OASIS

XACML TC
and
Rights Language TC

Hal Lockhart
hal.lockhart@entegrity.com

ENTEGRITY *Solutions* ®

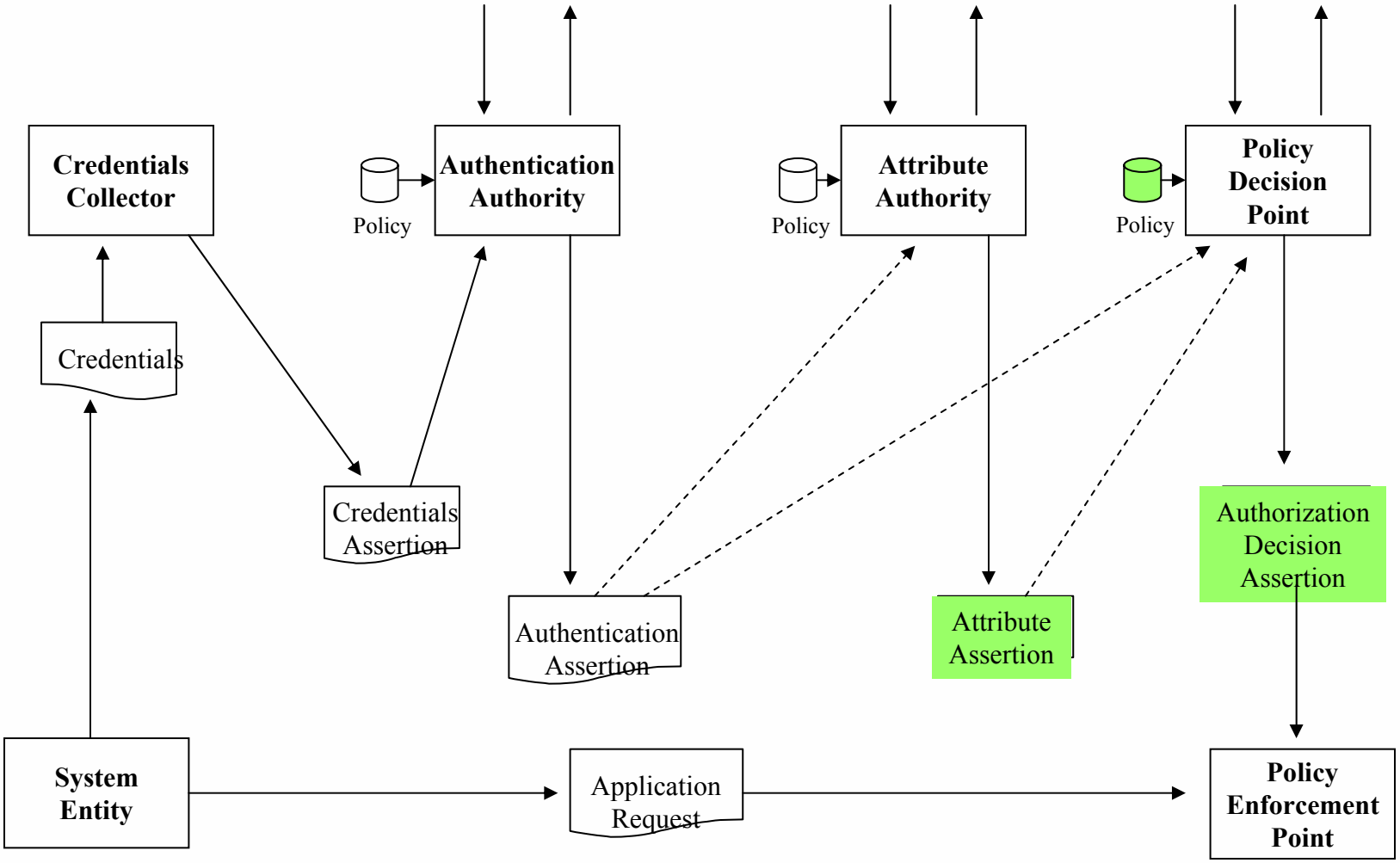
Outline

- Overview & Theory
- XACML TC
- Right Language TC
- Strengths, Applicability, Issues

Forty Thousand Foot View

- Both deal with the problem of Authorization
- Both draw requirements from many of the same application domains
- Both share many of the same concepts (but in some cases use different terms)
- Both base specification on XML Schema
- Each approaches the problem differently

First a Little Theory



ENTEGRITY Solutions

Types of Authorization Info - 1

- Attribute Assertion
  - Properties of a system entity (typically a person)
  - Relatively abstract – business context
  - Same attribute used in multiple resource decisions
  - Examples: X.509 Attribute Certificate, SAML Attribute Statement, XrML PossessProperty
- Authorization Policy
  - Specifies all the conditions required for access
  - Specifies the detailed resources and actions (rights)
  - Can apply to multiple subjects, resources, times…
  - Examples: XACML Policy, XrML License, X.509 Policy Certificate

Types of Authorization Info - 2

- AuthZ Decision
  - Expresses the result of a policy decision
  - Specifies a particular access that is allowed
  - Intended for immediate use
  - Example: SAML AuthZ Decision Statement

Implications of this Model

- Benefits
  - Improved scalability
  - Separation of concerns
  - Enables federation
- Distinctions not absolute
  - Attributes can seem like rights
  - A policy may apply to one principal, resource
  - Systems with a single construct tend to evolve to treating principal or resource as abstraction

XACML TC

ENTEGRITY Solutions®

XACML TC Charter

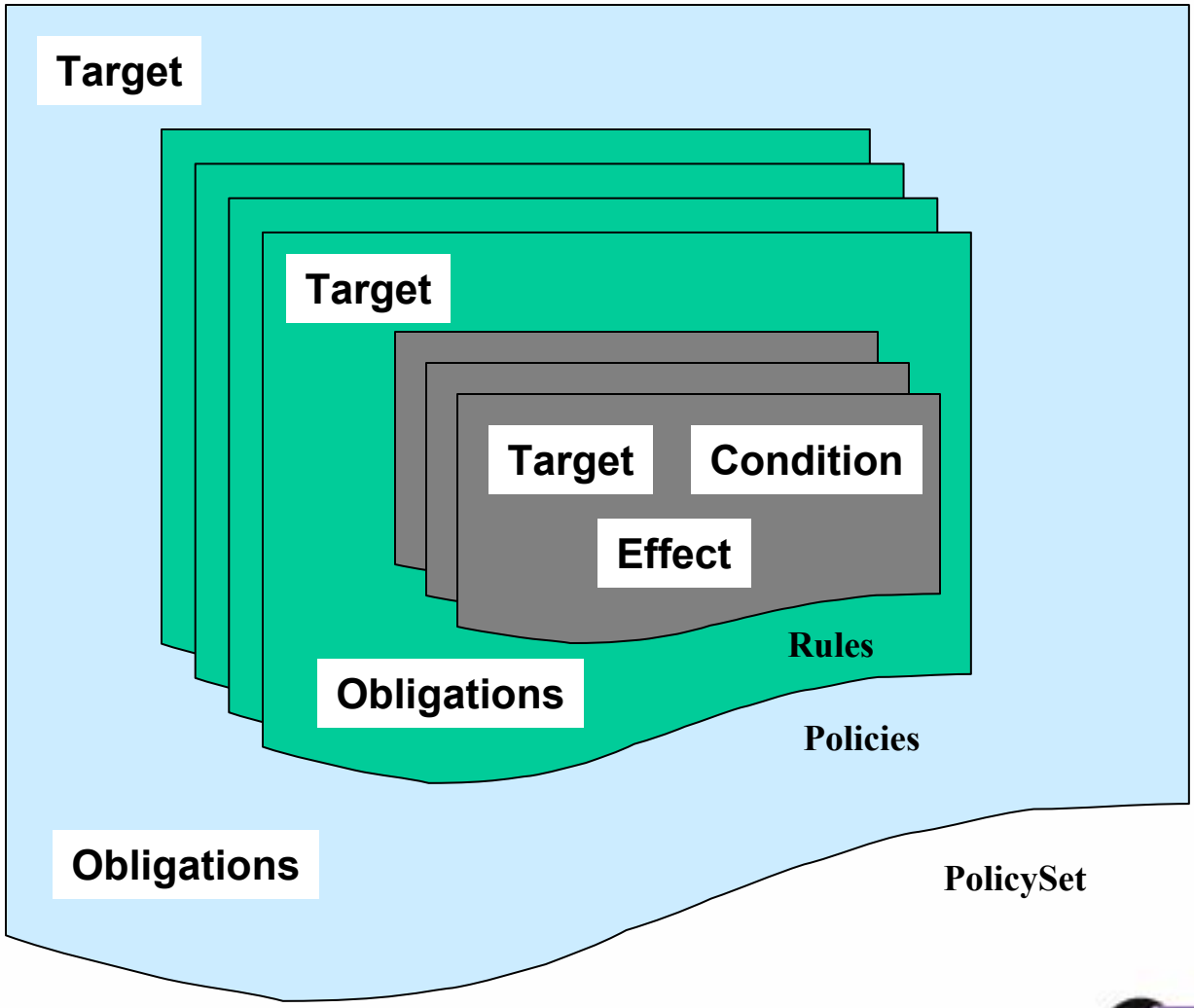
- Define a core XML schema for representing authorization and entitlement policies
- Target - any object - referenced using XML
- Fine grained control, characteristics - access requestor, protocol, classes of activities, and content introspection
- Consistent with and building upon SAML

XACML Membership

- Affinitex
- Crosslogix
- Entegrity Solutions
- Entrust
- Hitachi
- IBM
- OpenNetwork
- Overxeer, inc.
- Sterling Commerce
- Sun Microsystems
- Xtradyne
- Various individual members

ENTEGRITY Solutions

XACML Concepts



ENTEGRITY Solutions

XACML Concepts

- Policy & PolicySet – combining of applicable policies using CombiningAlgorithm
- Target – Rapidly index to find applicable Policies or Rules
- Conditions – Complex boolean expression with many operands, arithmetic & string functions
- Effect – “Permit” or “Deny”
- Obligations – Other required actions

XACML Status

- First Meeting – 21 May 2001
- Weekly or bi-weekly calls – 7 F2F Meetings
- Requirements from: Healthcare, DRM, Registry, Financial, Online Web, XML Docs, Fed Gov, Workflow, Java, Policy Analysis, WebDAV
- Deliverables: Glossary, Usecases & Requirements, Domain Model, 2 Schemas, Policy Semantics, Conformance Tests, Profiles, Security & Privacy Considerations, Extensibility Points
- Vote for Committee Specification – 28 August 2002
- Submit to OASIS – 1 December 2002 (or before)

Rights Language TC

ENTEGRITY *Solutions* ®

Rights Language Technical Committee (RLTC)

Charter (condensed)

1. Define the industry standard for a rights language that supports a wide variety of business models and has an architecture that provides the flexibility to address the needs of the diverse communities that have recognized the need for a rights language. The language needs to be:
    1. Comprehensive: Capable of expressing simple and complex rights
    2. Generic: Capable of describing rights for any type of digital content or service
    3. Precise: Communicates precise meaning to all components of the system
    4. Interoperable: Comprehends it is part of an integrated system
    5. Agnostic: To platform, media type or format
2. Use XrML as the basis in defining the industry standard rights language in order to maximize continuity with ongoing standards efforts.
3. Define governance and language extension process…
4. Liaison with complementary standards…(eg. web services)
5. Define relationship and establish liaisons with standards bodies that have identified the need for a rights language

(complete Charter at http://www.oasis-open.org/committees/rights/)

ENTEGRITY Solutions

Rights Language Technical Committee (RLTC)

Broad Cross Value Chain Membership:

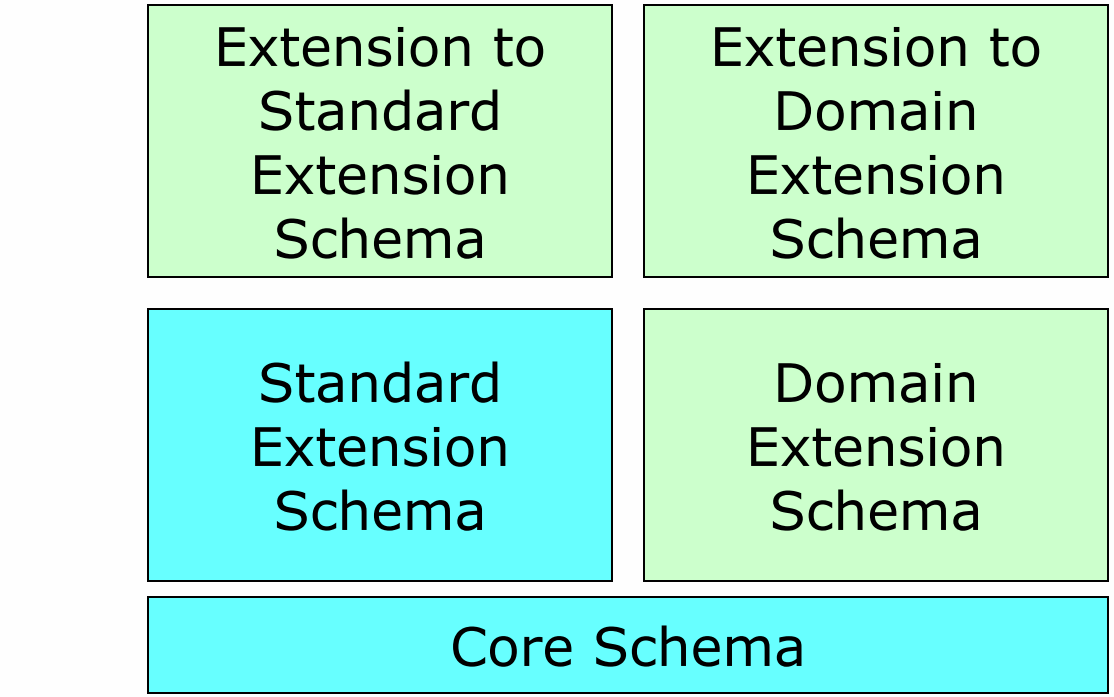
Cisco Systems
Commerce One
ContentGuard
Entrust
Entegrity Solutions
H.P.
IBM
Lexis-Nexis
Microsoft
Sony
Sun
Verisign

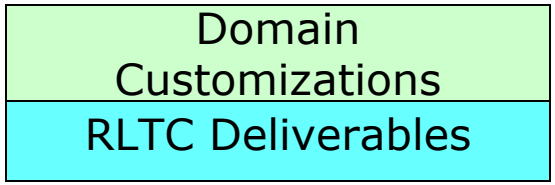
Plus Various Individual Members

ENTEGRITY Solutions

Rights Language Technical Committee (RLTC)

RLTC Schema Deliverables:

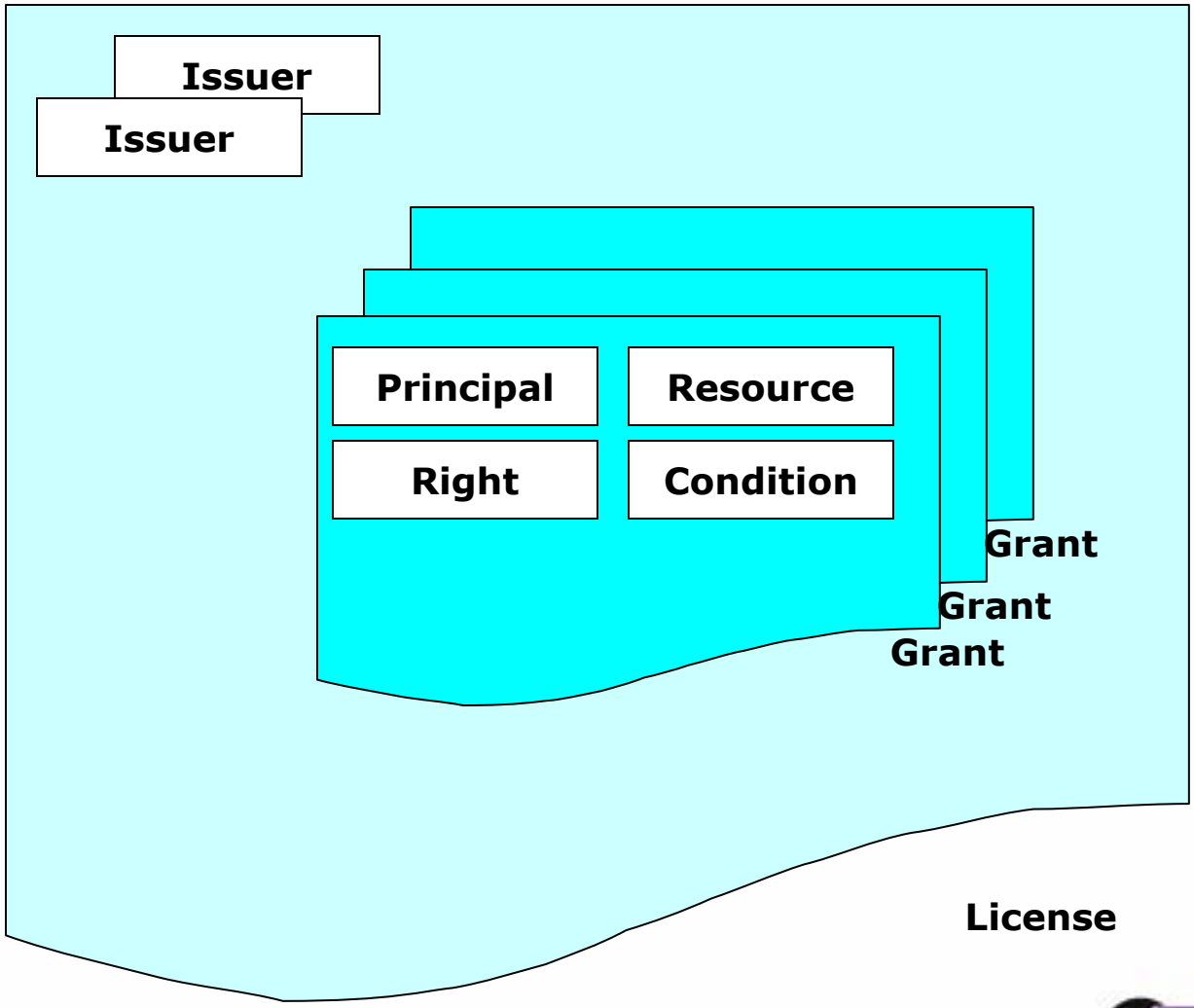




ENTEGRITY Solutions

Rights Language Technical Committee (RLTC)

XrML Basic Data Constructs



ENTEGRITY Solutions

Rights Language Technical Committee (RLTC)

Status:

1. **XrML 2.1 submitted and accepted**
    1. **Originated from Xerox PARC in early 1990s**
2. **Liaisons developed/developing with Global Standards Organizations**
    1. **ISO/IEC JTC1/SC29/WG11 (MPEG-21) – Class C Liaison**
        1. **XrML being used as the foundation of the MPEG-21 REL**
    2. **TV-Anytime Forum**
3. **Schedule developed for OASIS Spec Submission on 12/1/02**
4. **RLTC Organization developed and operational**
    1. **Governance-Liaison Subcommittee ("SC")**
    2. **Requirements SC**
    3. **Core and Standard Specification SC**
    4. **Examples SC**
    5. **Profiles SC**
    6. **Extensions SC**
5. **RLTC a member of OASIS Security Joint Committee**

ENTEGRITY Solutions

Web Services Security

- SAML, XACML and RLTC Spec can all convey AuthZ Info – carry in SOAP header
- Possible use in Policy Advertisement
- Issues
  - Substantial overlap between SAML/XACML & XrML - not clear what is best for what use
  - Intellectual Property Issues
  - Controversies over DRM itself
  - XACML and XrML are complex, will take time to understand