Policy Negotiation in Support of Interoperability

Problem and Charter Definition Meeting

21 February 2003

Purpose

This meeting will focus on the characterization of the policy related functionality required to support the interoperable use of mechanisms, including, but not limited to, the SOAP message security mechanisms being defined by the Web Services Security TC. The purpose of the meeting will be to capture these requirements in proposed charters for one or more open forums that will serve the industry by providing solutions to these important problems.

Expectations

In this meeting, we will not attempt to craft or enhance a technical specification built on contributions from the attendees. No attendee should have any expectations regarding the confidentiality of this meeting, its contents, or its results. Each speaker must be responsible for what they choose to say, keeping in mind that no expectation of confidentiality should be presumed to apply to the statements they make.

Agenda

- 10:00-10:15 Welcome and Introductions
- 10:15-10:30 Agenda Review and Refinement
- 10:30-12:15 Use Cases and Example Scenarios
- 12:15-12:45 Lunch/Break
- 12:45-2:15 Problem Decomposition
- 2:15-2:30 Break/Lunch
- 2:30-4:00 Work Descriptions
- 4:00-4:15 Break
- 4:15-5:45 Chartering Discussion
- 5:45-6:00 Wrap up

Informal Scope of it

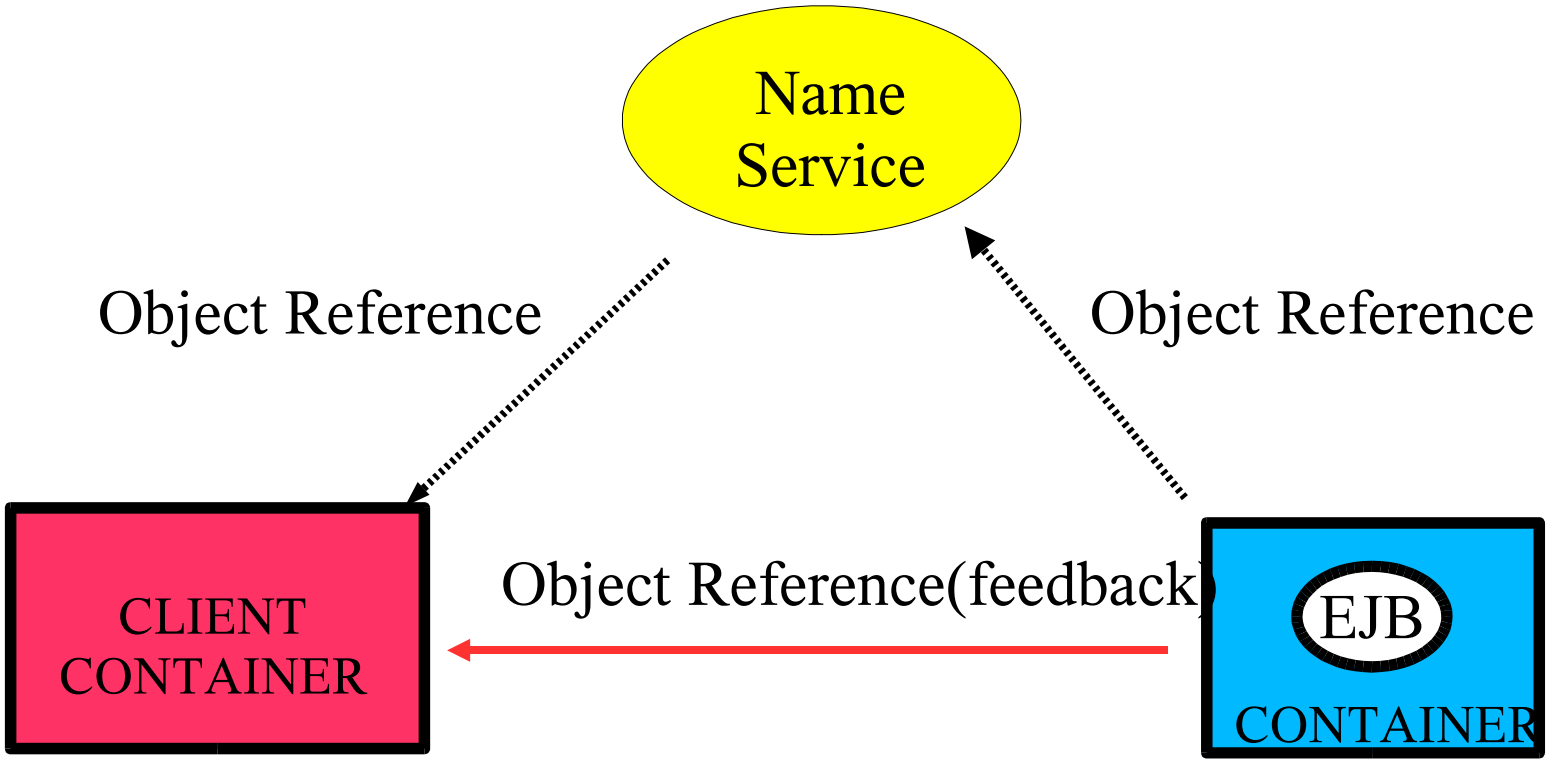
- The requirements and capabilities that affect the nature of the interactions entities will participate in with other systems
  - Requirements – behaviors that an entity demands of its peers
  - Capabilities – behaviors that an entity offers to support the requirements of a peers
- Discussion of how it is admin'ed from enterprise perspctive, predetermined agreement

Use Cases and Example Scenarios

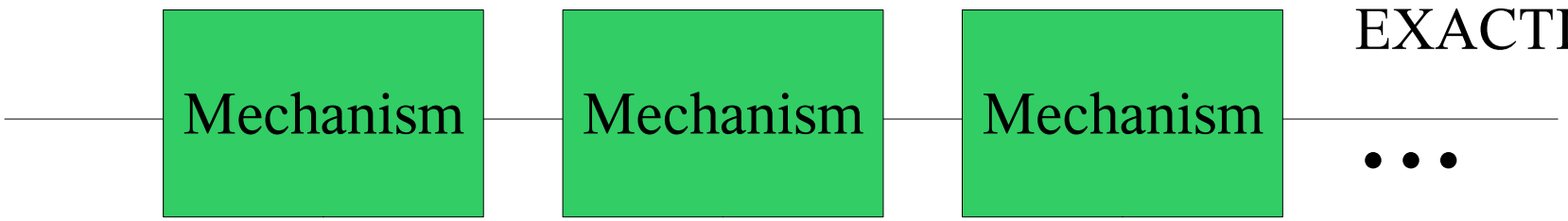
Some Considerations

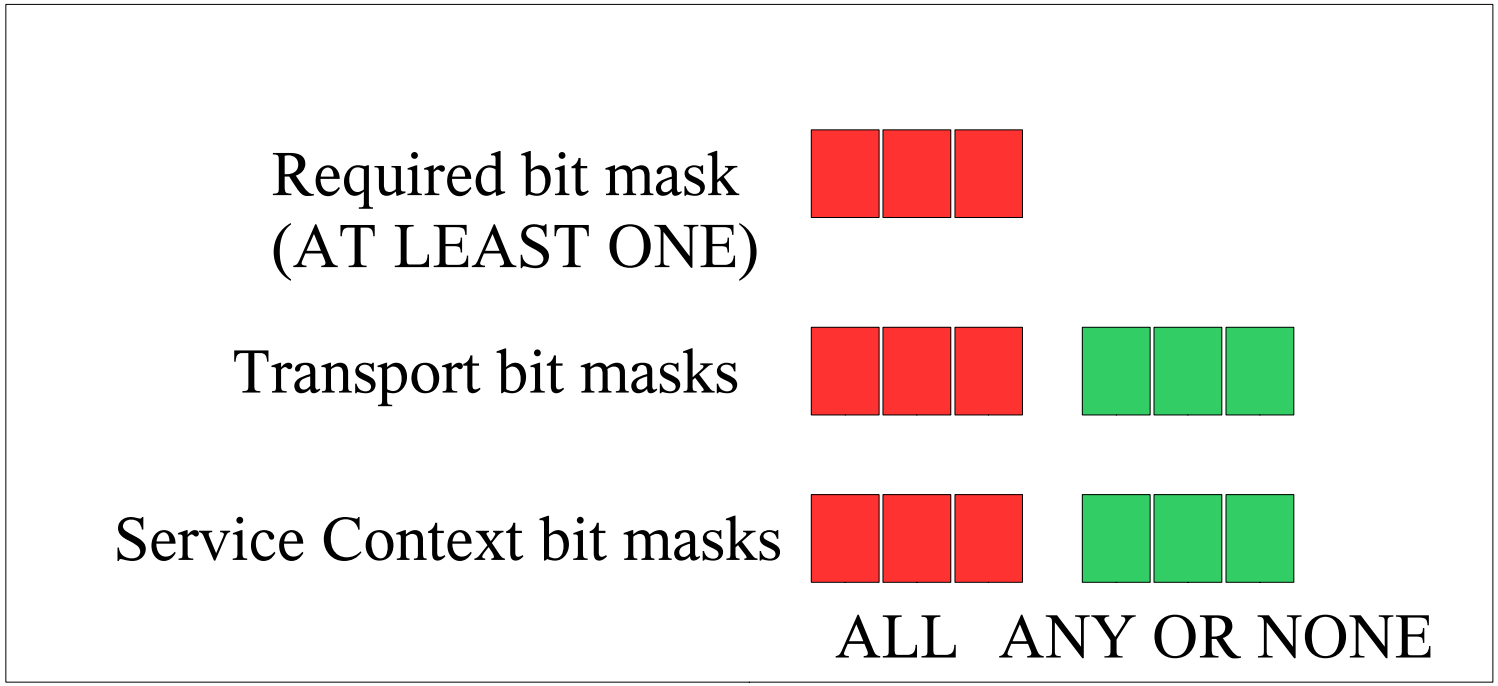
- What types of policy negotiation problems do we seek solutions for?
- What is the nature of the interactions whose properties are being negotiated?
- What is the relationship of the negotiation to the interaction whose properties are being negotiated?
- Where in the interactions is there a need to apply the policies of the various actors in an interaction?

Control Channel



Service Policy In Object Reference

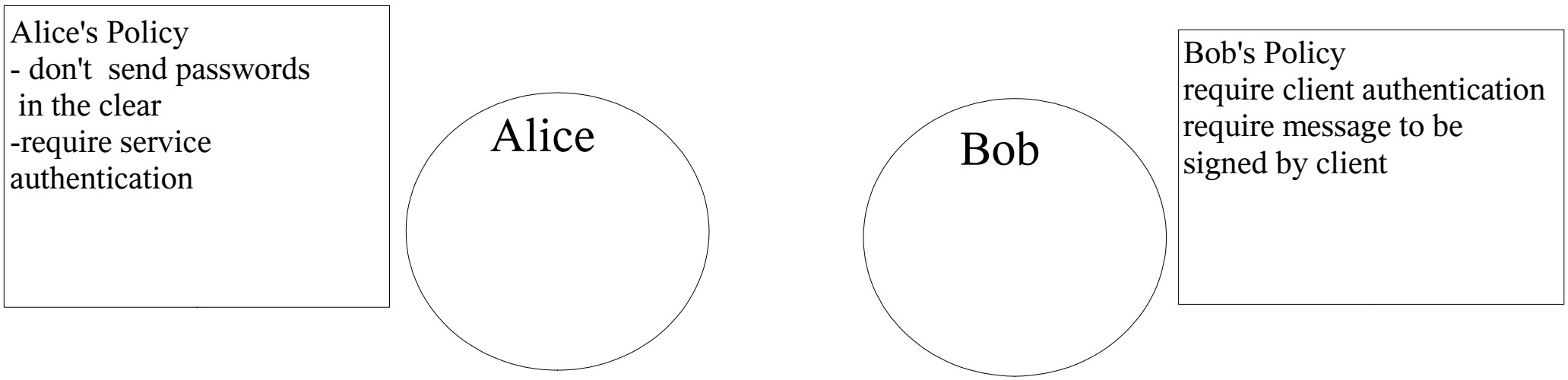




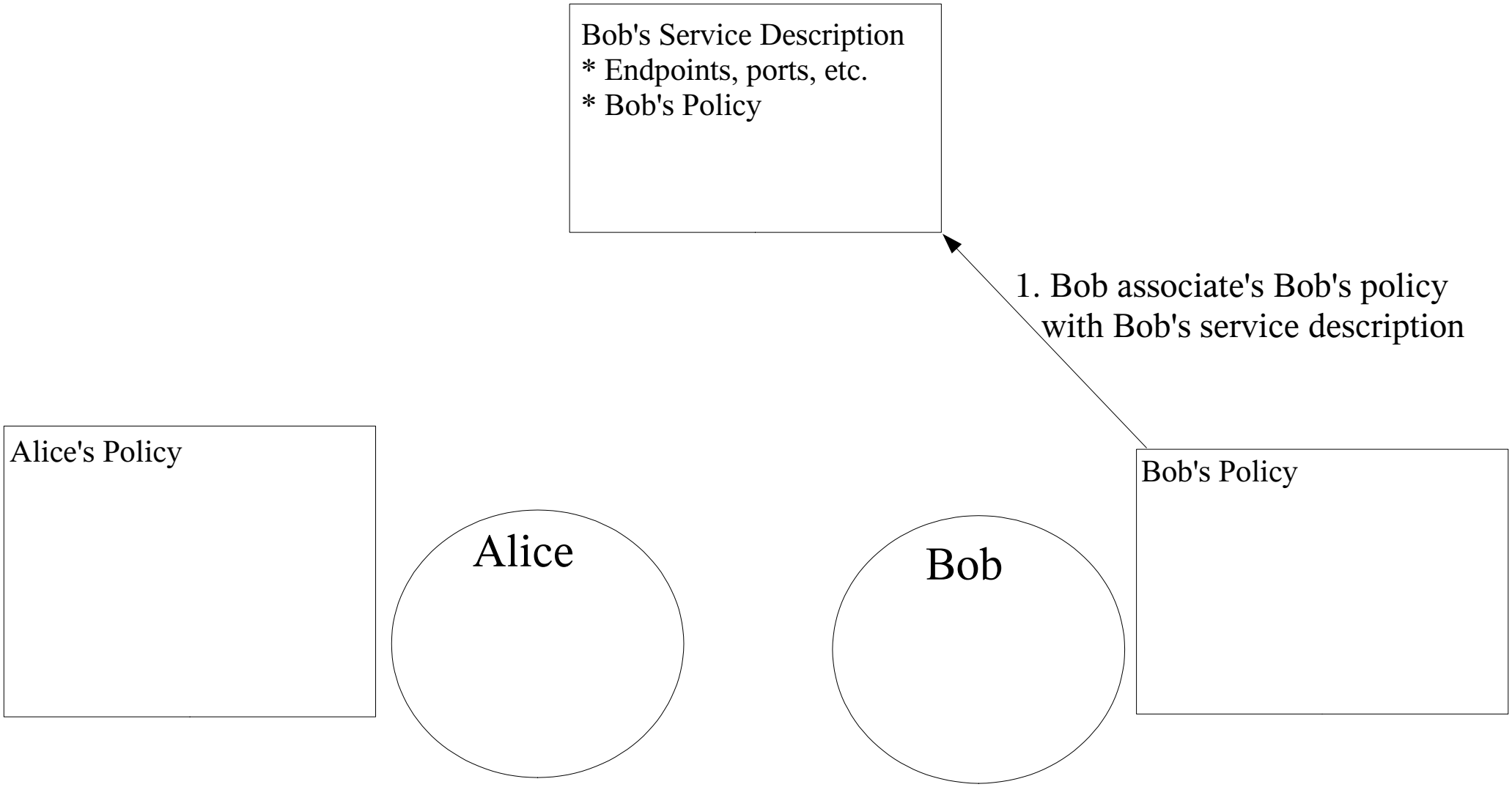
Bit positions correspond to behaviors (e.g client must authenticate)

Alice Wants to Have A secure Message Exchange with Bob

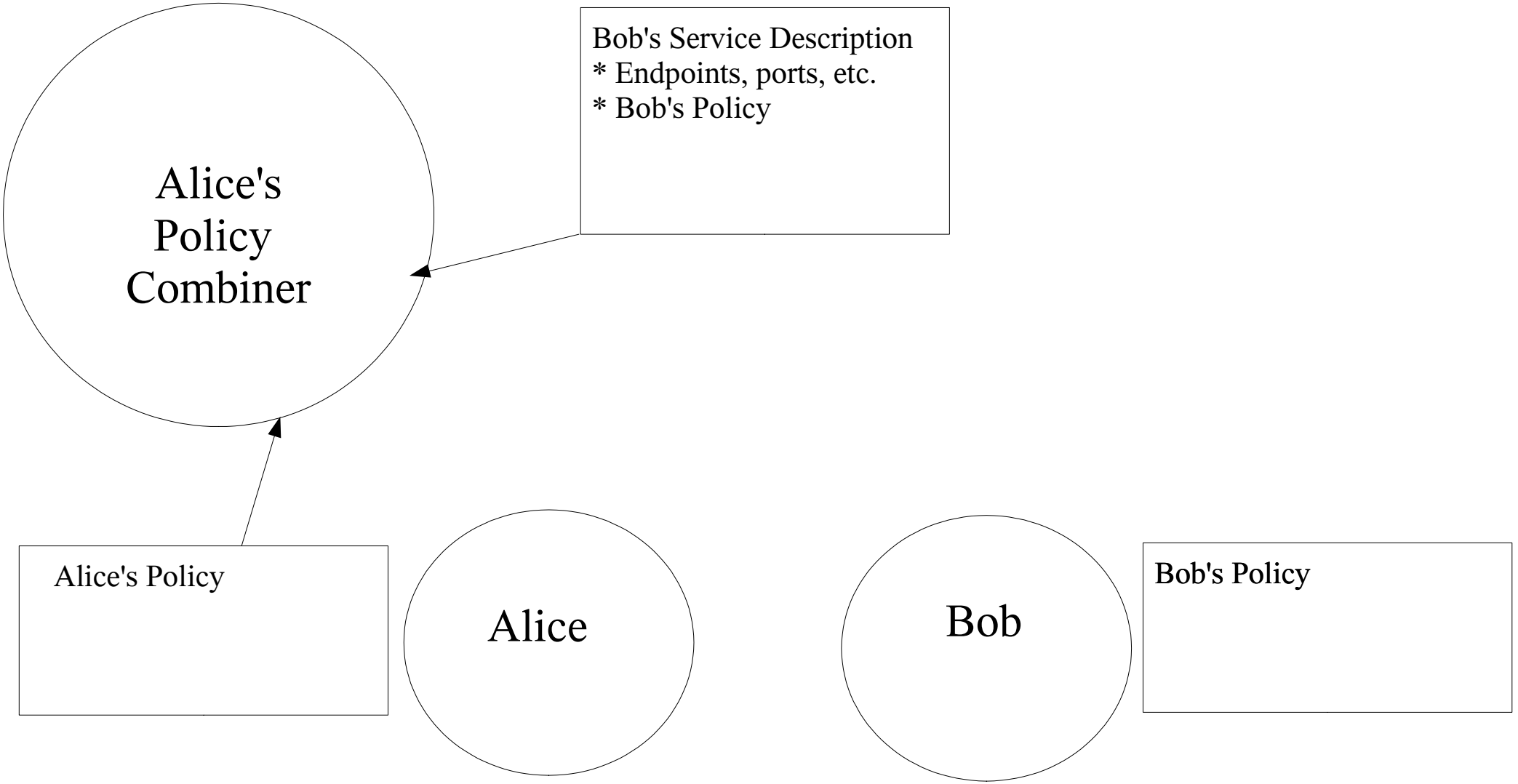
- Bob and Alice each have certain policy requirements and capabilities
- Secure message exchange can only happen if there is an intersection between Alice and Bob's policies



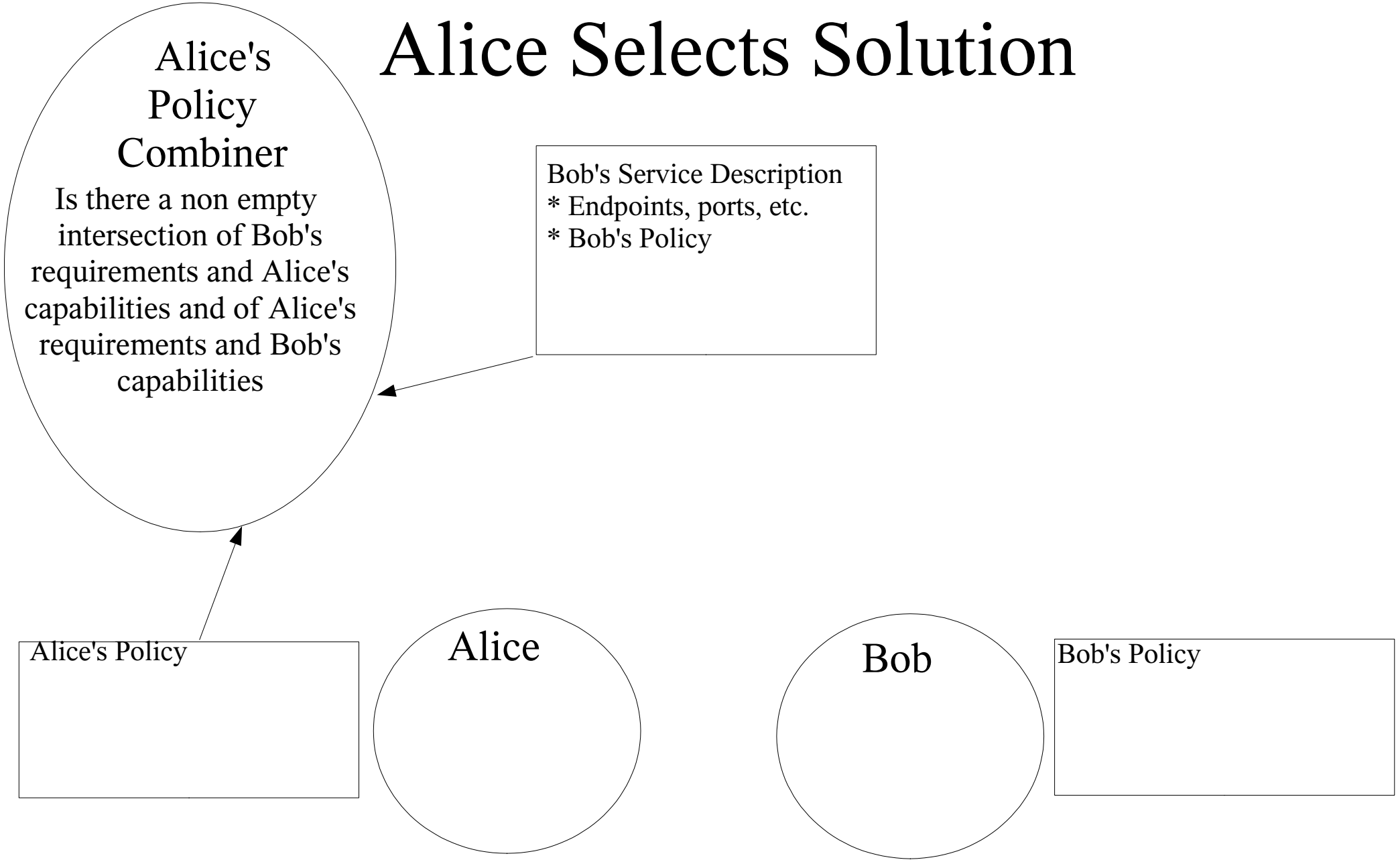
Bob Exports Policy



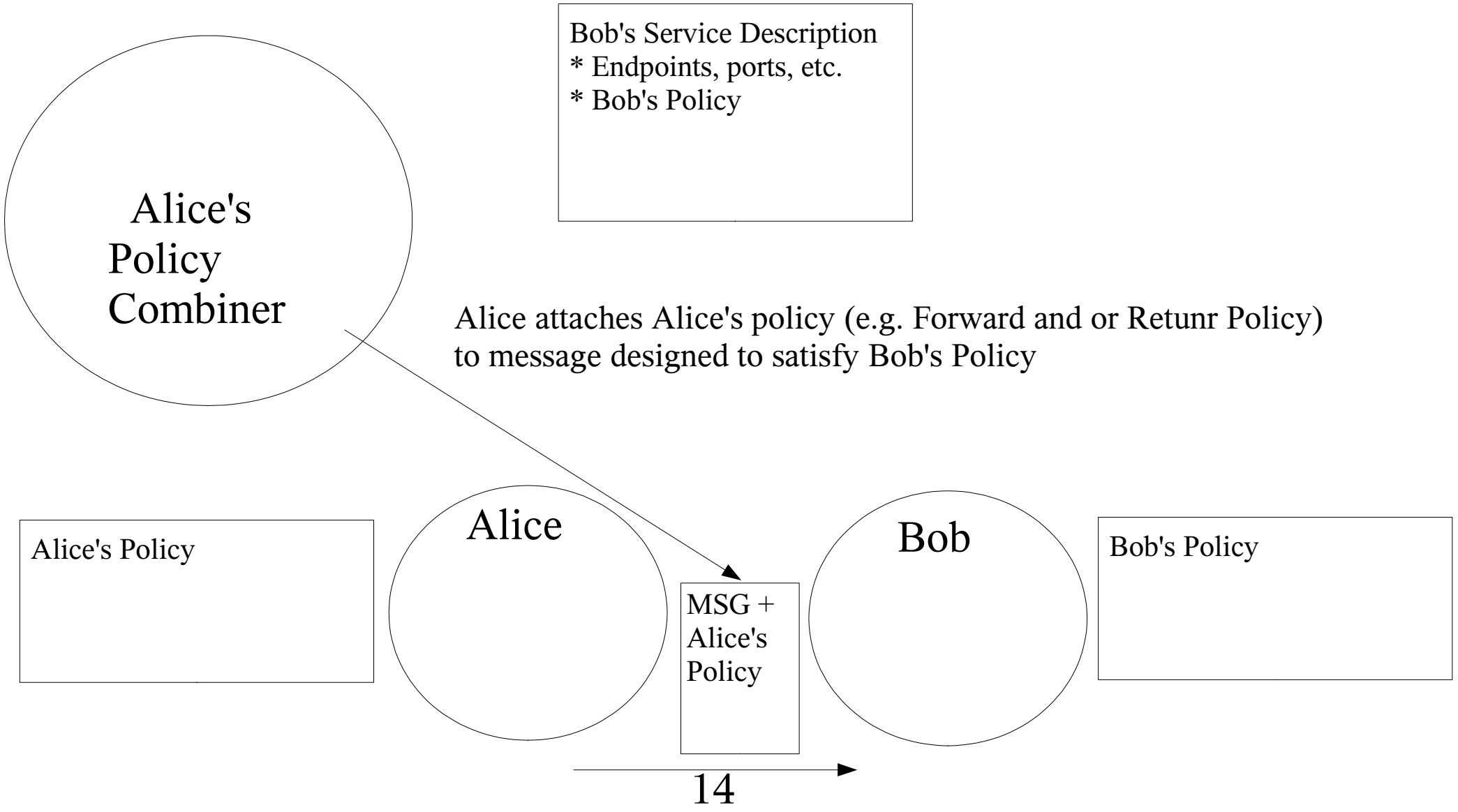
Alice Retrieves Bob's Policy



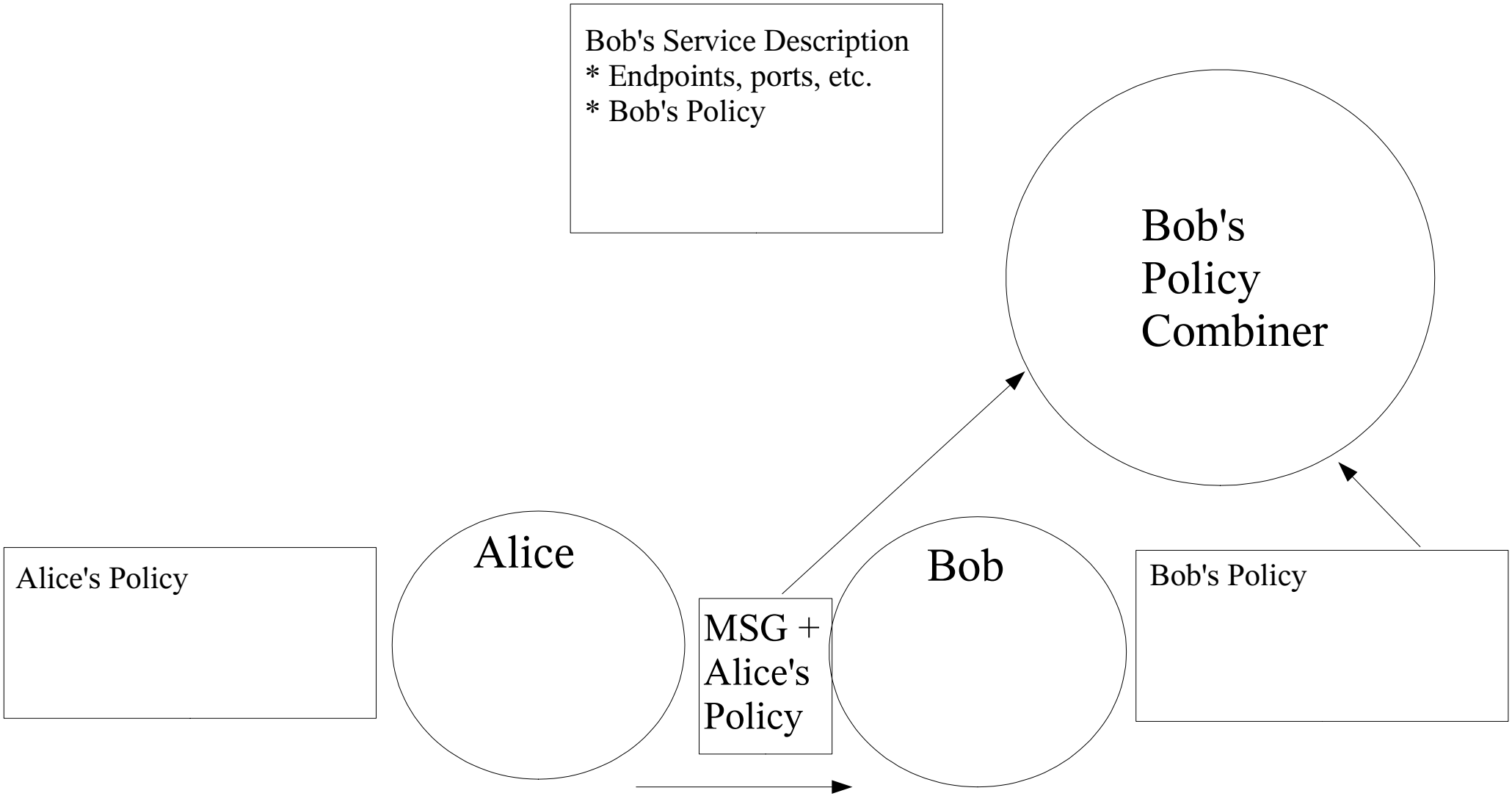
Alice Selects Solution



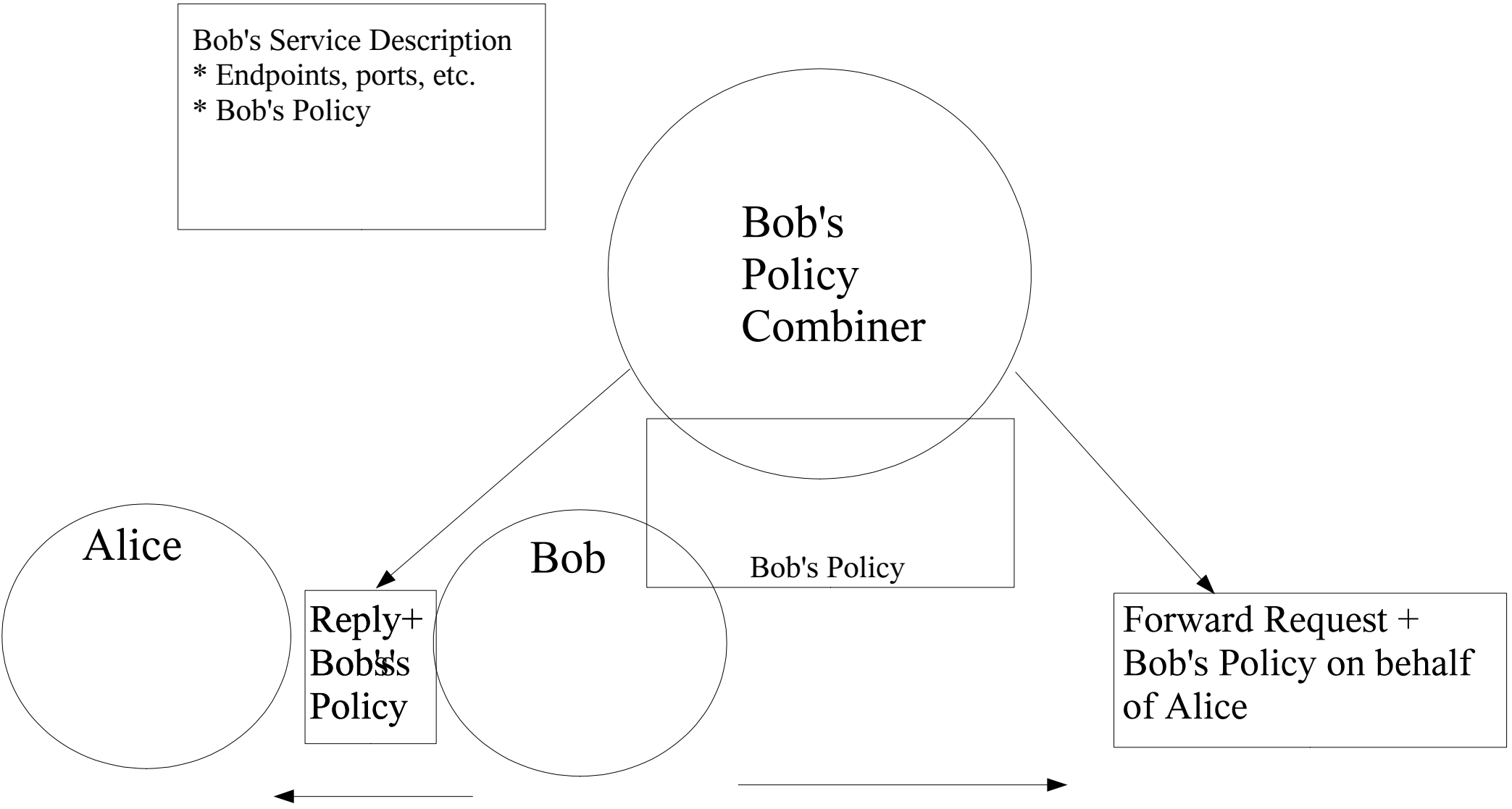
Alice Prepares and Sends Request



Bob Enforces and Satisfies Policy



Bob Responds to Alice or Invokes on Alice's Behalf



Problem Decomposition

Considerations

- The distribution or other communication of policy between interacting entities
  - How does Alice find Bob's requirements and capabilities?
  - How does Bob make his Policy available to Alice
  - How does Alice convey to Bob her requirements and capabilities?
  - How does Bob find Alice's Policy?
- The grouping of related policy statements or the composition of policy from smaller perhaps reusable statement groups.
- The reconciliation of policy negotiation with a layered processing model

Considerations(2)

- The need for a semantic model in which to configure, manage, and interpret (including in combination) groups of policy statements.
  - How does Alice determine if she is willing to talk to Bob and what Bob requires of her?
  - How does Bob Interpret and Use Alice's Policy
- The need to allow for (perhaps decentralized) evolution of the policy framework or statement model.
- Constraints imposed by the Invocation Model
  - One directory lookup and one network round trip?

Work Descriptions

Work(1)

- We need a language to express policy and to identify the resources that it applies to.
  - Need operators and a way to group alternatives such that semantics of: Any, (At Most One), Exactly One, One Or More, or ALL may be configured.
  - Grouping policy that pertains to a specific PEP/PDP
- Methods for service providers to make their policy available to service consumers and for service consumers to make their policies available to service providers
  - Discovery (directories, static stubs, etc.)
  - Attachment to service descriptions and requests (multiple forms of service descriptions and request protocols)

Work(2)

- We need methods for a service consumer and provider to negotiate how their interactions (e.g. The messages they exchange) are to be protected
  - Method(s) for negotiating a mutually-acceptable set of operations from representations of requirements and capabilities
  - Method(s) for service providers to apply the policies of their clients in the operations they perform on behalf of their clients
- We need methods to deal with invalid interpretation (and or invalidation) of policy
- We need to be able to ensure that policy may be secured such that neither the owner or the user of the policy is at risk

Chartering Discussion

Considerations

- What forums (eg. TCs), if any, do we perceive as the appropriate host for a particular piece of work?
- Definition of next steps:
  - How do we transfer problem description(s) to the appropriate forums, including potentially by deciding to charter a new forum?
  - Discussion of forum specific requirements, collection of advocates, sponsors, etc. to meet the requirements of the standard organization.