PIDSKG Workshop (2)

A Policy Framework for Usage Control

Inès Akaichi, Giorgos Flouris, Irini Fundulaki, and Sabrina Kirrane

University of Salerno, Salerno, Italy, February 14th 2023

Disclaimer!

This work is in progress

Usage Control
Context

- An extension of access control
- Regulates usage of the data: permissions (prohibitions) and obligations (dispensations)
- Ensures data sovereignty
- 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

Usage Control
Context

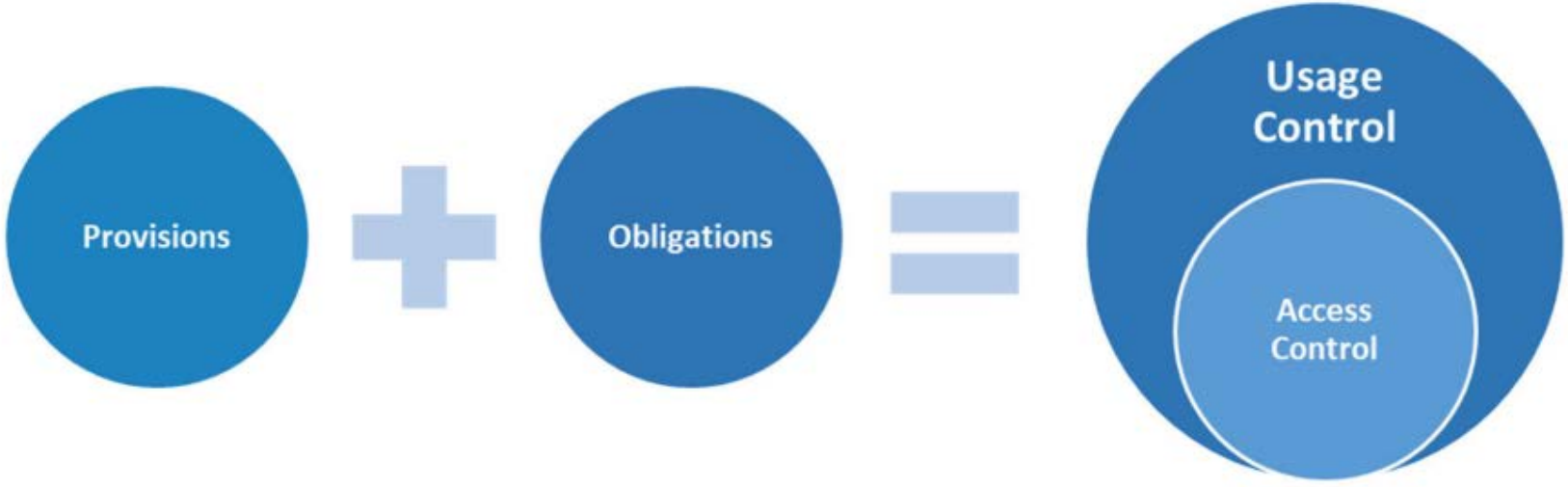


Figure taken from Usage Control in the International Data Spaces V3.0 (2021). Steinbuss et al.

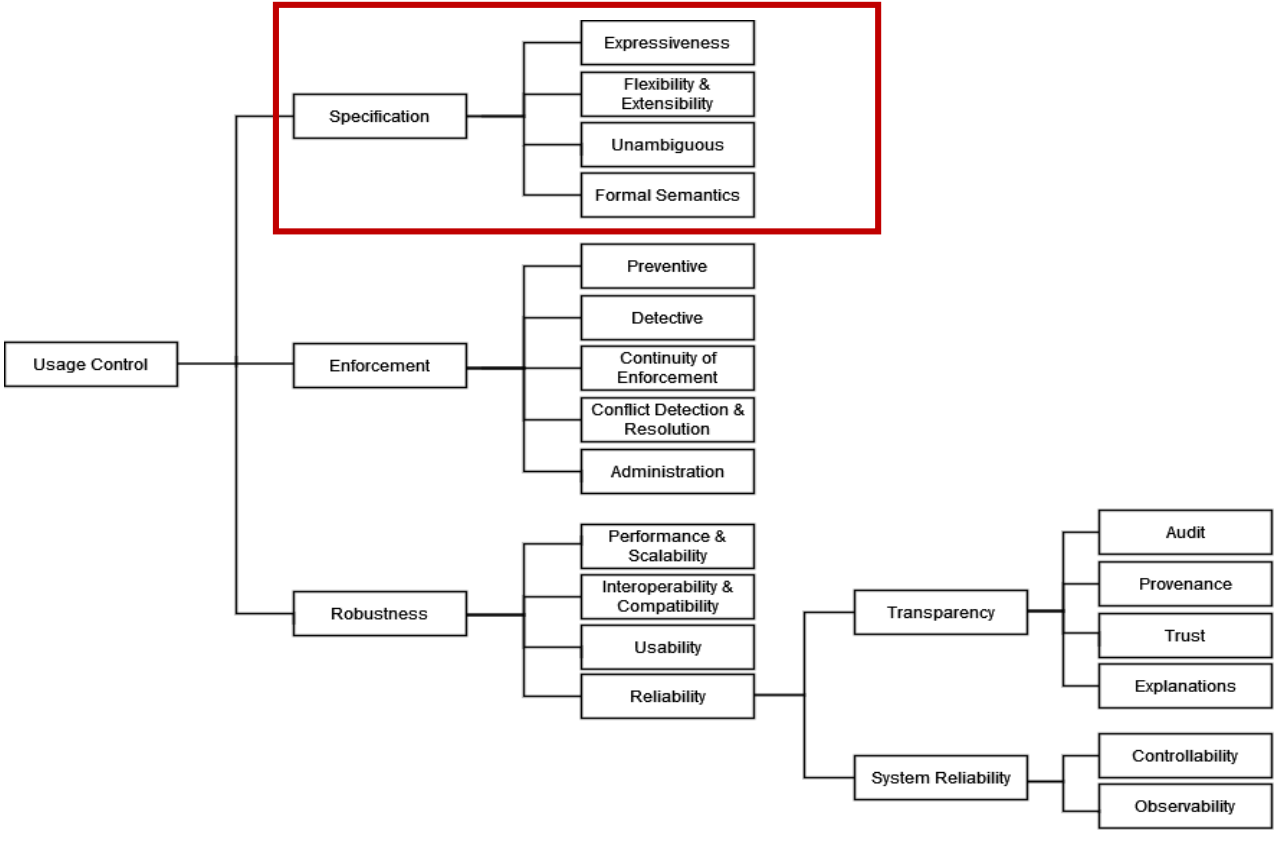
Usage Control Policy Languages
Related Work

- Usage control policy frameworks/ languages
  - UCON [1] and derivatives (cf., [2,3])
  - The Obligation Specifcation Language (OSL) [4]
  - …
- General policy languages
  - Kaos [5]
  - Rei [6]
  - …
- Tailored policy languages
  - ODRL [7]
  - The Special Policy Language [8]
  - …

Usage Control Policy Languages
Gaps

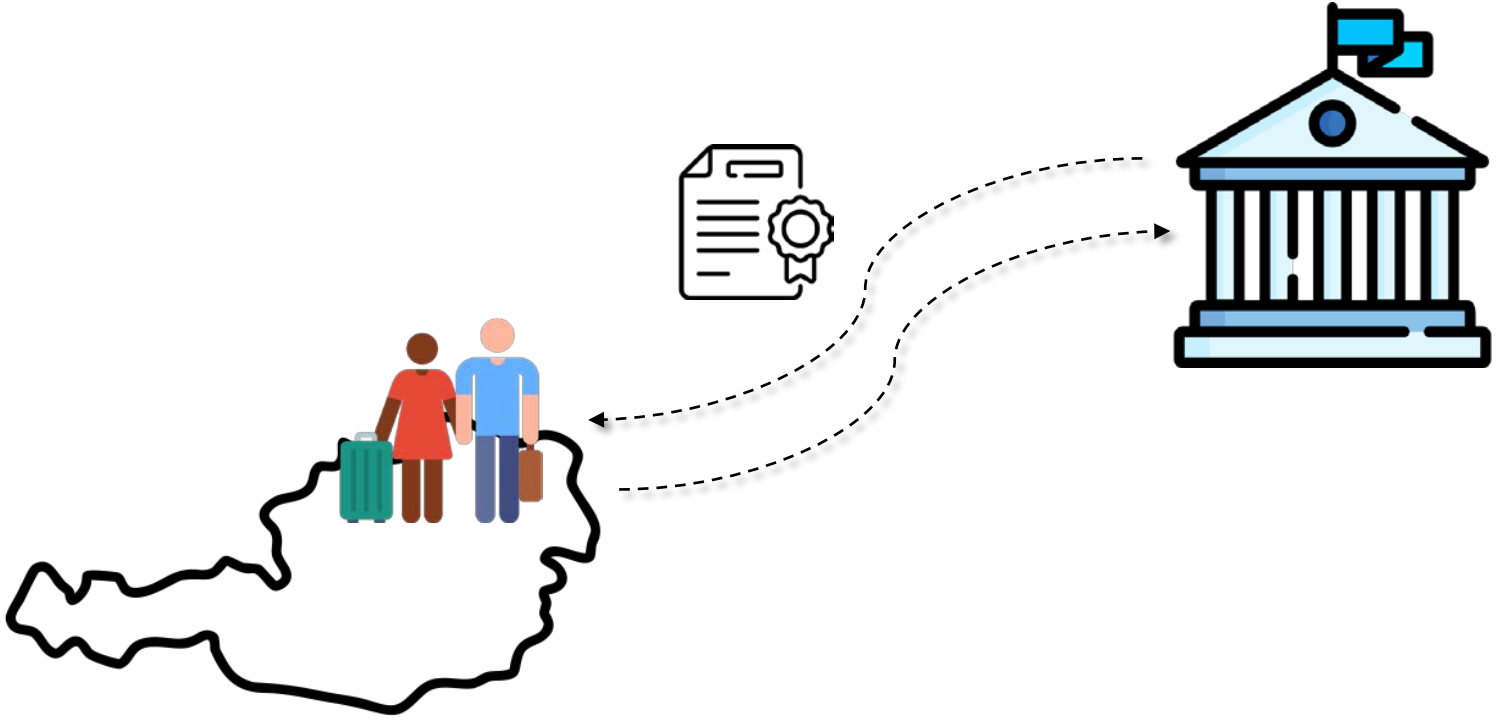
- Usage control policy frameworks/ languages
  - ✓ Abstract models [1]
  - ✓ Express only obligations [4]
  - ✓ Proposed for specific domains [cf., (9)]
  - ✓ Lack formal semantics [cf., (1,)]
- General policy languages
  - ✓ Not clear how to support general structurres encountered in usage control (obligations, dispensations, usage conditions, etc.) [cf., (5,6)]
  - ✓ Lack formal semantics [cf., (6)]
- Tailored policy languages
  - ✓ Too specific [cf., (7,8)]
  - ✓ Lack formal semantics [cf., (7)]

A Language for Usage Control
Requirements



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

Use Case (1)
The address registration process in Austria



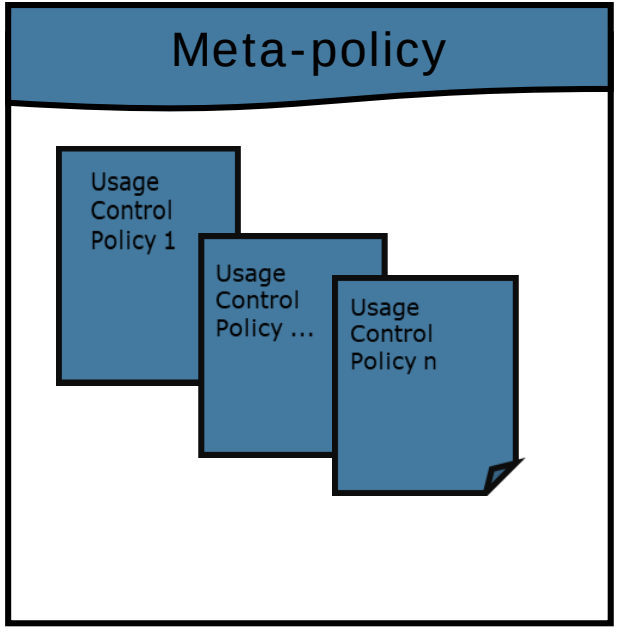
Use Case (2)
Legal requirements

- The legal requirements regarding the registration process in Austria:
  - **Rule 1.** A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria.
  - **Rule 2.** A person is obliged to deregister their old address within three days of changing their place of residence, or of leaving the country.
  - **Rule 3.** Tourists in Austria are exempt from registering their address.
  - **Rule 4.** If the person stays in a hotel, they are allowed to request a signature from the hotel.
  - **Rule 5.** If the person stays in with friends or family members, they are allowed to request a signature from the property owner.
  - **Rule 6.** A person is not allowed to open a bank account if they do not have a certificate of registration.

The Usage Control Policy (UCP) Framework

- ✓ Specification of usage control policies
- ✓ Representation of the state of affairs via Knowledge Bases
- ✓ Reasoning tasks

The UCP Framework
Usage Control Policies



Notation

- **O, D, P, A** denote the deontic operators **Obligation**, **Dispensation**, **Prohibition**, and **Permission** (allowance)
- *U* and *L* denote the set of *URIs* and *literals* respectively.
- We also consider two sets, P , A (subsets of U), such that $P \subseteq U$, $A \subseteq U$
- Assume additionally the existence of an infinite set V of variables disjoint from the above sets. We use "*?*" to denote variables (e.g., *?x*, *?y* etc.)

The UCP Framework
Basic Elements: element Pattern

Definition 2 (Element Pattern). *An* element pattern *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U \cup V$
- $mp \in U \cup V \cup \{\perp\}$
- $o \in U \cup L \cup V$
- $mo \in U \cup L \cup V \cup \{\perp\}$
- $pa \in P \cup A \cup V$

We denote by $\mathcal{EP}$ *the set of all element patterns.*

Example:

Rule 1. A *person* is obliged to *register* their *address* with one of the local authorities *within three days* of *changing residence* or having moved from abroad to Austria.

- This rule states that it is an obligation to: (?x, :register, ?y, ... , ...)
- Whenever these conditions are true: (?x, :type, :Person)
  (?x, :moveTo, ?y)
  (?y, :type, :Address)

The UCP Framework
Basic Elements: deontic Pattern

Definition 3 (Deontic Patterns). *Let* $\mathcal{D} = \{\mathbf{O}, \mathbf{D}, \mathbf{P}, \mathbf{A}\}$ *denote the* deontic operators Obligation, Dispensation, Prohibition, *and permission (*Allowance*), respectively. A* deontic pattern *is a statement of the form* da*, where* $d \in \mathcal{D}$ *and* $a \in \mathcal{EP}$.

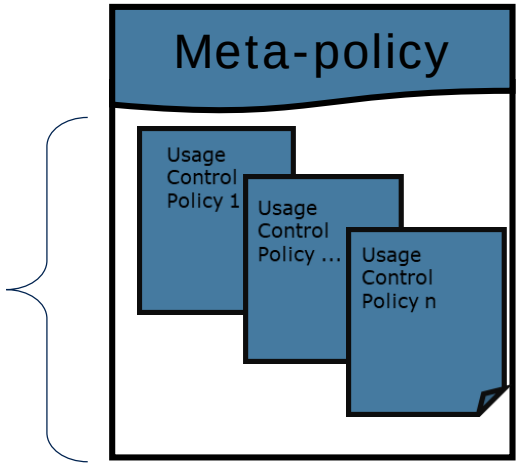
Example:

Rule 1. A person is *obliged* to *register* their *address* with one of the local authorities *within three days* of changing residence or having moved from abroad to Austria.

O(?x, :register, ?y, ..., ...)

The UCP Framework
Usage Control Policies

- A set of rules
- Each rule follows the form:
- *If* **condition** *then* **Aa, Pa, Oa,, Da**
- ***Condition:*** *graph pattern (defined based on element patterns)*
- ***Aa, Pa Oa, Da:*** *deontic pattern*

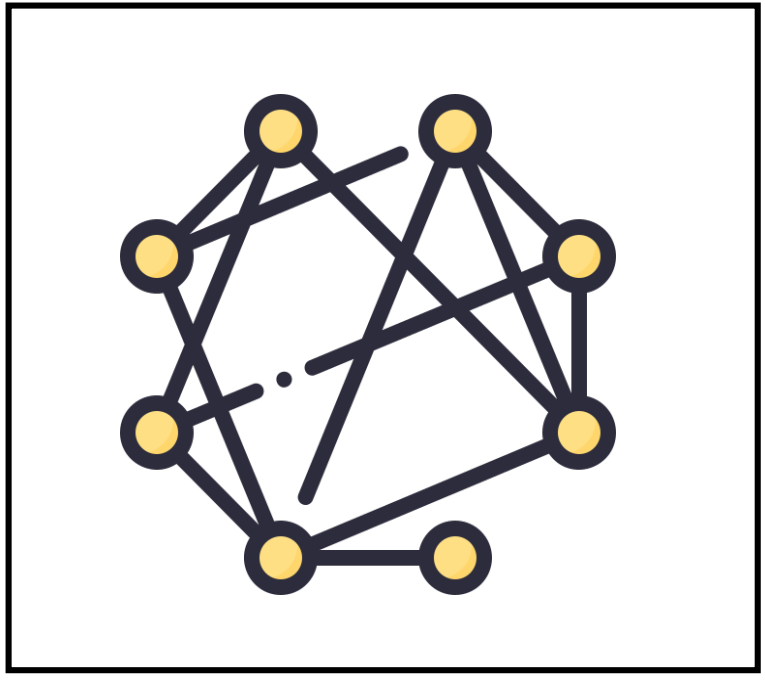


Example:

Rule 1. A *person* is obliged to *register* their *address* with one of the local authorities *within three days* of *changing residence* or *having moved* from abroad to Austria.

(?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) ⇝ **O**(?x, :register, ?y, ..., ...)

The UCP Framework
Knowledge Bases



The UCP Framework
Basic Elements: action and Factual Elements

Definition 1 (Element). *An* element *is a 5-tuple of the form* (s, pa, o, mp, mo) *such that:*

- $s \in U$
- $mp \in U \cup \{\perp\}$
- $o \in U \cup L$
- $mo \in U \cup L \cup \{\perp\}$
- $pa \in P \cup A$

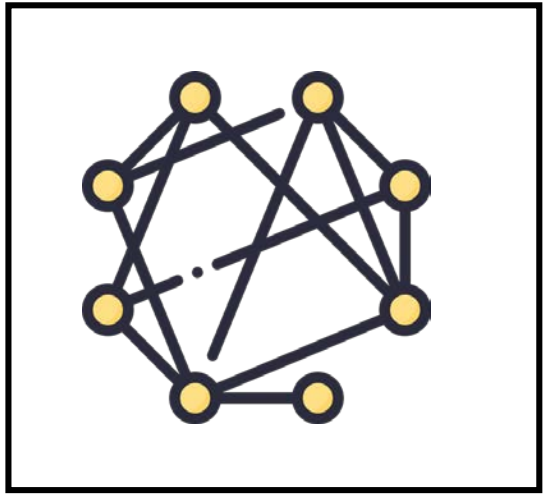
An element (s, pa, o, mp, mo) *is called an* action element *(or simply* action*) when* $pa \in A$*; it is called a* factual element *(or simply* fact*) when* $pa \in P$*. We denote by* $\mathcal{A}$ *the set of all actions and by* $\mathcal{F}$ *the set of all facts.*

Example (instantiation):

Action Element: (:alice, :register, :boulevard18, :at, :21-08-2022)

Factual Element: (:alice, :type, :Person); (:alice, :moveTo, :boulevard18, :at, :22-08-2022); (:boulevard18, :type, :Address)

The UCP Framework
Knowledge Bases



- Factual elements
- Action elements (executed)

Example:

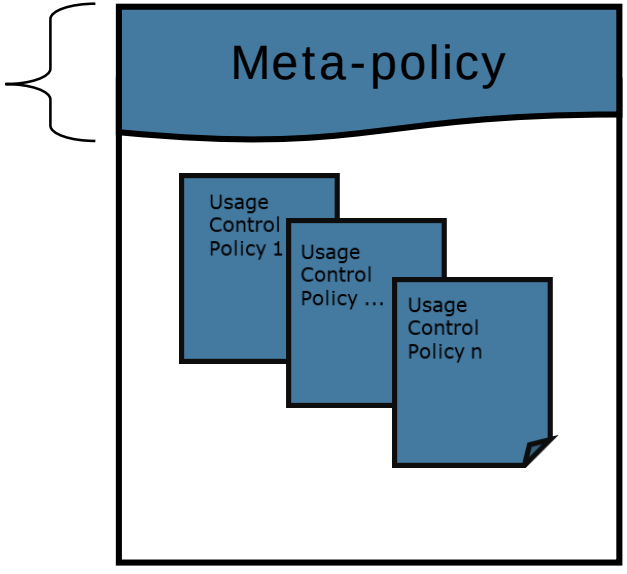
(:alice, :moveTo, :boulevard18, :at, :21-08-2022)
(:alice, :type, :Person)
(:boulevard18, :type, :Address)
(:alice, :register, :boulevard18, :at, :22-08-2022)

The UCP Framework
Modality Conflicts

- Given an elemen pattern *a*, modality conflicts arrise when:
  - **O**a and **P**a: both obligated and prohibited from doing a
  - **A**a and **P**a: both permitted and prohibited from doing a
  - **O**a and **D**a: both obligated and exempt from doing a

The UCP Framework
Usage Control meta-Policies

- Rules
- Precedence relationship ≤: order between rules
- Conflict resolution



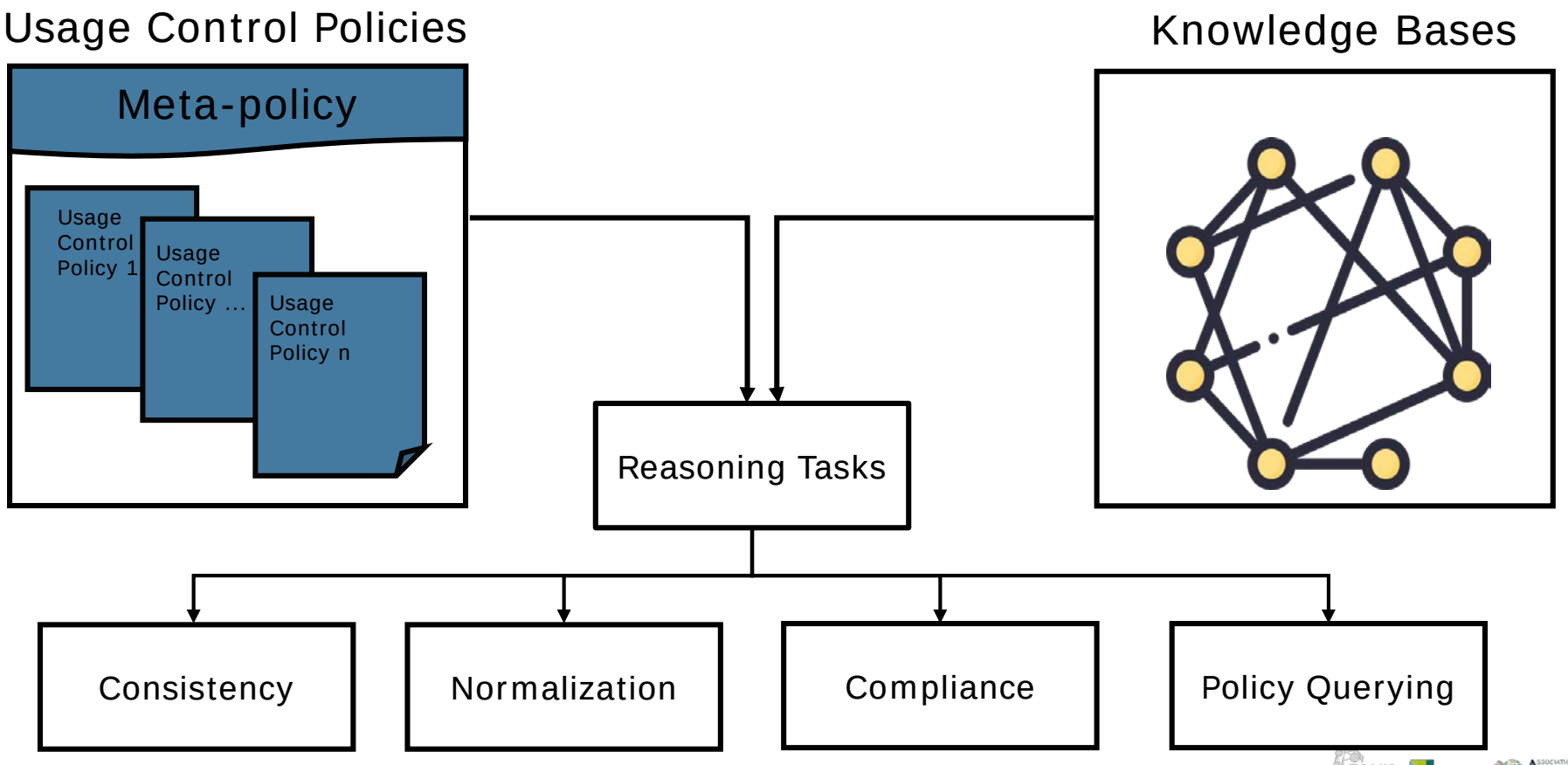
Precedence Strategies

- Negative policies override positive ones
- Specific overrides general
- New law overrides old law
- Etc.

Example (Dispensation overrides Obligation):

For any two rules $r_1 = \text{cond}_1 \rightsquigarrow \mathbf{D}a_1$, $r_2 = \text{cond}_2 \rightsquigarrow \mathbf{O}a_2$, such that $a_1 = a_2$, it holds that $r_2 \leq r_1$.

The UCP Framework
Overview



Reasoning Tasks
Consistency Checking

Example:

Rule 1. A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria:

Rule 1. (?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) ⇝ **O**(?x, :register, ?y, …, ….)

Rule 1'. (?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) ⇝ **D**(?x, :register, ?y, …, …)

Inconsistent Policy

Reasoning Tasks
Normalization

Example:

Rule 1. A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria:

Rule 1. (?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) $\rightsquigarrow$ **O**(?x, :register, ?y, …, …)

Rule 1'. (?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) $\rightsquigarrow$ **D** (?x, :register, ?y, …, …)

Given that Dispensation overrides Obligation: **Rule 1' would override Rule 1**

The new normalized policy would retain only Rule 1'

Reasoning Tasks
Compliance Checking

Example:

Rule 1. A person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria.

Policy rule
(?x, :moveTo, ?y). (?x, :type, :Person). (?y, :type, :Address) $\rightsquigarrow$ **O**(?x, :register, ?y, :within, :threeDays)
KB
(:alice, :moveTo, :boulevard18, :at, :21-08-2022)
(:boulevard18, :type, :Address)
(:alice, :type, :Person)
(:alice, :register, :boulevard18, :at, :22-08-2022)

Compliant or not?

Reasoning Tasks
Policy Querying

Example:

Given **Rule 1.** a person is obliged to register their address with one of the local authorities within three days of changing residence or having moved from abroad to Austria.

Question: I would like to move to austria, what are my obligations?

Future Steps
Instantiation

- Different Initiatives:
  - ODRL (*Ontology Engineering Group at Universidad Politécnica de Madrid*)
  - SHACL (*L3S research center at Leibniz Universität Hannover*)
  - RDF surfaces (*IDLab at Ghent University*)
  - Description Logics (*us*)

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

Questions

- Use cases
  - So far, the address registration process
  - Others: intellectual property protection, privacy protection, compliance with regulations and digital rights management
- Language representation (DLs, ODRL, etc.)
- Benchmark (The SPECIAL benchmark[1])

[1] Kirrane et al. (2020) The SPECIAL-K Personal Data Processing Transparency and Compliance Platform. https://arxiv.org/abs/2001.09461

References

[1] Park, Mason, G., & Sandhu, R.S. (2004). The UCON ABC Usage Control Model.

[2] Colombo, M., Lazouski, A., Martinelli, F., Mori, P. (2010). A Proposal on Enhancing XACML with Continuous Usage Control Features. In: Desprez, F., Getov, V., Priol, T., Yahyapour, R. (eds) Grids, P2P and Services Computing. Springer, Boston, MA.

[3] Reina Quintero, Antonia & Pérez, Salvador & Varela Vaca, Angel & Gómez López, María Teresa & Cabot, Jordi. (2021). A domain-specific language for the specification of UCON policies.

[4] Hilty, M., Pretschner, A., Basin, D.A., Schaefer, C., & Walter, T. (2007). A Policy Language for Distributed Usage Control. ESORICS.

[5] Uszok, Andrzej & Bradshaw, Jeffrey & Jeffers, R. & Suri, Niranjan & Hayes, Patrick & Breedy, Maggie & Bunch, Larry & Johnson, Matthew & Kulkarni, Saee & Lott, James. (2003). KAoS policy and domain services: toward a description-logic approach to policy representation, deconfliction, and enforcement. Proceedings - POLICY 2003: IEEE 4th International Workshop on Policies for Distributed Systems and Networks. 93- 96.

[6] Kagal, L., Finin, T., Joshi, A. (2003). A Policy Based Approach to Security for the Semantic Web. In: Fensel, D., Sycara, K., Mylopoulos, J. (eds) The Semantic Web - ISWC 2003. ISWC 2003. Lecture Notes in Computer Science, vol 2870. Springer, Berlin, Heidelberg.

[7] A W3C working group (2018). The Open Digital Rights Language (ODRL). https://www.w3.org/TR/odrl-model/

[8] Bonatti, P.A., Kirrane, S., Petrova, I.M. *et al.* (2020). Machine Understandable Policies and GDPR Compliance Checking. *Künstl Intell* 34, 303–315 (2020). https://doi.org/10.1007/s13218-020-00677-4

[9] Quyet H. Cao, Madhusudan Giyyarpuram, Reza Farahbakhsh, and Noel Crespi. (2020). Policy-based usage control for a trustworthy data sharing platform in smart cities. Future Gener. Comput. Syst. 107, C (Jun 2020), 998–1010. https://doi.org/10.1016/j.future.2017.05.039