W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement

Privacy Policy Negotiation Framework for Attribute Exchange

October 18, 2006

Makoto Hatakeyama, Hidehito Gomi
NEC Corporation

Outline

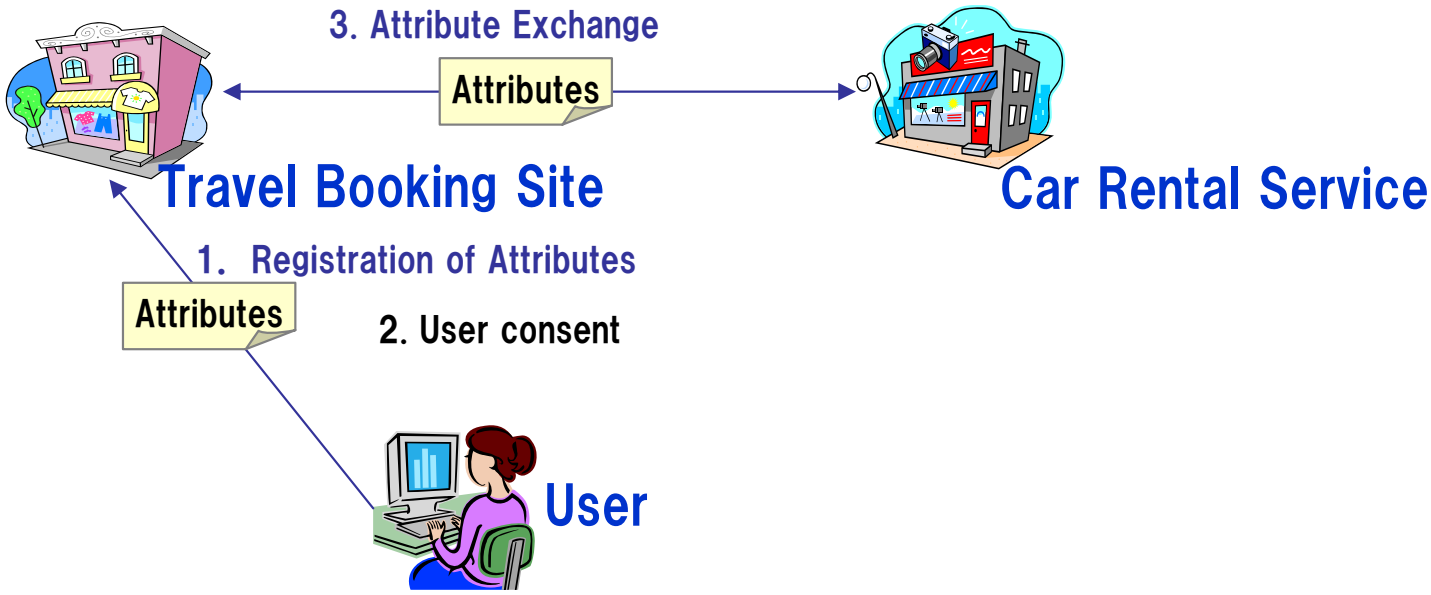
- Background
- Privacy Policy Negotiation Framework
  - Privacy Policy Management
  - Privacy Policy Negotiation Protocol
- Conclusion

Outline

- **Background**
- Privacy Policy Negotiation Framework
  - Privacy Policy Management
  - Privacy Policy Negotiation Protocol
- Conclusion

Overview of Attribute Exchange

- Sharing of user's attributes based on user's consent between service providers
  - Personalized service for a user
  - Reduce operation cost for registration of user's attributes



Requirement for Attribute Exchange

- Select only necessary attributes to be exchanged
  - Prevent privacy leakage
- Confirm a mutual agreement about privacy policy
  - Determine kinds of exchanged attributes
  - Confirm liabilities of how to use and enforce privacy protection

Previous Work

- Privacy policy description
  - P3P, APPEL
  - Between a user and a provider
- Regulating exchange of privacy information
  - Automated trust negotiation
  - Access control for disclosure of privacy information

Our Contribution

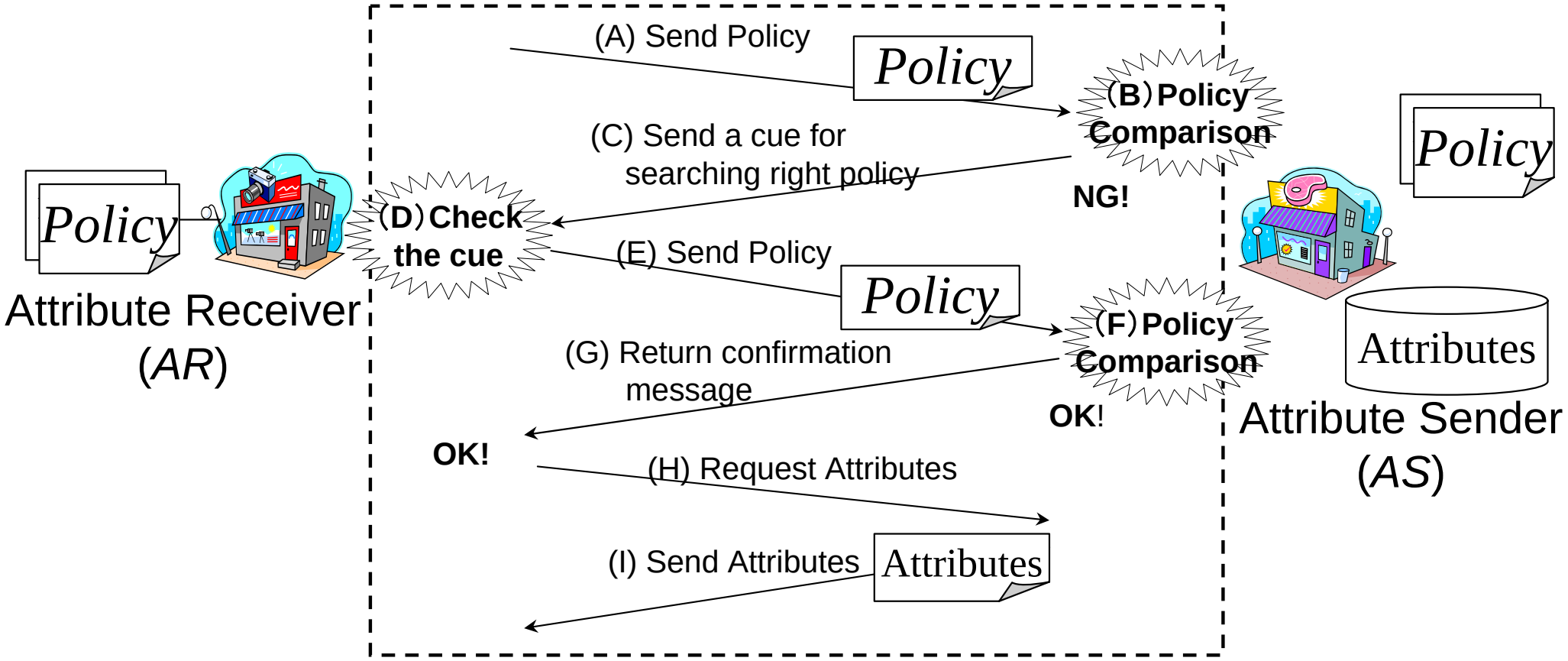
- Determine minimum attributes based on privacy policy
- Determine liabilities of attributes management
  - Decision of kinds of attributes to share
  - Confirmation of way to enforce privacy protection

Outline

- Background
- **Privacy Policy Negotiation Framework**
  - Privacy Policy Management
  - Privacy Policy Negotiation Protocol
- Conclusion

Overview of Privacy Policy Negotiation Framework

- Privacy policy
  - Kinds of attributes to be exchanged
  - Ways to enforce privacy protection
- Privacy policies preserved by providers
- Negotiation protocol for comparison of privacy policies



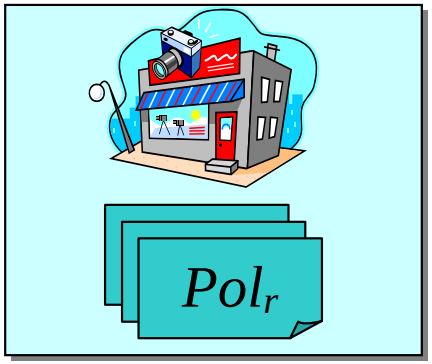
Outline

- Background
- Privacy Policy Negotiation Framework
  - **Privacy Policy Management**
    - Privacy Policy Negotiation Protocol
- Conclusion

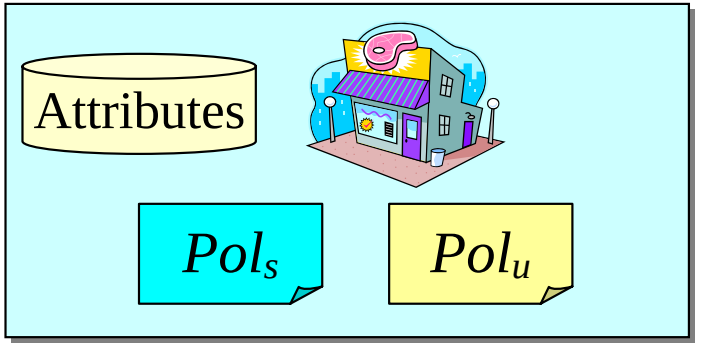
Privacy Policy Categorization

- User policy (Pol_u)
  - Rule for providers to manage attributes for privacy protection
- Sender policy (Pol_s)
  - Rule for Attribute Sender (AS) to forward attributes to Attribute Receiver (AR)
  - Described for AS not to forward many attributes
- Receiver policy (Pol_r)
  - Conditions for AR to use and preserve attributes
  - Described for AR to request only the minimum condition and not to get many attributes

Attribute Receiver (AR)



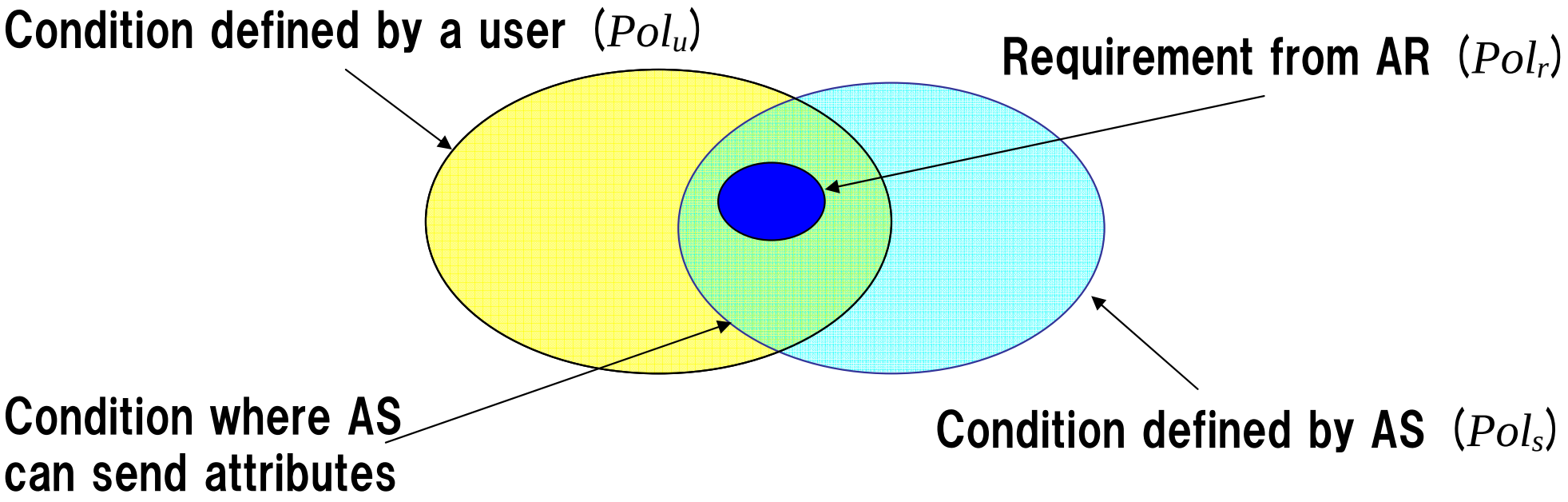
Attribute Sender (AS)



Privacy Policy Comparison

- **Condition for AS to send attributes to AR**

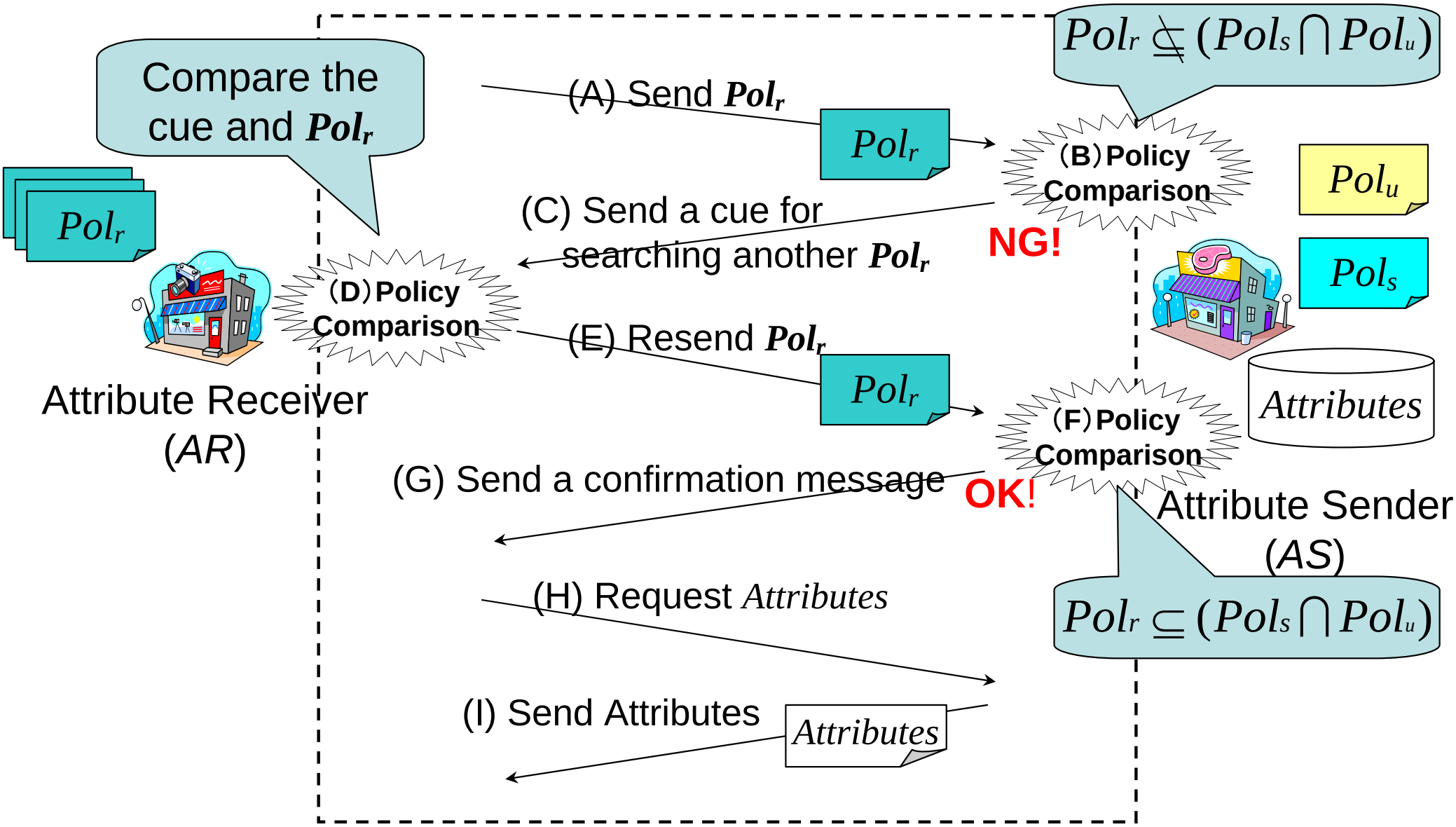
$$Pol_r \subseteq (Pol_s \bigcap Pol_u)$$



Outline

- Background
- Privacy Policy Negotiation Framework
  - Privacy Policy Management
  - **Privacy Policy Negotiation Protocol**
- Conclusion

Sequence of Privacy Policy Negotiation Protocol



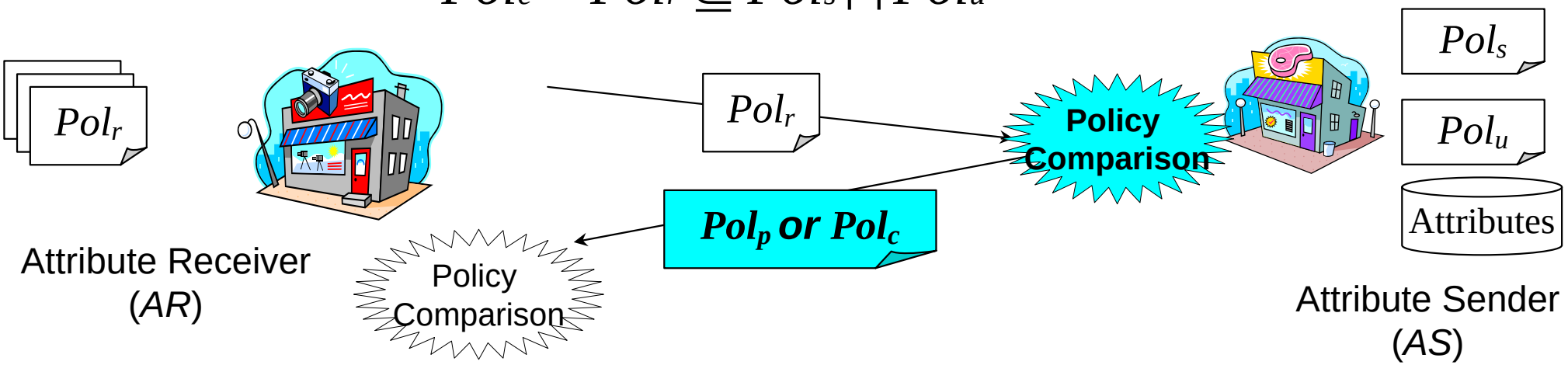
Operation of AS

- **Policy comparison**
  - **Comparison Failed** $(Pol_r \not\subseteq (Pol_s \bigcap Pol_u))$
    - **Disclose subset of Proposal Policy** Pol_p **as a cue of searching another** Pol_r

$$Pol_p = Pol_s \bigcap Pol_u$$

  - **Comparison succeeded** $(Pol_r \subseteq (Pol_s \bigcap Pol_u))$
    - **Disclose Confirmation Policy** $\boldsymbol{Pol_c}$

$$Pol_c = Pol_r \subseteq Pol_s \bigcap Pol_u$$

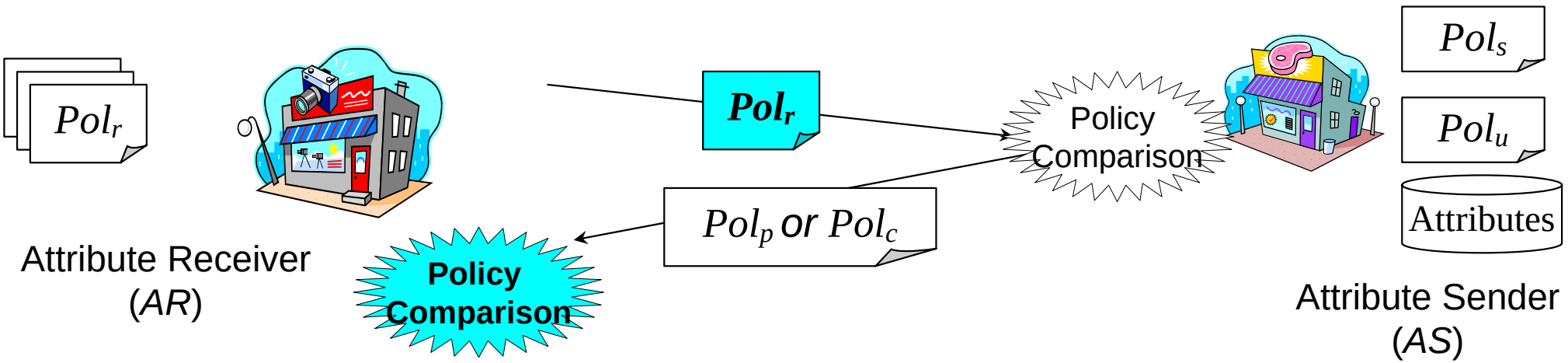


Operation of AR

- **AR sends Pol_r to AS**
  - **Decide Pol_r which satisfies AR's requirement**
- **Subset of proposal policy Pol_p received**
  - **Search new Pol_r satisfying the following condition:**

$$Pol_r \subseteq Subset\_of\_Pol_p$$

  - **Send the Pol_r**
- **Confirmation policy Pol_c received**
  - **Request user's attributes according to Pol_c**



Future Work

- Life cycle management of privacy policies
  - Expansion of privacy policy negotiation framework
    - Policy Registration
    - Policy Update
    - Policy Revocation

Outline

- Background
- Privacy Policy Negotiation Framework
  - Privacy Policy Management
  - Privacy Policy Negotiation Protocol
- **Conclusion**

Conclusion

- Privacy policy negotiation framework
  - Categorize Privacy policy into three types
  - Specify policy negotiation protocol
  - Determine necessary exchanged attributes
  - Confirm liabilities of how to utilize and enforce privacy protection

Empowered by Innovation