PLASMA
Straw Man Proposals

Jim Schaad

Soaring Hawk Consulting

Requirements

- Minimize the data stored on the server
- Validate server before talking to it
- Maximize backwards interoperability
- Place all policy enforcement on servers rather than on the client
- Set of recipients can be changed post message send
- Allow multiple types of authentication

S/MIME Recipient Info

New Custom Recipient

- Allows greatest flexibility
- Backwards capability issue with
    - Microsoft
    - Thunderbird
- Easiest client recognition

KEK Recipient Info

- Overloads existing structure
- Backwards compatible
- Currently ignored recipient info
- Detection relatively easy
- Create new OtherKeyAttribute

New KEK Attribute

- SignedData
  - Encapsulated Content is EnvelopedData
    - Encapsulated Content is new content EPS-LockBox
      - Names of recipients
      - Policy to apply for recipients
      - Key Encryption Keys
  - New signed attribute – URL(s) of Policy Server

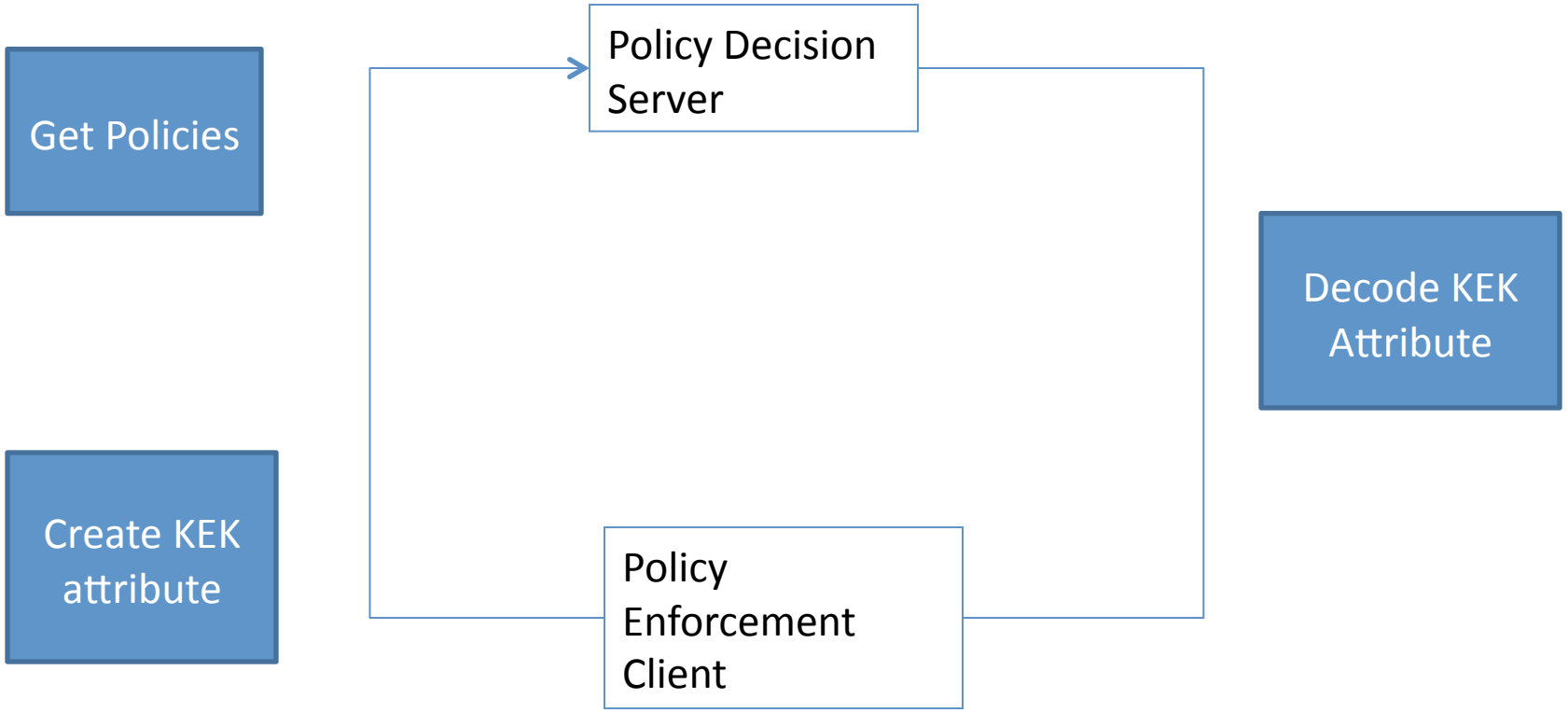
Complex Policy Structure

- Policy Identifier
  - URI or OID – to be decided
  - Need to have parameters for the policies?
- Policy Logic
  - And, or, exclude

Protocol

- Currently based on WS-Trust 1.3
  - OASIS standard
  - SOAP based
  - Requires client to manage SAML queries
- Potentially should base on ABFAB
  - Allows policy decision service to manage SAML queries

Protocol Steps Needed



Questions