J. M. Bradshaw, A. Uszok, M. Breedy,
L. Bunch, T. Eskridge, P. Feltovich,
M. Johnson, J. Lott and M. Vignati

The KAoS Policy Services Framework

Objective: A digital policy management framework for defining, analyzing, deconflicting, and enforcing semantically-rich policy constraints for virtually any application domain.

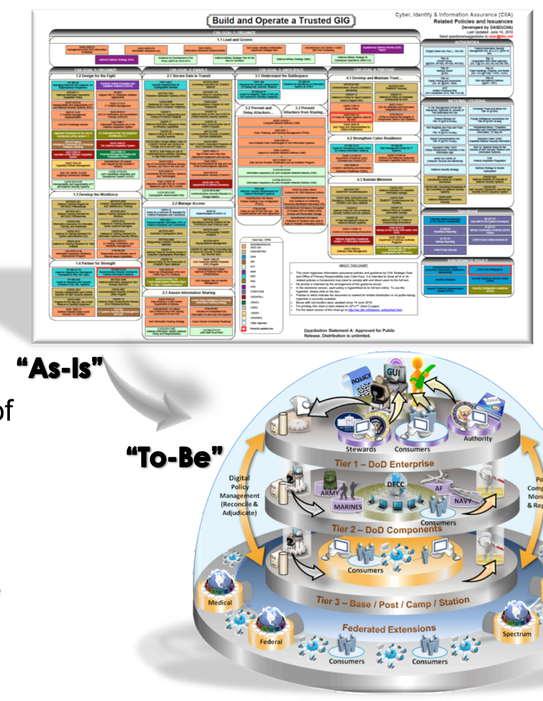
What Is KAoS?

- Handles both obligation and authorization policies
- Uses W3C standard OWL 2 as knowledge representation
- OWL policies can be defined in point-and-click fashion
- Uses general, spatial, temporal, and domain-specific reasoners for policy decisions
- Powerful analysis and conflict resolution algorithms available
- "Compiles" policies for efficient policy enforcement decisions
- Used for networks, access, human-agent teams, cyber…

Why Use OWL for Digital Policy Management?

OWL and DPM

- The US Government-sponsored Digital Policy Management (DPM) has adopted an OWL-based approach to policy representation.
- KAoS was the first to offer an ontology-based approach to policy, and is currently the most successful and mature of all such policy management systems.
- IHMC is collaborating with DPM to establish a common core ontology standard as the basis for future standards efforts in DPM.



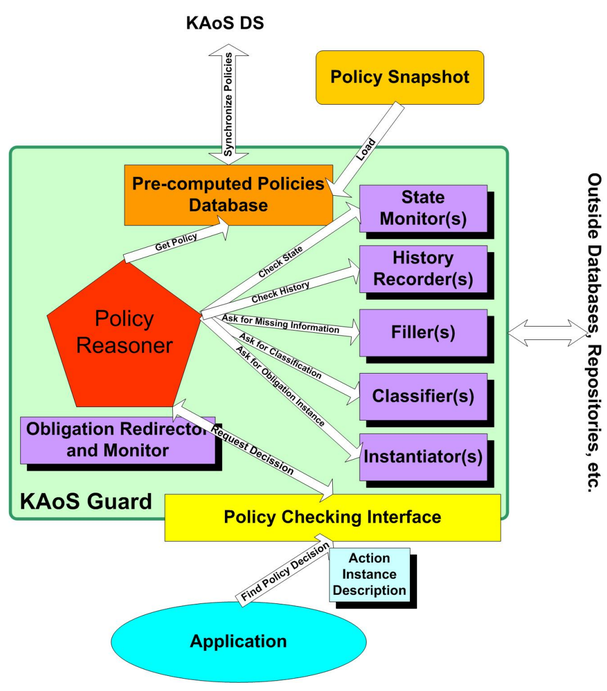
How OWL-based Policy Addresses DPM Challenges

• Policy generated at multiple levels of an Enterprise cannot be shared	• Can represent policy from different perspectives and at multiple levels of abstraction
• Difficult to identify conflicting or inconsistent policies	• Efficient description-logic-based deconfliction algorithms
• Multiple policy languages	• Expressiveness of OWL semantics obviates the need for multiple languages
• Current implementations not integrated across Enterprise	• Can provide end-to-end system integration across multiple policy domains
• Difficulty in translating policies from one language to another	• Expressiveness of OWL semantics enable automatic translation of niche-specific policy languages, if necessary

Advanced Features of KAoS

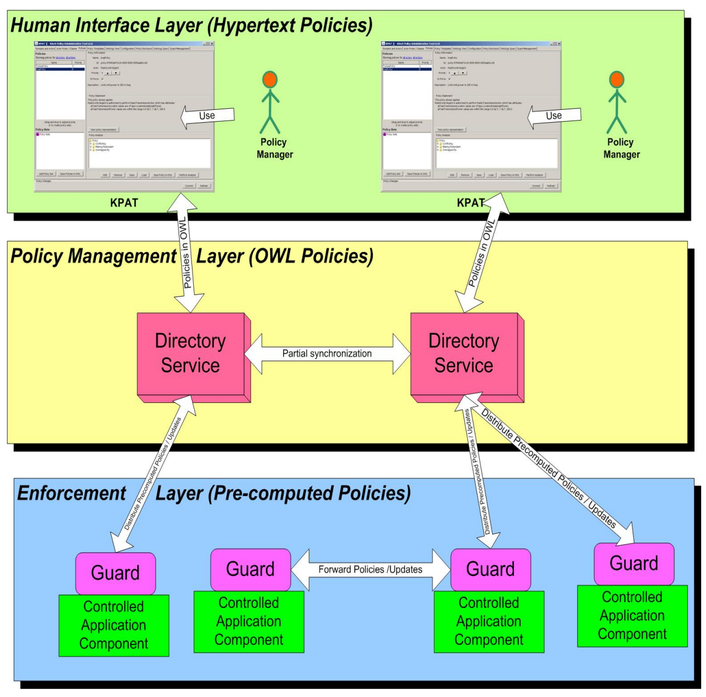
- *Policy Templates* simplify the creation of complex domain-specific policies
- *Custom GUIs* can replace the standard KPAT and template user interfaces
- *Self-Referential Policies* can be created through the use of KAoS role-value map extensions
- *Numeric, time-based, and geospatial data* is handled appropriately during policy creation
- *Powerful policy analysis tools* are available (e.g., test permission, get obligations, learn options)
- *Complex contextual information* (e.g., states, history) can be taken into account in policy enforcement
- *Priority-based Conflict Resolution* relies on numeric priorities to resolve policy conflicts
- *Precedence-based Conflict Resolution* relies on logical predicates to resolve policy conflicts
- *Spatial and Temporal Reasoners* efficiently resolve complex policy decisions
- *Delegation Reasoning* handles delegation of authority
- *Kaa Meta-Reasoner* uses probabilistic information and maximization of expected value to make decisions about policy exceptions (cf., risk-adaptive access control)
- *DRS Secure Core Module* proposed as tamper-proof platform for hosting of the KAoS Guard in sensitive environments

KAoS Guard



- Where KAoS meets the application - policy decision point
- Checks to see whether the AID is controlled by any policy
- Purple components are examples of optional extensions
- Guard can be populated from policy snapshot when network is not available (e.g., standalone sensors)

KAoS Conceptual Architecture



Human Interface Layer: KPAT is a hypertext-like graphical interface for policy management and specification as English sentences. Vocabulary is automatically provided from the ontologies. Application-specific templates further simplify policy definition.

Policy Management Layer: KPAT encodes and manages policy-related information as OWL. OWL is used by the Directory Service (DS) for policy analysis and deconfliction.

Policy Decision and Enforcement Layer: KAoS automatically "compiles" OWL policies to an efficient lookup format that provides the grounding of abstract ontology terms. These polices are sent from the DS to Guards, which serve as local policy decision points. Guards only receive the subset of policies relevant to the entities that they control. Policies can also be updated in peer-to-peer fashion.

For publications, see http://www.jeffreymbradshaw.net
For technical detail, see http://ontology.ihmc.us

ihmc
FLORIDA INSTITUTE FOR HUMAN & MACHINE COGNITION