IBM Zurich Research Lab

Privacy Policies as a Component of Policy-enabled Governance

M Hondo, T. Nadalin, R. Nagaratnam
IBM Software Group

G. Karjoth, M. Kudoh, B. Pfitzmann, M. Schunter
IBM Research

Outline

- Requirements for Privacy Languages
- Standardization Roadmap
- Summary

Core Language: Expressive and Unambiguous

Expressive

- Processes (notification after access)
- System requirements (trustworthiness, encryption)
- Access Control (which access for what purpose)
- Processing (How should data be handled?)
- Audit (possibilities & requirements)
- Mandatory and discretionary parts (must do, should do)

Unambiguous

- Clear semantics
- Well-defined scope (what is a particular policy talking about?)

Composable and Comparable

Composition: Distributed Authoring

- Connectors (and, or, not, first-applicable…)
- Projection (sub-policies)

Comparison: Enabling Sticky Policies

- Policy1 > Policy2
- Requires
  - Scope
  - Semantics
- Sticky Policies: Send data if Policy2<Policy1

Scope: Corporate Governance

Composition: Distributed Authoring

- Connectors (and, or, not, first-applicable…)
- Projection (sub-policies)

Comparison: Enabling Sticky Policies

- Policy1 > Policy2
- Requires
  - Scope
  - Semantics
- Sticky Policies: Send data if Policy2<Policy1

Parts of the Language / Framework

- a core language
  - including “purpose” and “obligation”
- binding mechanisms
  - to associate with other entities (such as messages, services, …)
- ontologies or vocabularies
  - sector-independent base ontology
  - sector-specific requirements

Compatible with Existing Standards

- HTTP
- SOAP
- WS-Policy
- XACML (if augmented with suitable profiles)
- P3P

Standardization Roadmap - Horizons

1. Engaging people – user-centric policy negotiation
2. Privacy-enhanced access control
3. Access and privacy control for Web Services
4. Interoperability and deployment by means of ontologies
5. Policy exchange, negotiation and consent
6. Governance beyond access

Conclusion

- governance requirements include not only “data labeling” but also policy enforcement
- privacy requirements have to be integrated into the decisions made by people & systems every day

design for privacy-enablement
and do not design systems that only do privacy !

Conclusion (cont'd)

Starting point

- use & extend existing access control to meet basic privacy requirements

Mid point

- provide business & industry with a map of product support including commitment of vendors & interoperability results
- focus on efforts that embed simple, enforceable policies in other deployed standards

End points

- update the language to meet all requirements
- understand the blockers for optimizing systems

Questions?