \sqsubseteq PRIVATE$
- $PRIVATE \sqsubseteq ORGANIZATION$
- $OWNER \sqsubseteq PERSON$
- $COMPANY \overset{domain}{\longleftarrow} HAS\_COOPERATIVE \overset{range}{\longrightarrow} COMPANY$
- $COMPANY \overset{domain}{\longleftarrow} HAS\_SUBSIDIARY \overset{range}{\longrightarrow} COMPANY$
- $HAS\_COOPERATIVE \equiv HAS\_COOPERATIVE^{-}$
- $PERSON \overset{domain}{\longleftarrow} IS\_STAFF\_OF \overset{range}{\longrightarrow} ORGANIZATION$
- $MAIL\_TRACE \overset{domain}{\longleftarrow} HAS\_MAIL\_TRACE \overset{range}{\longrightarrow} EMAIL$
- $EMAIL \sqsubseteq \exists\ HAS\_MAIL\_TRACE\_ONLINE^{-}.O\_EMAIL\_SENDER$
- $EMAIL \sqsubseteq \forall\ HAS\_MAIL\_TRACE\_ONLINE.O\_EMAIL\_RECEIVER$
- $DATA\_AUDIT\_ANNOUN. \sqsubseteq AUDIT\_ANNOUN.$

Ontology Module

Example (Ontology Module's Axiom)

- $COMPANY \sqsubseteq PRIVATE$
- $PRIVATE \sqsubseteq ORGANIZATION$
- $OWNER \sqsubseteq PERSON$
- $COMPANY \overset{domain}{\longleftarrow} HAS\_COOPERATIVE \overset{range}{\longrightarrow} COMPANY$
- $COMPANY \overset{domain}{\longleftarrow} HAS\_SUBSIDIARY \overset{range}{\longrightarrow} COMPANY$
- $HAS\_COOPERATIVE \equiv HAS\_COOPERATIVE^{-}$
- $PERSON \overset{domain}{\longleftarrow} IS\_STAFF\_OF \overset{range}{\longrightarrow} ORGANIZATION$
- $MAIL\_TRACE \overset{domain}{\longleftarrow} HAS\_MAIL\_TRACE \overset{range}{\longrightarrow} EMAIL$
- $EMAIL \sqsubseteq \exists\ HAS\_MAIL\_TRACE\_ONLINE^{-}.O\_EMAIL\_SENDER$
- $EMAIL \sqsubseteq \forall\ HAS\_MAIL\_TRACE\_ONLINE.O\_EMAIL\_RECEIVER$
- $DATA\_AUDIT\_ANNOUN. \sqsubseteq AUDIT\_ANNOUN.$

Ontology Module

Example (Ontology Module's Facts)

- *ORGANIZATION(G)*
- *HAS_SUBSIDIARY(G, J-Corp.)*
- *HAS_COOPERATIVE(G, Q-Corp.)*
- *IS_STAFF_OF(Alice, J-Corp.)*
- *IS_STAFF_OF(Bob, J-Corp.)*
- *IS_STAFF_OF(Charlie, Q-Corp.)*
- *HAS_EMAIL_ADDRESS (Charlie,Charlie@hotmail.com)*
- *O_EMAIL_RECEIVER(Bob@yahoo.com.tw)*
- *HAS_EMAIL_ADDRESS (Alice,Alice@gmail.com)*
- *HAS_EMAIL_ADDRESS (Bob,Bob@yahoo.com.tw)*
- *O_EMAIL_SENDER(Alice@gmail.com),*
- *O_EMAIL_RECEIVER (Charlie@hotmail.com)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Bob@yahoo.com.tw)*
- *HAS_MAIL_TRACE_ONLINE (Alice@gmail.com,Charlie@hotmail.com)*

Rule Module

Example (Rule Module's Rules)

- *cando(?c,?b-email, display)*
  ⟸ opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b),
  HAS_EMAIL_ADDRESS(?b,?b-email). ← (a1)
- *cando(?c,?b-email, nill)*
  ⟸ opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b),
  HAS_EMAIL_ADDRESS(?b, ?b-email). ← (a2)
- *opt-in(?b,?b-email,?p)*
  ⟸ data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_SUBSIDIARY(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). ← (a3)
- *opt-out(?b,?b-email,?p)*
  ⟸ data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_COOPERATIVE(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). ← (a4)

Rule Module

Example (Rule Module's Rules)

- *cando(?c,?b-email, display)*
  ⟸ opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b),
  HAS_EMAIL_ADDRESS(?b,?b-email). ← (a1)
- *cando(?c,?b-email, nill)*
  ⟸ opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b),
  HAS_EMAIL_ADDRESS(?b, ?b-email). ← (a2)
- *opt-in(?b,?b-email,?p)*
  ⟸ data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_SUBSIDIARY(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). ← (a3)
- *opt-out(?b,?b-email,?p)*
  ⟸ data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email),
  IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_COOPERATIVE(?c1,?c2),
  HAS_MAIL_TRACE_ONLINE(?a-email,?c-email),
  O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email). ← (a4)

Rule Module

Example (Rule Module's Facts)

- *data-user(Bob), data-owner(Bob),*
- *data-user(Charlie), data-owner(Charlie),*
- *purpose(data-auditing),*
- *data-type(Bob@yahoo.com.tw),*
- *data-type(Charlie@hotmail.com),*
- *opt-in(c,Charlie@yahoo.com, data-auditing),*
- *cando(Bob,Charlie@yahoo.com,display),*
- *cando(Charlie,Bob@yahoo.com.tw,nill),*
- *opt-out(b,Bob@yahoo.com.tw, data-auditing)*

Part V

Digital Rights Management

Agreement for Usage (Transfer) Rights

Definition (license agreement)

A principal $Prin_o$ allows another principal $Prin_{u_i}$ to use an asset r presumably owned by $Prin_o$, where $Prin_o$ is an asset owner, $Prin_{u_i}$ is one of n asset users, where $i \in (1, \cdots, n)$.

Prerequisites Expressions

Definition (prerequisites of agreement)

A prerequisite is either a constraint, a requirement, or a condition of rights agreement. If all of the prerequisites are met, then policies say that the agreement's users may perform the action for the license agreement's assets.

Definition (prerequisites as ontology expressions)

- $MaxCardinality{:}\leq_{\exists u}\ hasUsageCount_{\exists p}.Asset$
- $MaxCardinality{:}\ \leq_{\exists t}\ hasTransferCount_{\exists p}.Asset$
- $Cardinality{:}\ =_{\exists a}\ hasPrepaid_{\exists p}.Party$
- $Validity\ of\ time\ interval\ \forall Time \in (t_1, t_2){:}$
  $\geq_{\exists t_1}\ hasDateTime_{\exists p}.Time \wedge \exists \leq_{t_2}\ hasDateTime_{\exists p}.Time$

Prerequisites Expressions

Definition (prerequisites of agreement)

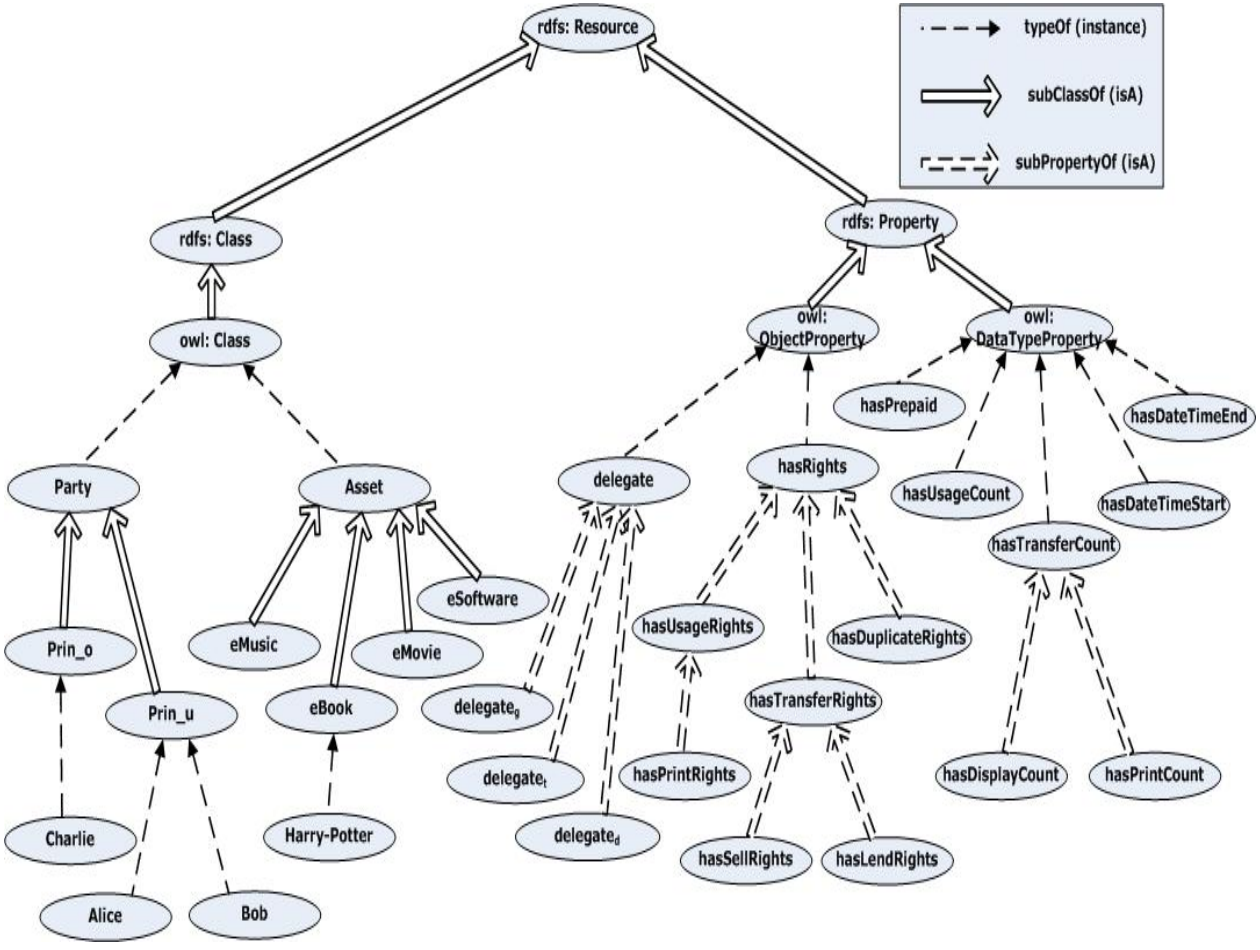
A prerequisite is either a constraint, a requirement, or a condition of rights agreement. If all of the prerequisites are met, then policies say that the agreement's users may perform the action for the license agreement's assets.

Definition (prerequisites as ontology expressions)

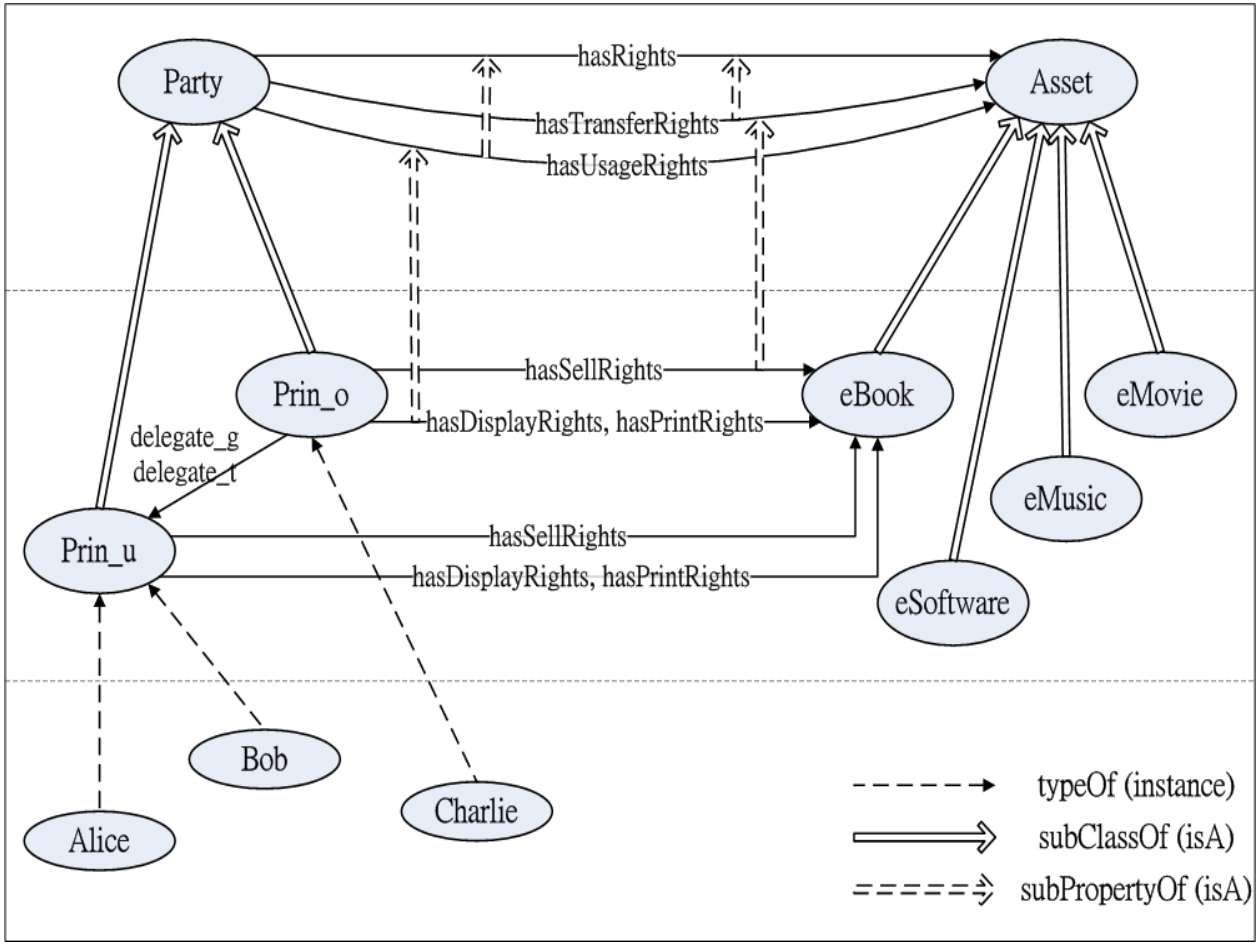
- *MaxCardinality:* $\leq_{\exists u}$ $hasUsageCount_{\exists p}.Asset$
- *MaxCardinality:* $\leq_{\exists t}$ $hasTransferCount_{\exists p}.Asset$
- *Cardinality:* $=_{\exists a}$ $hasPrepaid_{\exists p}.Party$
- *Validity of time interval* $\forall Time \in (t_1, t_2)$*:*

  $\geq_{\exists t_1}$ $hasDateTime_{\exists p}.Time \wedge \exists \leq_{t_2}$ $hasDateTime_{\exists p}.Time$

A Rights Delegation Ontology



A Rights Delegation Snapshot



Rights Delegation Policies

Definition (usage (or transfer) rights delegation)

The class and property terms in this rights delegation ontology will be considered as antecedents or conclusion(s) in the usage and transfer rights delegation rules to enforce real rights delegation inference.

Transfer Rights Delegation

Definition (*hasTransferRights*)

- *hasTransferRights* is an abstract property describing the transfer rights delegation of usage rights.
- The domain class of *hasTransferRights* is *Party* and the range class is *Asset*.

Definition ($delegate_g$ and $delegate_t$)

- $Prin_o$ might use $delegate_g$ to transfer usage rights only to $Prin_{u_i}$, but does not delegate his transfer rights.
- $Prin_o$ might use $delegate_t$ for both usage and transfer rights to propagate further.

Transfer Rights Delegation

Definition (*hasTransferRights*)

- *hasTransferRights* is an abstract property describing the transfer rights delegation of usage rights.
- The domain class of *hasTransferRights* is *Party* and the range class is *Asset*.

Definition ($delegate_g$ and $delegate_t$)

- $Prin_o$ might use $delegate_g$ to transfer usage rights only to $Prin_{u_i}$, but does not delegate his transfer rights.
- $Prin_o$ might use $delegate_t$ for both usage and transfer rights to propagate further.

Rules for Rights Transfer Delegation

Definition (rules for usage rights delegation)

- $hasUsageRights(?x, ?r) \wedge hasTransferRights(?x, ?r) \Longrightarrow hasUsageTransferRights(?x, ?r) \Leftarrow (o1)$
- $hasUsageTransferRights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \wedge <_{\exists u} hasUsageCount(?r) \Longrightarrow hasUsageRights(?y, ?r) \Leftarrow (o2)$

Definition (rules for transfer rights delegation)

- $hasUsageRights(?x, ?r) \wedge <_{\exists u} hasUsageCount(?r) \wedge \geq_{\exists t_1} hasDateTime(?t) \wedge \leq_{\exists t_2} hasDateTime(?t) \Longrightarrow Permitted(Usage, ?r) \Leftarrow (o3)$
- $hasUsageTransferRights(?x, ?r) \wedge delegate_t(?x, ?y) \wedge hasPrepaid(?y, ?a) \wedge \geq_1 hasTransferCount(?r) \Longrightarrow hasUsageTransferRights(?y, ?r) \Leftarrow (o4)$

Rules for Rights Transfer Delegation

Definition (rules for usage rights delegation)

- $hasUsageRights(?x, ?r) \wedge hasTransferRights(?x, ?r) \Longrightarrow hasUsageTransferRights(?x, ?r) \Leftarrow (o1)$
- $hasUsageTransferRights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \wedge <_{\exists u} hasUsageCount(?r) \Longrightarrow hasUsageRights(?y, ?r) \Leftarrow (o2)$

Definition (rules for transfer rights delegation)

- $hasUsageRights(?x, ?r) \wedge <_{\exists u} hasUsageCount(?r) \wedge \geq_{\exists t_1} hasDateTime(?t) \wedge \leq_{\exists t_2} hasDateTime(?t) \Longrightarrow Permitted(Usage, ?r) \Leftarrow (o3)$
- $hasUsageTransferRights(?x, ?r) \wedge delegate_t(?x, ?y) \wedge hasPrepaid(?y, ?a) \wedge \geq_1 hasTransferCount(?r) \Longrightarrow hasUsageTransferRights(?y, ?r) \Leftarrow (o4)$

Natural Language of License Agreement

Example

Content distributor Charlie c makes an agreement with two content consumers, Alice a and Bob b. After each paying five dollars, and then both receiving acknowledgement from Charlie, Alice and Bob are given the usage rights and may each display an eBook asset, Harry Potter and the Deathly Hallows, up to five times. They may each print it only once. However, the total number of actions, either displays or prints done by Alice and Bob, may be at most ten. The usage rights validity period is between 2007/05/07/09:00 - 2007/05/10/24:00.

Abstract Syntax of License Agreement

Example

agreement
between Charlie and {Alice,Bob}
about Harry Potter and the Deathly Hallows
with inSequence[prePay[5.00],attribution[Charlie]]
$\Longrightarrow$ *not[and[Time* $<$ *2007/05/07/09:00,*
Time $>$ *2007/05/10/24:00]]* $\Longrightarrow$ *with count[10]*
$\Longrightarrow$ *and[forEachMember[Alice,Bob;count[5]]*
$\Longrightarrow$ *display, forEachMember[Alice,Bob;count[1]]*
$\Longrightarrow$ *print]*

FOL of License Agreement

Example

$$\forall x((x = Alice \vee x = Bob) \Longrightarrow \exists t_1 \exists t_2 (t_1 < t_2 \wedge Paid(5, t_1) \wedge Attributed(Charlie, t_2))) \Longrightarrow$$
$$\forall t \wedge hasDateTime(t) \geq 2007/05/07/09:00 \wedge hasDateTime(t) \leq 2007/05/10/24:00 \Longrightarrow$$
$$count(Alice, id_1) + count(Alice, id_2) + count(Bob, id_1) + count(Bob, id_2) < 10 \Longrightarrow$$
$$(count(Alice, id_1) < 5 \wedge count(Bob, id_1) < 5 \Longrightarrow \textbf{Permitted}(x, display, ebook)) \wedge$$
$$(count(Alice, id_2) < 1 \wedge count(Bob, id_2) < 1 \Longrightarrow \textbf{Permitted}(x, print, ebook)))$$

Ontologies for License Agreement

Example (Ontology for content distributor Charlie)

- $\mathit{hasDisplayRights} \sqsubseteq \mathit{hasUsageRights}$
- $\mathit{hasPrintRights} \sqsubseteq \mathit{hasUsageRights}$
- $\leq (\mathit{hasDisplayCount}_{\{a,b\}}.\mathit{eBook},\ \mathit{hasUsageCount}_c.\mathit{eBook})$
- $\leq (\mathit{hasPrintCount}_{\{a,b\}}.\mathit{eBook},\ \mathit{hasUsageCount}_c.\mathit{eBook})$
- $\{\mathit{Alice}, \mathit{Bob}\} \overset{domain}{\Leftarrow} \mathit{hasUsageRights} \overset{range}{\longrightarrow} R_1$, where $R_1 = \leq_{10} \mathit{hasUsageCount}_c \wedge \geq_{2007/05/07/0900} \mathit{hasDateTime}_c.\mathit{Time} \wedge \leq_{2007/05/10/2400} \mathit{hasDateTime}_c.\mathit{Time}$
- $\exists =_\alpha \exists = \mathit{sum}(\exists \leq_5 \mathit{hasDisplayCount}_i.\{\mathit{HarryPotter}\})$, $i \in \{a, b\}$, where α: $\exists \mathit{hasDisplayCount}_c.\{\mathit{HarryPotter}\}$
- $\exists =_\beta \exists = \mathit{sum}(\exists \leq_1 \mathit{hasPrintCount}_i.\{\mathit{HarryPotter}\})$, $i \in \{a, b\}$, where β: $\exists \mathit{hasPrintCount}_c.\{\mathit{HarryPotter}\}$
- $\exists =_\delta \mathit{sum}(\alpha, \beta)$, where $\delta : \exists \mathit{hasUsageCount}_c\{\mathit{HarryPotter}\}$

Ontologies for License Agreement

Example (Ontology for content distributor Charlie)

- $hasDisplayRights \sqsubseteq hasUsageRights$
- $hasPrintRights \sqsubseteq hasUsageRights$
- $\leq (hasDisplayCount_{\{a,b\}}.eBook,\ hasUsageCount_c.eBook)$
- $\leq (hasPrintCount_{\{a,b\}}.eBook,\ hasUsageCount_c.eBook)$
- $\{Alice, Bob\} \overset{domain}{\Leftarrow} hasUsageRights \overset{range}{\longrightarrow} R_1$, where $R_1 = \leq_{10} hasUsageCount_c \wedge \geq_{2007/05/07/0900} hasDateTime_c.Time \wedge \leq_{2007/05/10/2400} hasDateTime_c.Time$
- $\exists =_\alpha \exists = sum(\exists \leq_5 hasDisplayCount_i.\{HarryPotter\})$, $i \in \{a, b\}$, where α: $\exists hasDisplayCount_c.\{HarryPotter\}$
- $\exists =_\beta \exists = sum(\exists \leq_1 hasPrintCount_i.\{HarryPotter\})$, $i \in \{a, b\}$, where β: $\exists hasPrintCount_c.\{HarryPotter\}$
- $\exists =_\delta sum(\alpha, \beta)$, where $\delta : \exists hasUsageCount_c\{HarryPotter\}$

Rules for License Agreement

Example (Rules for content distributor Charlie)

- $hasDisplayRights(?x, ?r) \wedge hasSell_dRights(?x, ?r) \Longrightarrow hasDisplaySell_dRights(?x, ?r)$
- $hasPrintRights(?x, ?r) \wedge hasSell_dRights(?x, ?r) \Longrightarrow hasPrintSell_dRights(?x, ?r)$
- $hasDisplaySell_dRights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \Longrightarrow hasDisplayRights(?y, ?r)$
- $hasPrintSell_dRights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \Longrightarrow hasPrintRights(?y, ?r)$

Rules for License Agreement

Example (Rules for content distributor Charlie)

- $hasDisplayRights(?x, ?r) \wedge hasSell_d Rights(?x, ?r) \Longrightarrow hasDisplaySell_d Rights(?x, ?r)$
- $hasPrintRights(?x, ?r) \wedge hasSell_d Rights(?x, ?r) \Longrightarrow hasPrintSell_d Rights(?x, ?r)$
- $hasDisplaySell_d Rights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \Longrightarrow hasDisplayRights(?y, ?r)$
- $hasPrintSell_d Rights(?x, ?r) \wedge delegate_g(?x, ?y) \wedge hasPrepaid(?y, ?a) \Longrightarrow hasPrintRights(?y, ?r)$

Facts for License Agreement

Example (Facts for content distributor Charlie)

- $eBook(HarryPotter)$
- $hasDisplayRights(Charlie, HarryPotter)$
- $hasPrintRights(Charlie, HarryPotter)$
- $hasSell_d Rights(Charlie, HarryPotter)$
- $hasDisplaySell_d Rights(Charlie, HarryPotter)$
- $hasPrintSell_d Rights(Charlie, HarryPotter)$
- $\exists =_5 hasPrepaid(Alice)$
- $hasDisplayRights(Alice, HarryPotter)$
- $hasPrintRights(Alice, HarryPotter)$
- $\exists =_5 hasPrepaid(Bob)$
- $hasDisplayRights(Bob, HarryPotter)$
- $hasPrintRights(Bob, HarryPotter)$

$\ldots \ldots \ldots$

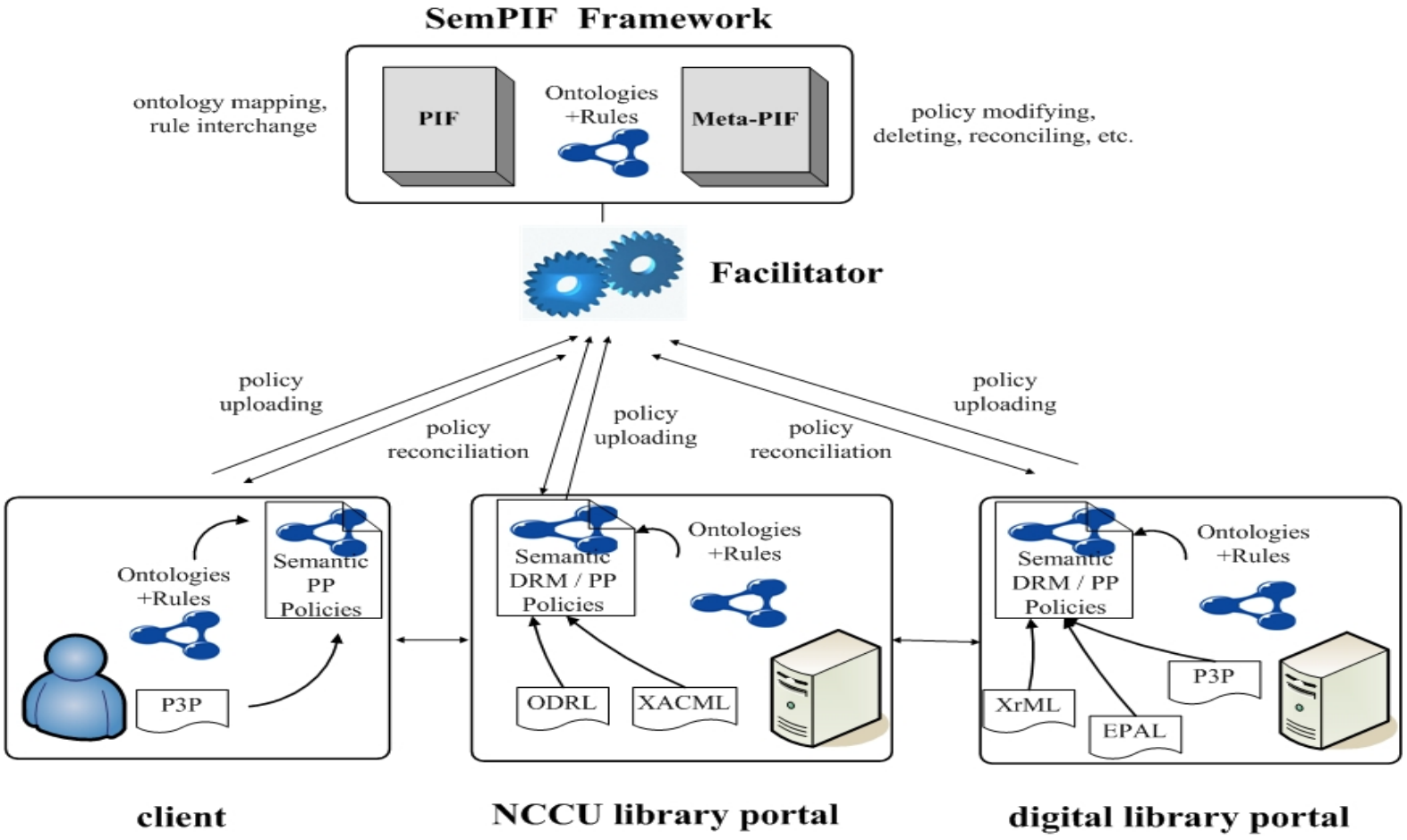
Part VI

SemPIF for DRM and Privacy Protection

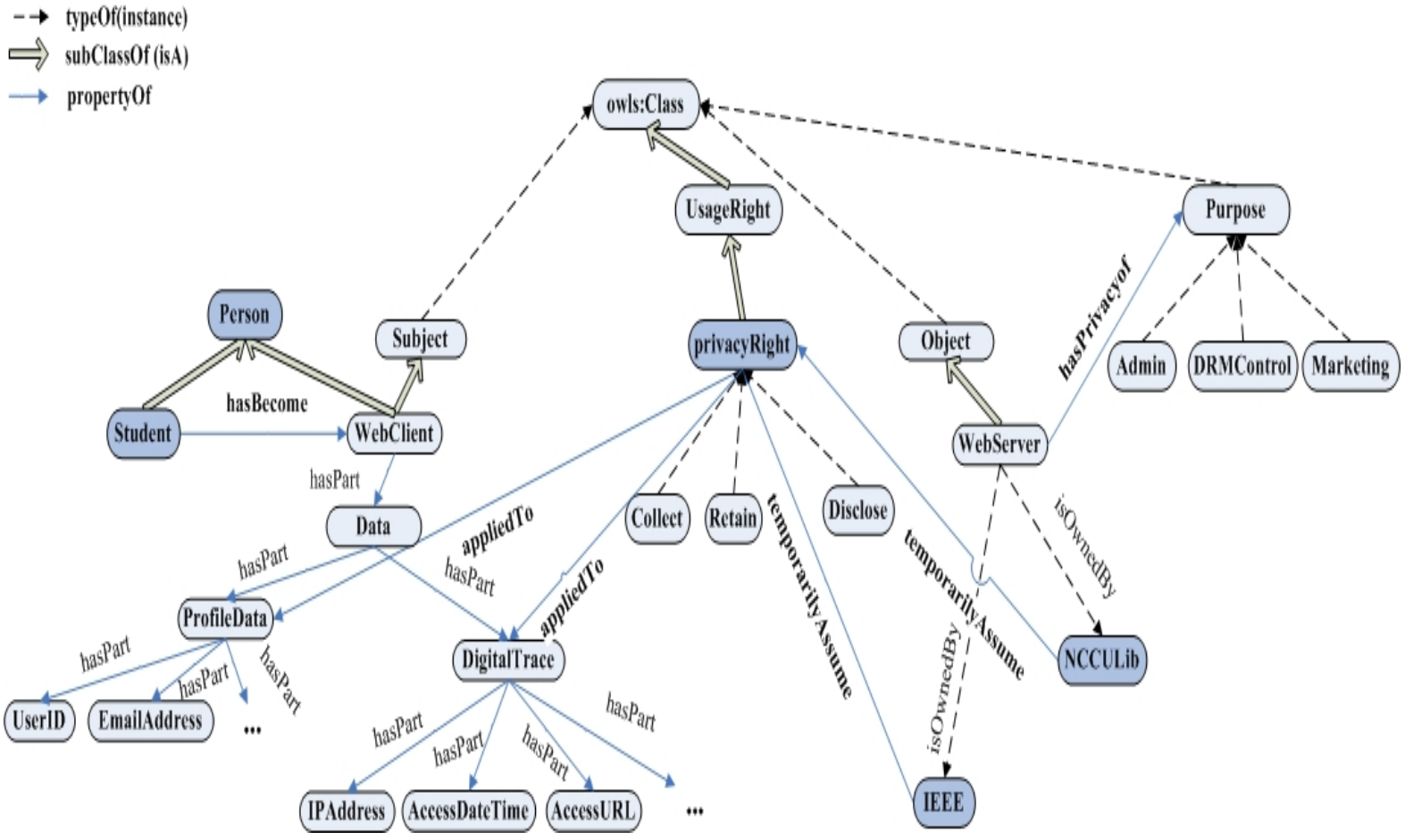
What Are the Research Issues in SemPIF?

- Policy representation and enforcement in terms of knowledge systems, e.g. ontology+rule
- Multiple Web policies interoperability and management services
- Policies conflicts resolution for agents (or facilitators) to use SemPIF architecture

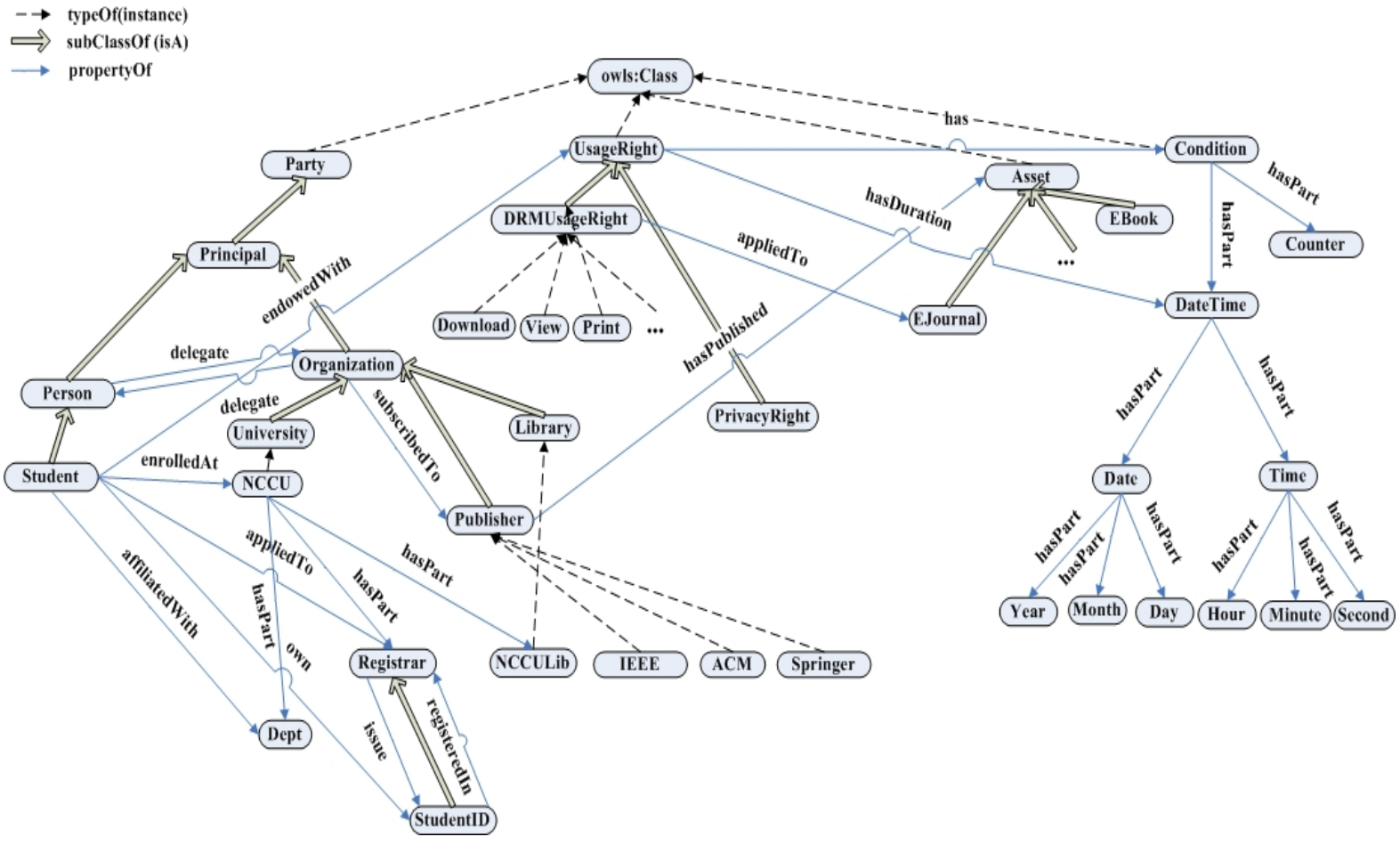
SemPIF framework for a Client Server Model



A PIF-based Privacy Protection Ontology



A PIF-based DRM Ontology



A Web Server's DRM Policy

Natural (Controlled) Language

Example (*Policy ID: drm1-IEEE*)

If a Student owns a valid student ID (StudentID) issued by the Registrar of a University and the Library of the University is one of the subscribers in the IEEE publisher list, then the student is endowed with DRM usage rights {download,view,print} of an EJournal from a Web server of the IEEE publisher.

A Web Server's DRM Policy

OWL 2+RIF

Example (*Policy ID: drm1-IEEE*)

$?st\#Student \wedge ?id\#StudentID \wedge ?uni\#University \wedge ?rg\#Registrar \wedge ?lib\#Library$
$\wedge ?ejr\#EJournal \wedge ?usrgt\#UsageRight \wedge ?st[own \longrightarrow ?id] \wedge ?uni[hasPart \longrightarrow ?rg]$
$\wedge ?st[enrolledAt \longrightarrow ?uni] \wedge ?rg[issue \longrightarrow ?id] \wedge ?uni[hasPart \longrightarrow ?lib]$
$\wedge ?lib[subscribedTo \longrightarrow IEEE] \wedge IEEE[hasPublished \longrightarrow ?ejr]$
$\wedge IEEE[endowedWith \longrightarrow ?usrgt] \wedge ?usrgt[appliedTo \longrightarrow ?ejr]$
$\Longrightarrow IEEE[delegate \longrightarrow ?st] \wedge ?st[endowedWith \longrightarrow ?d] \wedge ?st[endowedWith \longrightarrow ?v]$
$\wedge ?st[endowedWith \longrightarrow ?p] \wedge ?d\#\ Download \wedge ?d[appliedTo \longrightarrow ?ejr]$
$\wedge ?v\#View \wedge ?v[appliedTo \longrightarrow ?ejr] \wedge ?p\#Print \wedge ?p[appliedTo \longrightarrow ?ejr].$

A Web Server's DRM Policy

Natural (Controlled) Language

Example (*Policy ID: drm1-IEEE*)

If a Student owns a valid student ID (StudentID) issued by the Registrar of a University and the Library of the University is one of the subscribers in the IEEE publisher list, then the student is endowed with DRM usage rights {download,view,print} of an EJournal from a Web server of the IEEE publisher.

A Web Server's Privacy Policy

OWL2+RIF

Example (*Policy ID: pp1-IEEE*)

$$
\begin{aligned}
&?per\#Person \wedge ?usrgt\#UsageRight \wedge ?ejr\#EJournal \wedge \wedge ?prfl\#Profile \wedge ?trc\#Trace \\
&\wedge ?prrgt\#PrivacyRight \wedge ?per[endowedWith \rightarrow ?usrgt] \wedge ?usrgt[appliedTo \rightarrow ?ejr] \\
&\wedge IEEE[hasPublished \rightarrow ?ejr] \wedge IEEE[hasPrivacyOf \rightarrow DRMControl] \\
&\wedge ?per[hasPart \rightarrow ?prfl] \wedge ?per[hasPart \rightarrow ?trc] \wedge ?per[endowedWith \rightarrow ?prrgt] \\
&\Longrightarrow ?per[delegate \rightarrow IEEE] \wedge IEEE[temporarilyAssume \rightarrow ?prrgt] \\
&\wedge ?prrgt[hasDuration \rightarrow month(2)] \\
&\wedge ?prrgt[appliedTo \rightarrow ?prfl] \wedge ?prrgt[appliedTo \rightarrow ?trc] \\
&\wedge ?c\#Collect \wedge ?c[appliedTo \rightarrow ?prfl] \wedge ?c[appliedTo \rightarrow ?trc] \\
&\wedge ?r\#Retain \wedge ?r[appliedTo \rightarrow ?prfl] \wedge ?r[appliedTo \rightarrow ?trc] \\
&\wedge ?i\#Disclose \wedge ?i[appliedTo \rightarrow ?prfl] \wedge ?i[appliedTo \rightarrow ?trc].
\end{aligned}
$$

A Web User's Privacy Policy

Natural (Controlled) Language

Policy ID: pp5-John

If an EJournal Publisher **other than** *IEEE has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John's data then it temporarily assumes privacy rights {collect,retain} on John's digital Traces under the condition of a retention period less than seven days.*

Policy ID: pp6-John

If the IEEE EJournal Publisher has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John's data then it temporarily assumes privacy rights {collect,retain} on John's digital Traces under the condition of retention period less than fourteen days.

A Web User's Privacy Policy

Natural (Controlled) Language

Policy ID: pp5-John

If an EJournal Publisher **other than** *IEEE has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John's data then it temporarily assumes privacy rights {collect,retain} on John's digital Traces under the condition of a retention period less than seven days.*

Policy ID: pp6-John

If the IEEE EJournal Publisher has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John's data then it temporarily assumes privacy rights {collect,retain} on John's digital Traces under the condition of retention period less than fourteen days.

Discussion

Policy Representation and Enforcement

Natural Language

- Pros: human readable and understandable
- Cons: machine unfriendly but no formal semantics for the machine

Pure FOL

- Pros: formal and clear syntax and semantics
- Cons: machine unfriendly, possibly undecidable computation complexity, and policies writer (reader) needs to be a logician

Discussion

Policy Representation and Enforcement

Natural Language

- Pros: human readable and understandable
- Cons: machine unfriendly but no formal semantics for the machine

Pure FOL

- Pros: formal and clear syntax and semantics
- Cons: machine unfriendly, possibly undecidable computation complexity, and policies writer (reader) needs to be a logician

Discussion (conti.)

Policy Representation and Enforcement

Rights Expression Languages

- Pros: XML-based documents for machine processing
- Cons: no formal semantics for the machine

Ontology+Rule with XML Presentation Syntax

- Pros: formal semantics for automatic machine processing and understanding
- Cons: limited expressing power under certain conditions, such as negation-free, function-free, and with limited number of parameters in the Datalog

Discussion (conti.)

Policy Representation and Enforcement

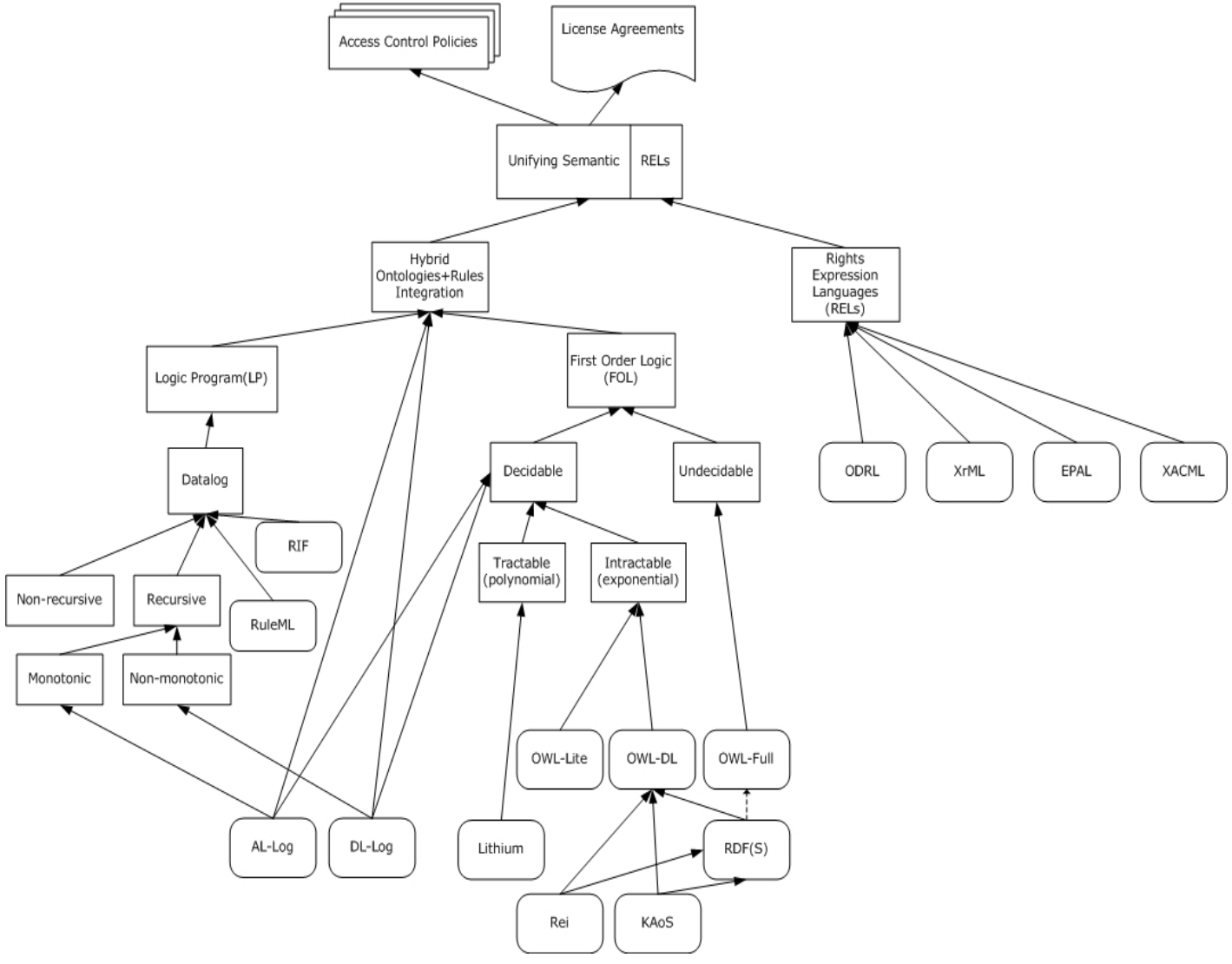
Rights Expression Languages

- Pros: XML-based documents for machine processing
- Cons: no formal semantics for the machine

Ontology+Rule with XML Presentation Syntax

- Pros: formal semantics for automatic machine processing and understanding
- Cons: limited expressing power under certain conditions, such as negation-free, function-free, and with limited number of parameters in the Datalog

Policy Languages for Access Rights Permission



Conclusion and Future Work

- Semantics-enabled policies for DRM, privacy protection, and both
- Semantics-enabled DRM policies in terms of SWRL with ODRL.
- Semantics-enabled of privacy protection policies in terms of a combination of ontology+rule with P3P.
- SemPIF policy layered architecture is proposed for the following purposes:
  1. SemPIF extends W3C's semantic web architecture.
  2. Policy in Policy Interchange Format (PIF) is available for facilitators (or agents) to provide regular policy interchange services.
  3. Meta-policy in meta-PIF is available for facilitators (or agents) to provide the management services for PIF-based policies and regular policies in the current and future policy languages.
  4. Three scenarios for each protection domain have been given to demonstrate our applicable approaches.

Conclusion and Future Work

- Semantics-enabled policies for DRM, privacy protection, and both
- Semantics-enabled DRM policies in terms of SWRL with ODRL.
- Semantics-enabled of privacy protection policies in terms of a combination of ontology+rule with P3P.
- SemPIF policy layered architecture is proposed for the following purposes:
  1. SemPIF extends W3C's semantic web architecture.
  2. Policy in Policy Interchange Format (PIF) is available for facilitators (or agents) to provide regular policy interchange services.
  3. Meta-policy in meta-PIF is available for facilitators (or agents) to provide the management services for PIF-based policies and regular policies in the current and future policy languages.
  4. Three scenarios for each protection domain have been given to demonstrate our applicable approaches.

A. H. Anderson.

A comparison of two privacy policy languages: EPAL and XACML.

In *Proceedings of the 3rd ACM Workshop on Secure Web Services (SWS'06)*, pages 53–60. ACM, 2006.

M. Blaze, J. Figenebaum, and M. Strauss.

Compliance checking in the policymaker trust management system.

In *Proc. of the Financial Cryptography*, LNCS 1465, pages 254–274. Springer, 1998.

Bonatti, P. and D. Olmedilla.

Policy language specification, enforcement, and integration

Project Deliverable D2, Working Group I2,REWERSE, 2005

A. Borgida.

On the relative expressiveness of description logic and predicate logics.

Artificial Intelligence, 82:353–367, 1996.

L. Cranor et al.

The platform for privacy preferences (p3p) 1.0 (p3p 1.0) specification, 2002.

`http://www.w3.org/P3P/`.

M. F. Donini et al.

AL-log: Integrating Datalog and description logics.

Journal of Intelligent Information Systems, 10(3):227–252, 1998.

R. Garcia, I. Gallego, and J. Delgado.

Formalising ODRL semantics using web ontologies.

In *2nd International ODRL Workshop*, Lisbon, Portugal, July 2005. The Open Digital Rights Language (ODRL) Initiative.

http://odrl.net/workshop2005/.

N. B. Grosof et al.

Description logic programs: Combining logic programs with description logic.

In *World Wide Web 2003*, pages 48–65, Budapest, Hungary, 2003.

S. Guth, G. Neumann, and M. Strembeck.

Experiences with the enforcement of access rights extracted from ODRL-based digital contracts.

In *Digital Rights Management (DRM) Workshop 2003*, Washington, DC, USA, 2003. ACM.

Joseph Y. Halpern and Vicky Weissman.

A formal foundation for XrML.

Journal of the ACM, 55(1):1–42, 2008.

Y. J. Halpern and V. Weissman.

Using first-order logic to reason about policies.

In *Proc. of 16th IEEE Computer Security Foundations Workshop (CSFW'03)*, pages 187–201, July 2003.

I. Horrocks et al.

SWRL: A semantic web rule language combing owl and RuleML, 2004.

http://www.w3.org/Submission/SWRL/.

Ian Horrocks et al.

OWL rules: A proposal and prototype implementation.

J. of Web Semantics, 3(1):23–40, 2005.

Y. J. Hu.

Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies.

In *Workshop on Privacy Enforcement and Accountability with Semantics in conjunction with ISWC+ASWC 2007*, 2007.

Y. J. Hu, H. Y. Guo, and G. D. Lin.

Semantic enforcement of privacy protection policies via the combination of ontologies and rules.

In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, Taichung, Taiwan, June 2008.

R. Iannella.

Open digital rights language (ODRL), version 1.1.

W3c note 19, The ODRL Initiative, September 2002.

http://www.w3.org/TR/odrl/.

ContentGuard Inc.

eXtensible rights Markup Language (XrML), ver. 2.0.

Technical report, ContentGuard Inc., 2002.

`http://www.xrml.org/index.asp`.

S. Jajodia et al.

Flexible support for multiple access control policies.

ACM Trans. on Database Systems, 26(2):214–260, June 2001.

A. B. LaMacchia.

Key challenges in DRM: An industry perspective.

In *Digital Rights Management (DRM) Workshop 2002*, LNCS 2696. Springer, 2003.

Y. Alon Levy and M.-C. Rousset.

CARIN: A representation language combining horn rules and description logics.

In *Proc. of the 12th Eur. Conf. on Artificial Intelligence (ECAI'96)*, pages 323–327, 1996.

N. Li, B. N. Grosof, and J. Feigenbaum.

Delegation logic: A logic-based approach to distributed authorization.

ACM Trans. Information and System Security, 6(1):128–171, 2003.

B. Motik et al.

Can OWL and logic programming live together happily ever after?

In *5th International Semantic Web Conference (ISWC) 2006*, LNCS 4273, Athens, GA, USA, Nov. 2006.

B. Motik, U. Sattler, and R. Studer.

Query answering for OWL-DL with rules.

In *3rd International Semantic Web Conference (ISWC) 2004*, LNCS 3298, pages 549–563. Springer, 2004.

J. Pan and I. Horrocks.

Web ontology reasoning with datatype groups.

In *ISWC 2003*, LNCS2870, pages 47–63. Springer, 2003.

J. Park and R. T. Sandhu.

The UCON$_{ABC}$ usage control model.
ACM Trans. on Information and System Security, 7(1):128–174, 2004.

R. Pucella and V. Weissman.
A formal foundation for ODRL.
In *Workshop on Issues in the Theory of Security (WITS)*, 2004.

R. Rosati.
On the decidability and complexity of integrating ontologies and rules.
Web Semantics: Science, Services and Agents on the World Wide Web 3, pages 61–73, 2005.

R. Rosati.
DL+log: Tight integration of description logics and disjunctive Datalog.
In *Proc. of the 10th International Conference on Principles of Knowledge Representation and Reasoning (KR)*, 2006.

R. Rosati.
Integrating ontologies and rules: Semantic and computational issues.
In *Reasoning Web 2006*, LNCS 4126, pages 128–151, 2006.

M. Stefik.
Letting loose the light: Igniting commerce in electronic publication.

In *Internet Dreams: Archetypes, Myths, and Metaphors*. MIT Press, 1996.

G. Tonti et al.

Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rein, and Ponder.

In *2nd International Semantic Web Conference (ISWC) 2003*, LNCS 2870, pages 419–437. Springer, 2003.

D. J. Weitzner et al.

Creating a policy-aware web: Discretionary, rule-based access for the world wide web.

In E. Ferrari and B. Thuraisingham, editors, *Web and Information Security*, pages 1–31. Idea Group Inc., 2006.

T. Yu, A. N. Li, and I. Antón.

A formal semantics for p3p.

In *ACM Workshop on Secure Web Services*, Fairfax, VA, USA, Oct. 2004.

`http://citeseer.ist.psu.edu/750176.html`.