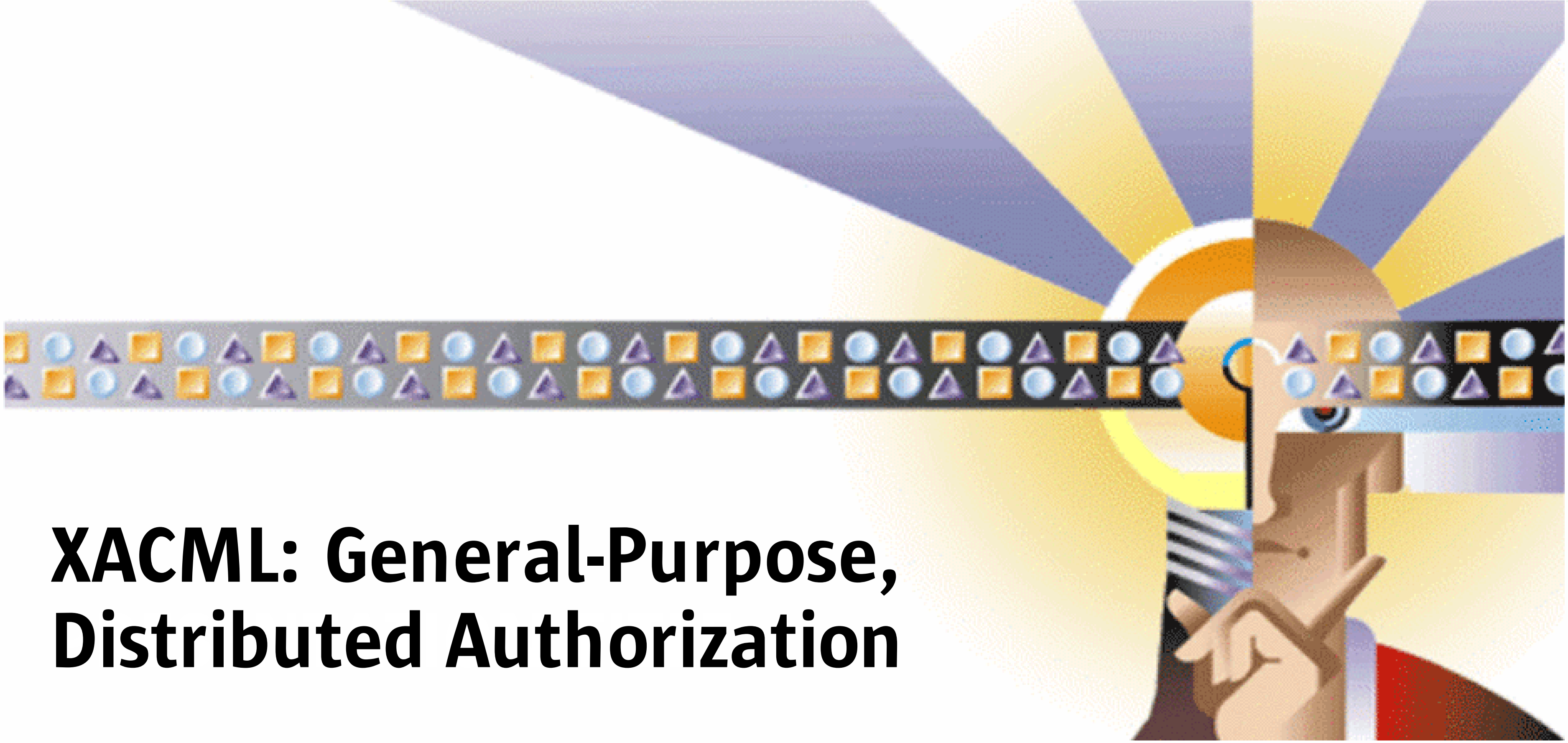


XACML: General-Purpose, Distributed Authorization

Seth Proctor

Member of Technical Staff

Sun Microsystems Laboratories

Sun microsystems
We make the net work.

Outline

- Introduction & Motivations
- Brief Tour of XACML
- Sun's Implementation
- Current & Future Directions

Authorization Policy

- Authorization is “what you can do”
  - Identity, Groups, Attributes, Roles, etc.
- Decision made based on Access Control Policies
  - Typically a question with a yes/no response

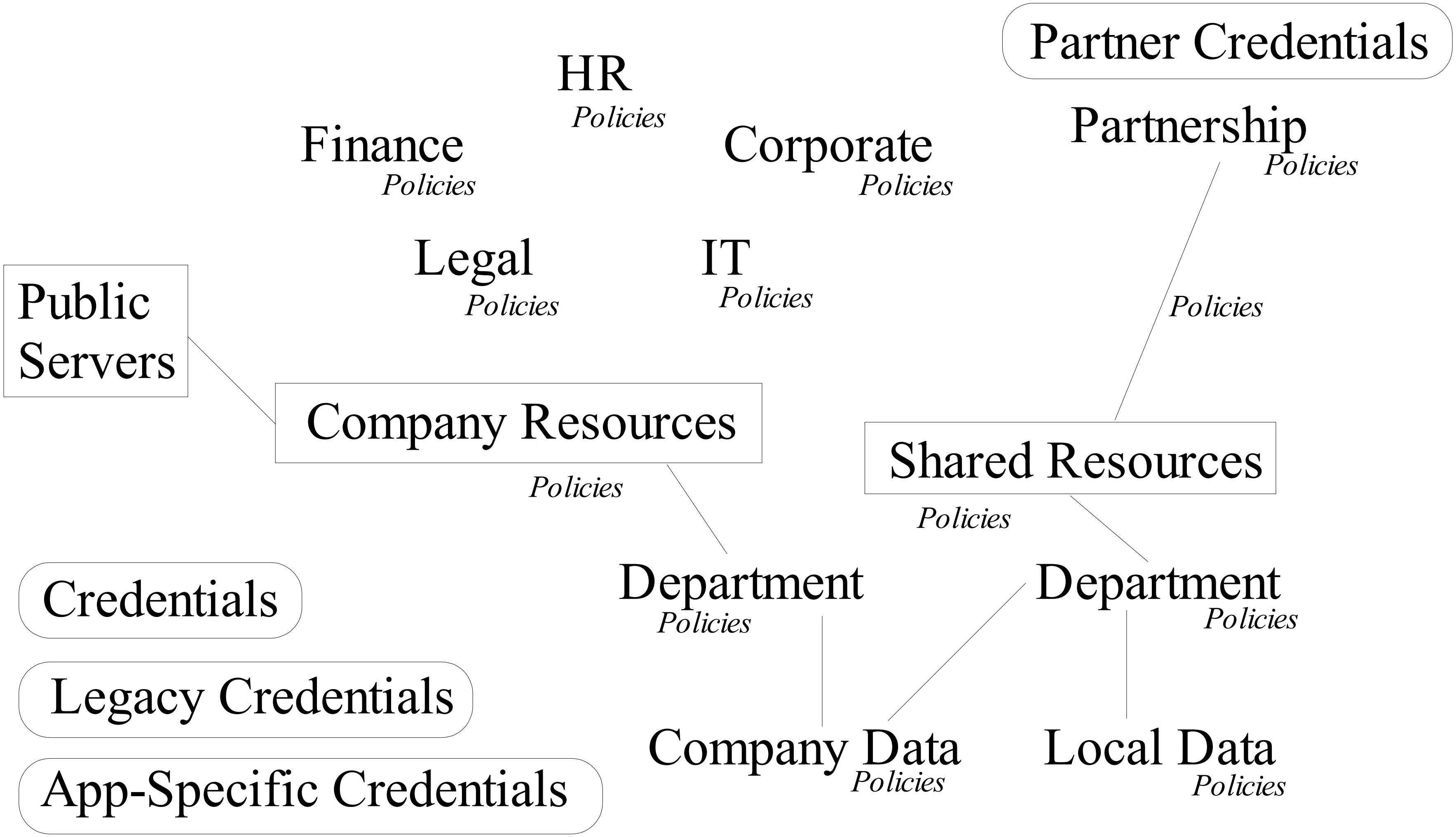
What is XACML?

- The eXtensible Access Control Markup Language is an OASIS Open Standard
  - Standardized in February 2003
- General-purpose access control policy and query languages
- Designed to work in a distributed, decentralized environment

Why XACML?

- Designed to help enterprises scale
  - Easier administration and interoperability
  - Easier for development and deployment
  - Share a single language, share tools
- Useful as an intermediate language
- Ties into legacy systems “easily”
  - No requirements about what supplies info

Does This Sound Familiar?



HR
Policies

Finance
Policies

Corporate
Policies

Partner Credentials

Partnership
Policies

Legal
Policies

IT
Policies

Policies

Public Servers

Company Resources
Policies

Shared Resources
Policies

Credentials

Legacy Credentials

App-Specific Credentials

Department
Policies

Department
Policies

Company Data
Policies

Local Data
Policies

XACML Specification

- Separation of PEP and PDP
- Processing and applicability semantics
- Standard datatypes and functions
  - New ones can easily be defined
- Remote referencing model
  - Policies and attributes may be drawn from any arbitrary source, as needed

XACML Policy

- An XACML policy is a tree
  - Each node has applicability criteria
  - Nodes may be placeholders for remote policies
  - The leaf nodes contain predicates
  - Combining algorithms define the relationship between nodes at each level of the tree

XACML Queries

- Request is a collection of Attributes
  - Subjects, Resource, Action, Environment
- Response is a 4-valued “boolean”
  - May include status codes and messages
  - May include Obligations

SunXACML

- Open Source & written in the Java™ Programming Language
- Full support for XACML 1.0/1.1
- Pluggable and extensible
- Well documented with many examples
- Actually being used in large systems

XACML 2.0 & Related Work

- XACML 2.0 (June 2004-ish)
  - Several new features and enhancements
- Related standards working with XACML
  - SAML 2.0, ebXML Registry 2.x, GGF, etc.
- Profile work in the XACML TC
  - RBAC, WSPL, LDAP, Resource Hierarchies, etc.

Current & Future Research

- Protocols & Performance
- Privacy & Trust Negotiation
- Delegation
- Visualization & Management
- Reasoning

Conclusion

- XACML is an open standard for general-purpose, decentralized Access Control
  - Powerful and scalable
  - Driven by real-world use-cases
  - Reviewed by security and language experts
- An Open Source implementation makes it easy to get started
  - Other free and commercial systems too

References

- The XACML TC

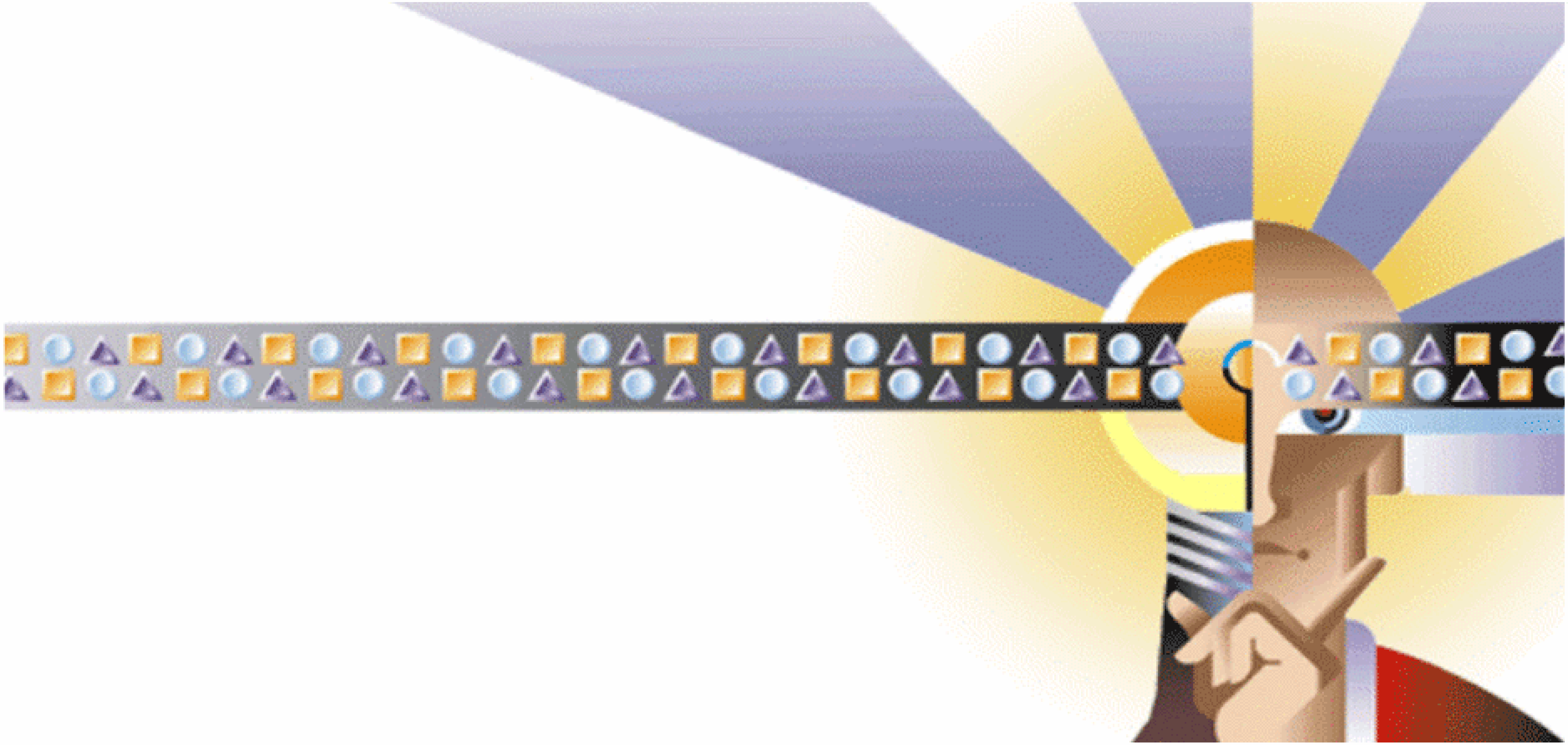
  http://www.oasis-open.org/committees/xacml

- Sun's XACML Implementation

  http://sunxacml.sourceforge.net

- SunLabs

  http://research.sun.com



Seth Proctor

seth.proctor@sun.com

Sun microsystems

We make the net work.