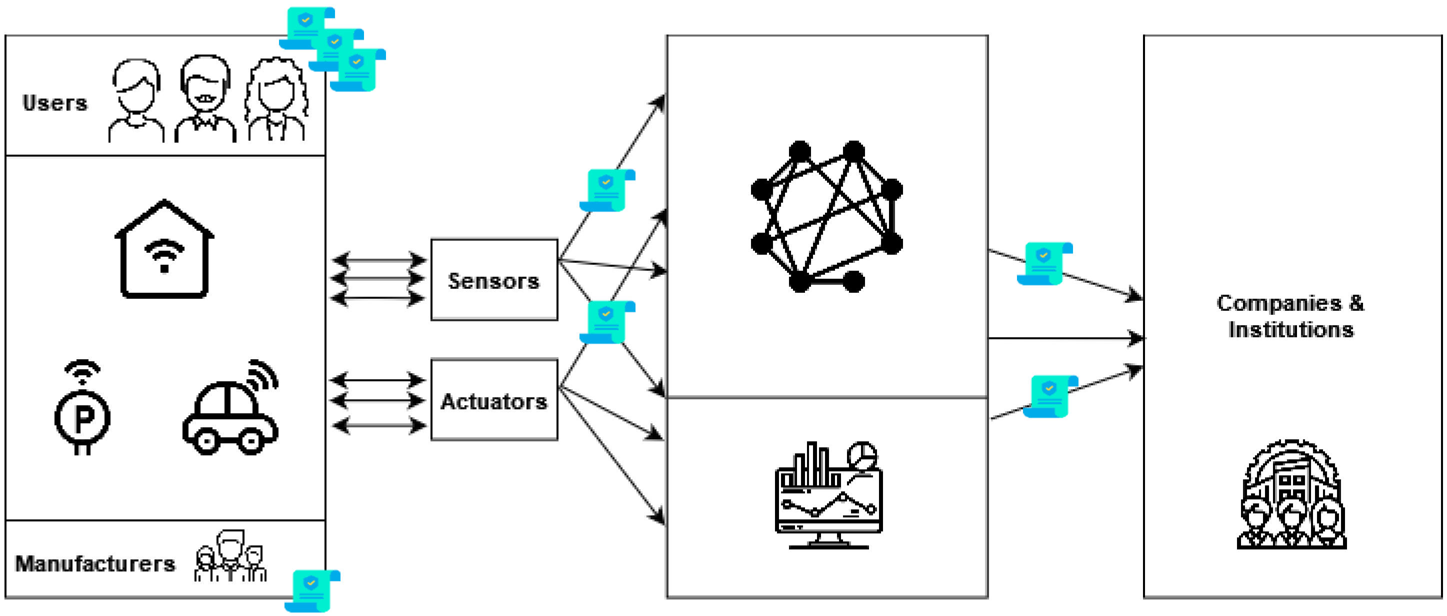
Semantic Technology based Usage Control for Decentralized Systems

ISWC Doctoral Consortium
24/10/2022
Online

Insitute for Information Systems & New Media
Inès Akaichi
Supervised by: Dr. Sabrina Kirrane

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Usage Control
Motivation



- Data abundance
- Risk of data misuse
- Users & Lack of Control

Usage Control
Definitions

- An extension of access control
- Ensures data sovereignty
- Regulates what is allowed to the data (future usage)
- It involves data consumers and data providers/owners
- Related to data storage, distribution, aggregation and processing
- Context of intellectual property protection, privacy protection, compliance with regulations and digital rights management

We focus on **policy-based usage control**, where we use **machine-readable policies** to express requirements for future data usage and mechanisms to enforce the respective usage policies

Pretschner, A., Hilty, M., & Basin, D. (2006). Distributed usage control. *Commun. ACM* 49, 9, 39–44.
Park, J. & Sandhu, R. (2004). The UCONABC usage control model. *ACM Trans. Inf. Syst. Secur.* 7, 1, 128–174.

Usage Control
Specification, Enforcement, and Robustness

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Requirements Elicitation

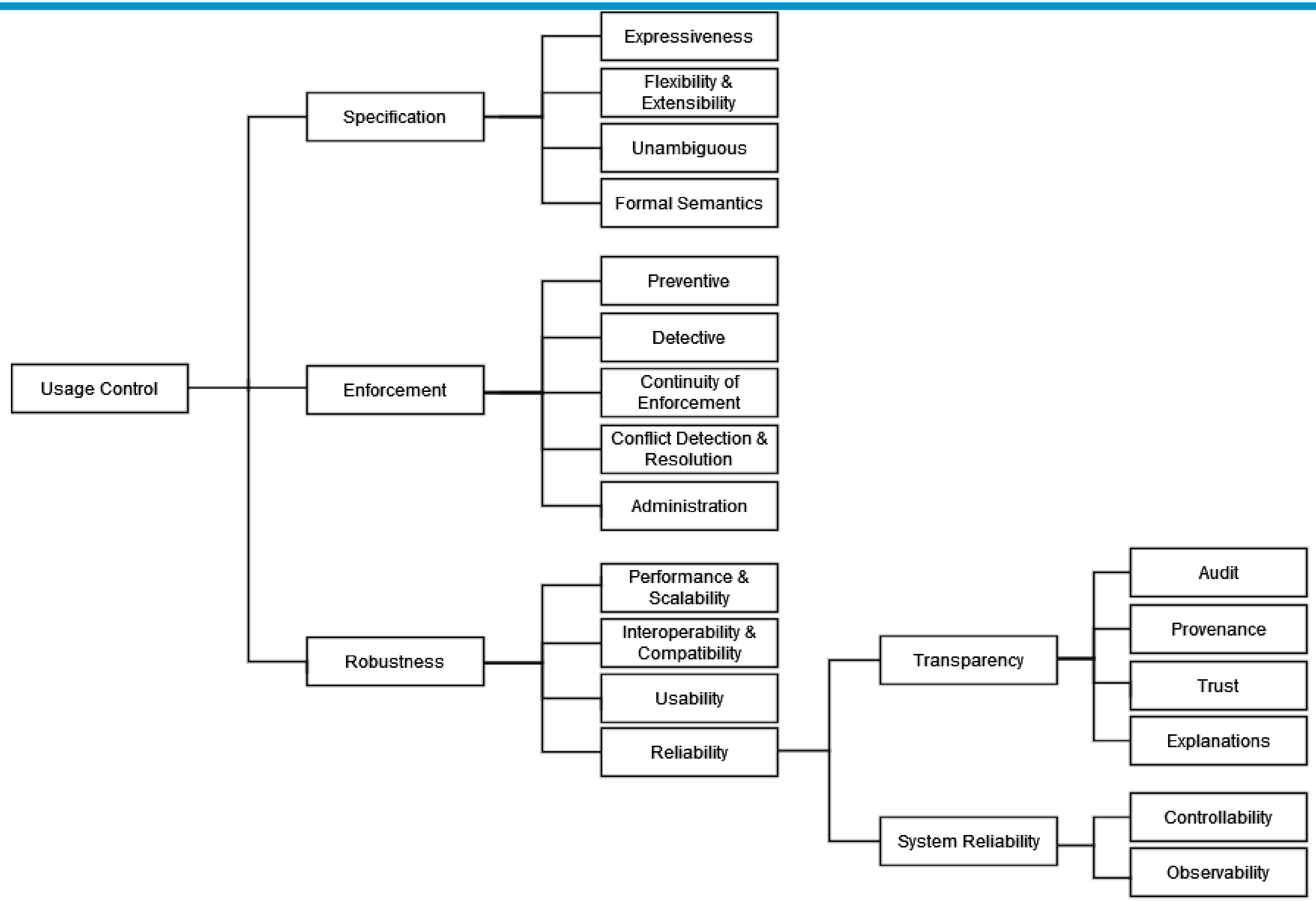
Framework Comparison

Policy Languages

Gaps & Research Questions

Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.

Requirements Elicitation



Taxonomy excerpt from Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.

Frameworks Comparison
Specification

Table excerpt from Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.

Framework	Expressiveness				Flexibility & Extensibility		Unambiguous	Formal Seman-tics
	Operators/ Rules	Conditions	Attributes	Context	Represent-ation	Model		
Bai et al. [5]	A, O	environmental system-oriented	mutability	model based	XML	UCON	–	–
Baldini et al. [6], Neisse et al. [78]	E, C, A	cardinal temporal event-defined		model based	XML	–	–	OSL
Cao et al. [13]	P, Pr, O	actor spatial temporal purpose monetization		model based	XML	DUPO	–	defeasible logic
Carniani et al. [14], Lazouski et al. [62]	A, O	environmental system-oriented	mutability	system based	XML	XACML	–	–
Costantino et al. [20]	A, O	environmental system-oriented	mutability	system based	XML	XACML	–	–
Cirillo et al. [15]	P, Pr, O	purpose temporal spatial event-defined	–	–	XML	ODRL	–	–
Feth and Pretschner [28]	E, C, Ac	cardinal temporal spatial	–	–	XML	–	–	OSL
Giorgi et al. [32]	A, O	environmental system-oriented	mutability	system based	XML	XACML	–	–
Jung et al. [44]	E, C, Ac	cardinal		system-	XML			OSL

Frameworks Comparison
Enforcement

Table excerpt from Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.

Framework	Preventive	Detective	Continuity of Enforcement	Conflict Detection & Resolution	Administration
Bai et al. [5]	permission, inhibition, revoke, delay, update	_	monitor attribute and context updates, monitor obligation fulfillment	_	PAP interface
Baldini et al. [6], Neisse et al. [78]	permission, inhibition, revoke, delay, modification	_	monitor condition updates and obligations fulfillment	combining algorithms	graphical user interface
Carniani et al. [14], Lazouski et al. [62]	permission, inhibition, revoke, update	_	monitor attribute, context, and condition updates	_	PAP interface
Cao et al. [13]	permission, inhibition, revoke, delay	_	monitor condition and context updates, monitor obligation fulfillment	logic-based	jDUPO
Costantino et al. [20]	permission, inhibition, revoke, update	_	monitor attribute, context, and condition updates	_	PAP interface
Cirillo et al. [15]	permission, inhibition, execution	execution actions	_		graphical user interface
Feth and Pretschner [28]	permission, inhibition, revoke, delay, modification, execution	execution actions	monitor condition updates and obligations fulfillment	_	Android interface
Giorgi et al. [32]	permission, inhibition, revoke, update	_	monitor attribute, context, and condition updates	_	PAP interface
Jung et al. [44]	permission, inhibition, modification, execution, revoke	execution actions	monitor condition updates and obligations fulfillment	_	PAP interface
Kateb et al. [48]	permission, inhibition,	_	monitor obligation fulfillment	_	_

Frameworks Comparison
Robustness

Table excerpt from Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.

Framework	Performance & Scalability	Interoperability & Compatibility	Usability	Reliability	
				Transparency	System Reliability
Bai et al. [5]	performance metrics comparison	XML	–	–	–
Baldini et al. [6], Neisse et al. [78]	performance metrics	XML	use of templates	trust	support for trust management
Cao et al. [13]	performance metrics	XML REST APIs	technical expertise required	explanations provenance	–
Carniani et al. [14], Lazouski et al. [62]	performance metrics	XML	–	–	–
Costantino et al. [20]	performance metrics	XML	–	–	–
Cirillo et al. [15]	performance metrics	XML	–	audit provenance	decentralized policy enforcement
Feth and Pretschner [28]	performance metrics other evaluation metrics	XML	–	trust	–
Giorgi et al. [32]	performance metrics	XML	–	–	–
Jung et al. [44]	–	XML	technical expertise required	audit	–
Kateb et al. [48]	–	XML	–	–	–
Lazouski et al. [64]	performance metrics	XML	–	–	–
La Marra et al. [58], Martini et al. [69]	performance metrics	XML	–	–	–
La Marra et al. [60]	performance metrics	XML	–	–	–
La Marra et al. [61]	performance metrics	XML	–	–	–
La Marra et al. [59]	performance metrics	XML	–	–	–
Martinelli et al. [67]	–	XML	–	–	–
Martinelli et al. [68]		XML			

Policy Languages

- Usage control frameworks [1]
  - IND²UCE
  - ConUCON
  - U-XACML, etc.

- General policy languages and frameworks [2]
  - KaoS
  - Rei
  - Protune, etc.

- Custom policy languages and frameworks [3]
  - The SPECIAL Usage Policy Language
  - The Open Digital Rights Language (ODRL), etc.

There are many other different policy languages, of which the following are the most relevant to our topic!

[1] Akaichi, I., & Kirrane, S. (2022). Usage Control Specification, Enforcement, and Robustness: A Survey. ArXiv, abs/2203.04800.
[2] Kirrane, S., Mileo, A. & Decker, S. (2017). Access control and the Resource Description Framework: A survey. Semant. web 8, 2, 311–352.
[3] Esteves, B. & Rodríguez-Doncel, V. (2021). Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR. Semant. web (forthcoming)

Gaps & Research Questions

Specification	Enforcement	Robustenss
Generality of Policies	Automated Formal Analysis	Usability
The decentralized usage control		

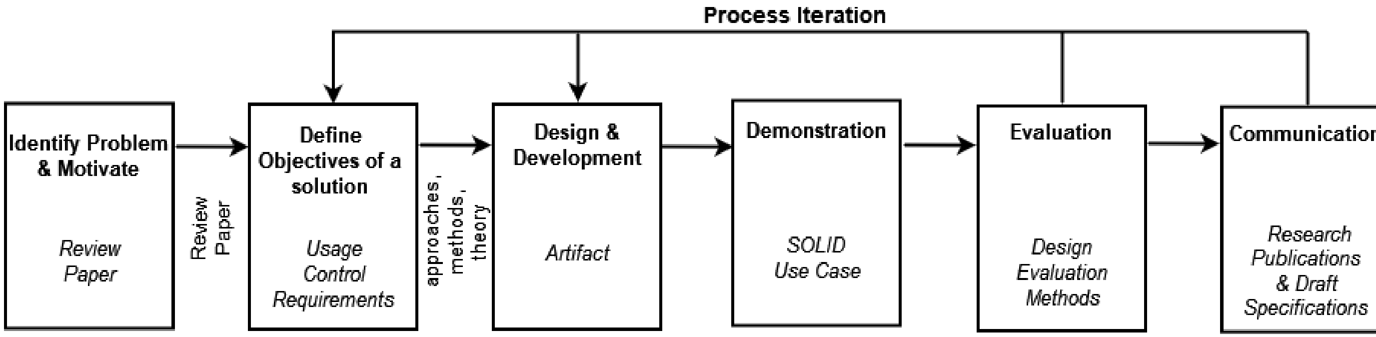
RQ1. *To what extent do semantic web technologies improve the flexibility and extensibility of usage control policy languages?*

RQ2*. What are the most suitable mechanisms for enforcing usage control policies in decentralized environments?*

RQ3. *What are the most effective tools and techniques that can be used to provide data owners with more control, trust and transparency with respect to how their data are being used?*

Methodology & Artifacts

- The Design Science Research Methodology (DSRM) [1]



- Artifacts
  - A usage control policy language
  - An enforcement framework
  - Data empowerment tools and technologies

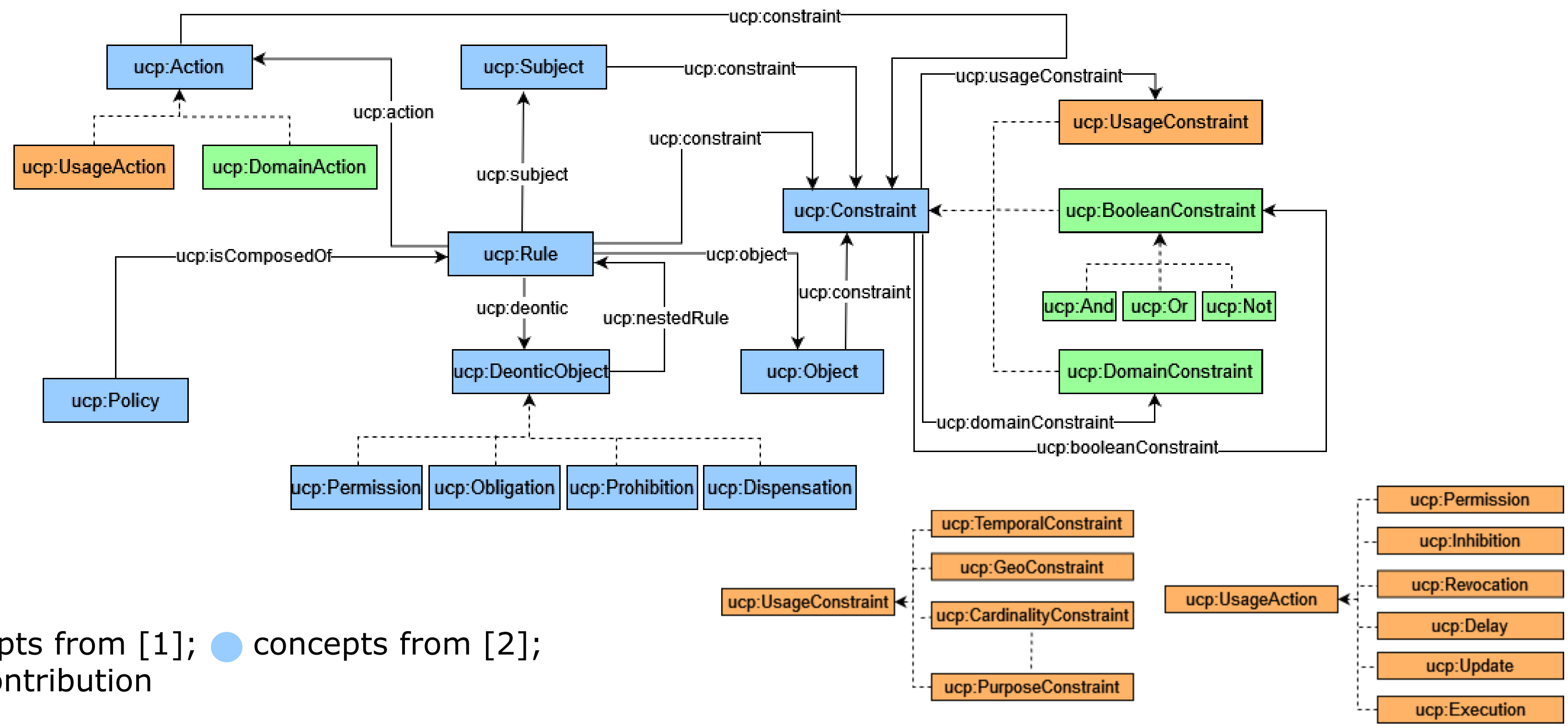
[1] Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. J. Manage. Inf. Syst. 24, 3, 45–77.

A usage control policy language

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

- Leverage semantic web technologies to enable the flexibility and extensibility of usage control policy languages
- Develop a layered Policy Language for Usage Control using semantic technologies:
  - The Usage Control Policy (UCP) Core Model
  - An ontology
  - Formalization
  - Description Logic Profiles

The Usage Control Policy (UCP) Core Model



Legend:
concepts from [1]; concepts from [2];
out contribution

Akaichi, I., & Kirrane, S. (2022). A Semantic Policy Language for Usage Control. *In Proceedings of Semantics*, Vienna, Austria.
[1] Kagal, L., Finin, T.W., & Joshi, A. (2003). A Policy Based Approach to Security for the Semantic Web. *SEMWEB*.
[2] De Vos, M., Kirrane, S., Padget, J., & Satoh, K. (2019). ODRL policy modelling and compliance checking.

The Usage Control Policy (UCP) Core Model

Model Instantiation

- **P1.** Only subscribed marketing companies are allowed to download power consumption data. They must keep the downloaded data for a maximum of 6 months

1

```
<http://example.com/mcp#Perm_MarketingCompDownloading>
  a <http://example.com/ucp#Permission> .

<http://example.com/mcp#IsSubsribed>
  a <http://example.com/ucp#DomainConstraint> ;
  ucp:subject
  <http://example.com/mcp#MarketingCompany> ;
  ucp:predicate
  <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> ;
  ucp:object
  <http://example.com/mcp#Subscriber> .

<http://example.com/mcp#Oblig_MarketingCompStoring>
  a <http://example.com/ucp#Obligation> .

<http://example.com/mcp#For6Months>
  a <http://example.com/ucp#TemporalConstraint> ;
  time:hasDurationDescription
  <http://example.com/mcp#Duration6Months> .
  <http://example.com/mcp#Duration6Months> a
  <http://www.w3.org/2006/time#GeneralDurationDescription> ;
  time:months 6.0 .
```

2

```
<http://example.com/mcp#Rule_MarketingCompDownloading>
  a <http://example.com/ucp#Rule> ;
  ucp:subject
<http://example.com/mcp#SubscribedMarketingCompany> ;
  ucp:object
  <http://example.com/mcp#PowerConsumptionData> ;
  ucp:action
 <http://example.com/mcp#ActionMarketingCompDownloading> ;
  ucp:constraint
  <http://example.com/mcp#IsSubsribed> ;
  ucp:deontic
  <http://example.com/mcp#Perm_MarketingCompDownloading> .

<http://example.com/mcp#Rule_MarketingCompStoring>
  a <http://example.com/ucp#Rule> ;
  ucp:subject
  <http://example.com/mcp#MarketingCompany> ;
  ucp:object
  <http://example.com/mcp#PowerConsumptionData> ;
  ucp:constraint
  <http://example.com/mcp#For6Months> ;
  ucp:action
  <http://example.com/mcp#ActionMarketingCompStoring> ;
  ucp:deontic
  <http://example.com/mcp#Oblig_MarketingCompStoring> .

<http://example.com/mcp#Perm_MarketingCompDownloading>
  ucp:nestedRule
  <http://example.com/mcp#Rule_MarketingCompStoring> .
```

The Usage Control Policy (UCP) Core Model
Model Instantiation

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

- **P2.** Subscribed marketing companies are allowed to download power consumption data for aggregation purposes only.

```
<http://example.com/mcp#ConstraintUsagePurposes>
  a <http://example.com/ucp#PurposeConstraint> ;
  ucp:usageConstraint
  <http://example.com/mcp#AggregationPurpose> .
```

Formalization
Description Logics

- Why Description Logics?
  - ✓ Decideability
  - ✓ Use off-the-shelf reasoners (e.g., FaCT++, HermiT)

	Syntax	Semantics
Individuals:		
individual name	a	$a^{\mathcal{I}}$
Roles:		
atomic role	R	$R^{\mathcal{I}}$
inverse role	R^-	$\{\langle x, y\rangle \mid \langle y, x\rangle \in R^{\mathcal{I}}\}$
universal role	U	$\Delta^{\mathcal{I}} \times \Delta^{\mathcal{I}}$
Concepts:		
atomic concept	A	$A^{\mathcal{I}}$
intersection	$C \sqcap D$	$C^{\mathcal{I}} \cap D^{\mathcal{I}}$
union	$C \sqcup D$	$C^{\mathcal{I}} \cup D^{\mathcal{I}}$
complement	$\neg C$	$\Delta^{\mathcal{I}} \setminus C^{\mathcal{I}}$
top concept	$\top$	$\Delta^{\mathcal{I}}$
bottom concept	$\bot$	$\emptyset$
existential restriction	$\exists R.C$	$\{x \mid$ some $R^{\mathcal{I}}$-successor of x is in $C^{\mathcal{I}}\}$
universal restriction	$\forall R.C$	$\{x \mid$ all $R^{\mathcal{I}}$-successors of x are in $C^{\mathcal{I}}\}$
at-least restriction	$\geqslant n\, R.C$	$\{x \mid$ at least n $R^{\mathcal{I}}$-successors of x are in $C^{\mathcal{I}}\}$

Formalization
Policy Rules

The SPECIAL Policy Language [1]	The UCP Policy Language
An authorization: $\exists$hasData.SomeData $\sqcap$ $\exists$hasProcessing.SomeProcessing $\sqcap$ $\exists$hasPuropose.SomePurpose $\sqcap$ $\exists$ hasRecipient.SomeRecipient $\sqcap$ $\exists$hasStorage.SomeStorage	A rule: $\exists$ hasSubject.SomeSubject $\sqcap$ $\exists$ hasObject.SomeObject $\sqcap$ $\exists$ hasAction.SomeAction $\sqcap$ $\exists$ hasConstraint.SomeConstraint

- A rule can be a permission, a prohibition, an obligation, or a dispensation
- Use Deontic Logic to interdefine Policy rules
- Express nesting rules, e.g., a permission that requires an obligation

[1] Bonatti, P.A., Kirrane, S., Petrova, I.M. *et al.* (2020). Machine Understandable Policies and GDPR Compliance Checking. *Künstl Intell* 34, 303–315.

Formalization
Policy Rules

The SPECIAL Policy Language [1]	The UCP Policy Language
An authorization: ∃hasData.SomeData ⊓ ∃hasProcessing.SomeProcessing ⊓ ∃hasPuropose.SomePurpose ⊓ ∃ hasRecipient.SomeRecipient ⊓ ∃hasStorage.SomeStorage	A rule: ∃ hasSubject.SomeSubject ⊓ ∃ hasObject.SomeObject ⊓ ∃ hasAction.SomeAction ⊓ ∃ hasConstraint.SomeConstraint
Verify compliance of authorization requests by data consumers against data owner‵s consent	Verify usage compliance (e.g., reconstructed from logs) against policy rules (defined by data owners/providers)

- Use subsumption reasoning for compliance checking

[1] Bonatti, P.A., Kirrane, S., Petrova, I.M. *et al.* (2020). Machine Understandable Policies and GDPR Compliance Checking. *Künstl Intell* 34, 303–315.

A usage control policy language
Ongoing Work

- Continue the formalization of rules
- Formalize the usage control constraints (e.g., use the OWL_{time} ontology to express temporal constraints)
- Study the expressiveness of various obligations and constraints
- Propose Description Logic Policy Profiles with the possibility of varying combinations of obligations and constraints
- Evaluate the expressiveness of the policy languages

Summary & Future Work

- Usage control is required to control the dispersion of information within decentralized solutions
- In order to achieve effective policy-based usage control, various gaps still need to be addressed

RQ1

A usage control policy language

- Expressiveness Evaluation

RQ2

An enforcement framework

- Performance Evaluation

RQ3

Data empowerment tools and technologies

- Usability testing

RQ2

Demonstrate the suitability of our proposal

- Integrate our framework to SOLID[1], a decentralized technology for data storage

[1]https://solidproject.org/