# Requirements for Policies

Fuming Shih

Joe Pato

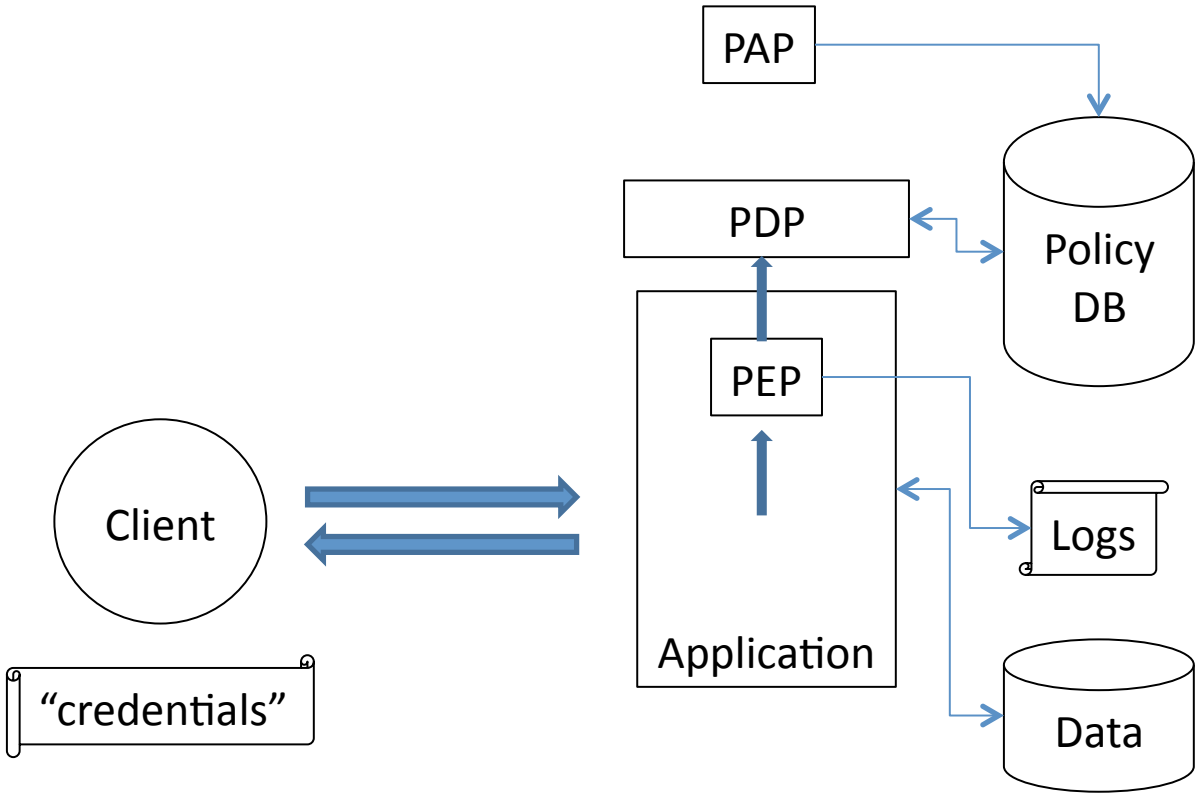
# PrimeLife

- Follow-on to EC PRIME (Privacy and Identity Management for Europe) project
- Aims to design a next generation policy language and system

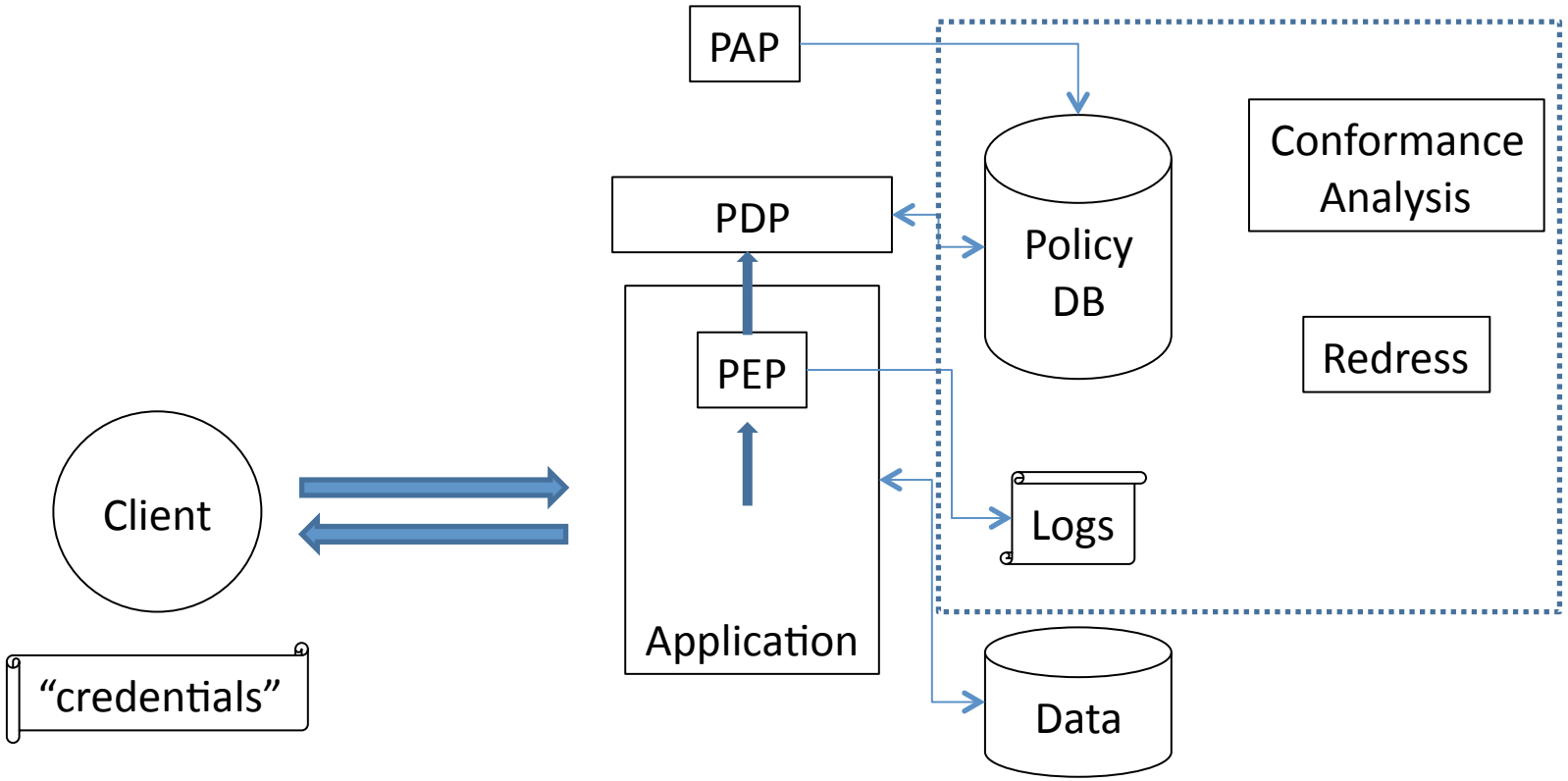
# Definitions

- Data Handling policies
  - How data can be used (purposes, obligations, preferences)
- Access Control policies
  - Who can do what in which circumstances
- Trust policies
  - Evidence needed to evaluate DH and AC controls

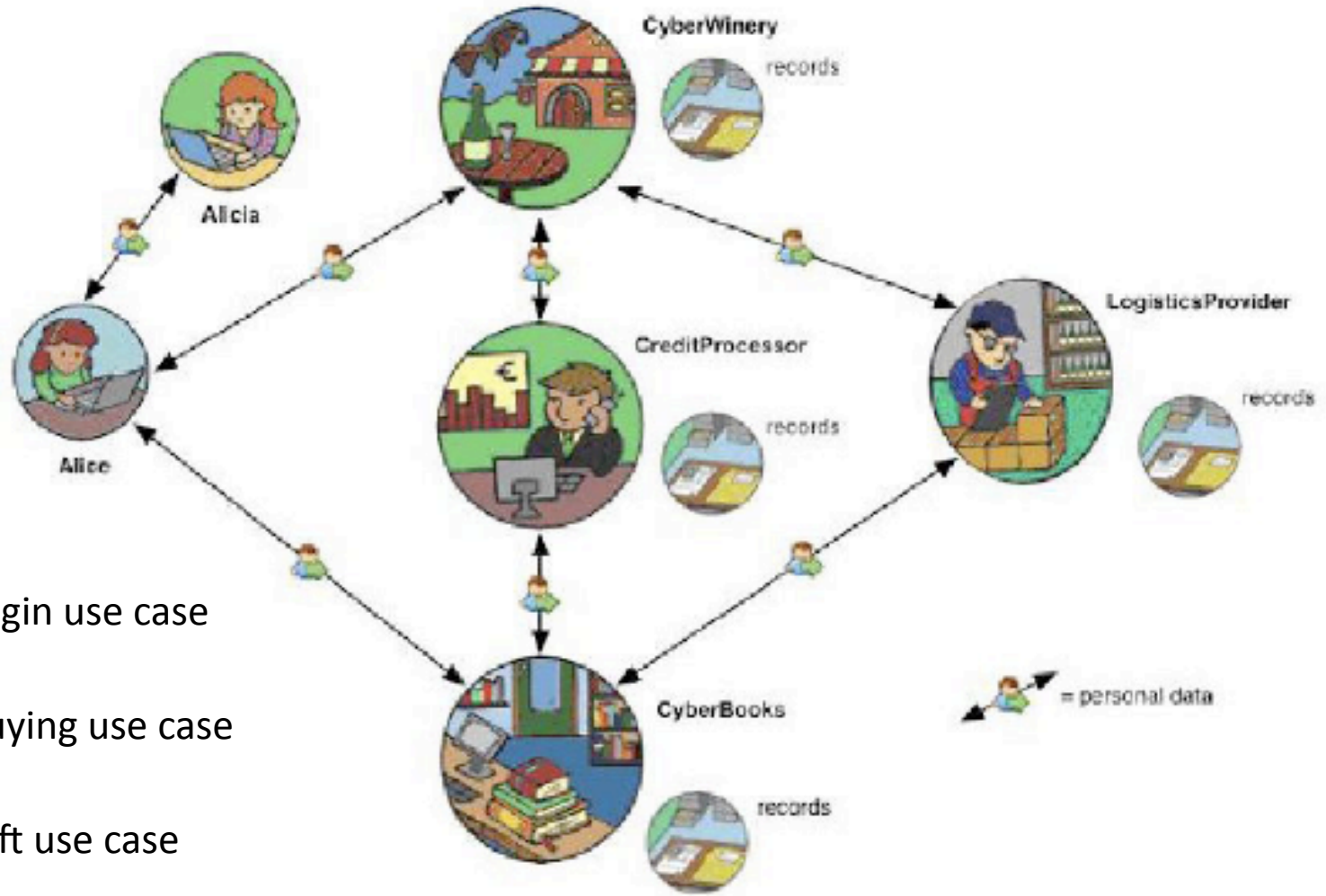
# Conventional Access Control Model



# Accountable Access Control Model



# SCENARIOS




1. Login use case

2. Buying use case

3. Gift use case

# REQUIREMENTS

# 1.1 General Principles – Data Handling

- Measurability
- Unified model
- Semantic compatibility (w/P3P)
- Stickable (“sticky”) policies
- Revocability
- Transparency
- High-level

# 1.2 General Principles – Access Control

- Data minimization
- Anonymous or pseudonymous access control
- Link to data handling policy

# 2. Language model and expressivity

- Meta policies and policy generation

# 2.1 Language model – Data Handling

- Business logic to describe data usage
- New usage should trigger consent (*)
- Legal policies need differentiated layering
  - Short, condensed, full, iconographic
- Technical representation of legal policies
- Policy templates
- Policy matching (domains, variables, _fill in blank values_)
- Support variables
- Support nested policies

# 2.1 Language model – Data Handling

- Express user preferences
- Describe server policies
- Originator's policy
- Logging/Monitoring/Auditing policies
  - Inform user of data collected
  - Express scope of retention
  - Express how data collected
- Data model primitives
  - Date, time, location

# 2.1 Language model – Data Handling

- Security levels
- DHP ontology
- Enforcing DHPs
- Auditability – obligations toward where to log access
- Breaking the glass (exception handling)

# 2.1 Language model – Data Handling

- Capture user intent
- Purpose of data processing
- Express obligations
- Constraint restrictions
- Notification / feedback channels

# 2.2 Language model – Access Control

- Declarative model to represent preferences
- Inheritance; propagation (of credentials – tokens)
- Role models – family, friends, wider access control
- Information from third-party sources
- Credentials or similar objects
- Attribute based access control to data on fora

# 2.2 Language model – Access Control

- Expiration date
- Time or event of “begin of validity”
- Priority of policies or combination rule for policies
- User choice for monitoring
- Choose strength of protection
- Change policy
- Property-based – challenge response, secret handshake

# 2.2 Language model – Access Control

- Technical representation and description in user-centric terms
- Support for complex claims
- Support for complex rules
- Third-party restrictions
- Use of ontologies

# 2.3 Language Model – Trust Policies

- Link to Data Handling policies
- Trust establishment
- Statement and certification
- Make statement content-pluggable
- Security breach

# 2.3 Language Model – Trust Policies

- Link to Access Control policies
- End user trust
- Build trust through third party
- Trust reasoning
- Trust ontologies
- Transparency, reciprocity
- Specification of liabilities

# 3.1 Policy Composition – Data Handling

- Prior agreement and contract
- Aggregation of policies
- Combination of policies
- Cascading policies
- Prioritization of rules
- Generalization of policies
- Multi-rounds policy definition
- Policy negotiation

# 3.1 Policy Composition – Access Control

- Delegation of rights
- Revocation of rights
- Composition of access control policies
- Prior agreement and contracts
- Privacy-aware audit mechanism
- Support for data and PII
- Link between AC and DH

# 3.1 Policy Composition – Trust

- Dynamic trust
- Scope
- Proof of enforcement

# 4 Use of anonymous credentials

- Technology-independent certification of data by trusted third parties
- Trust in certified data
- Predicates over attributes, extensible with ontologies
- Embedded or referenced ontologies
- Expression of proved statement
- Derived PII
- Revealing of data
- Alternative data recipient + associated access conditions
- Notion of atomic credentials
- Macros
- Limited spending
- Alternative DHP
- Choice based on access control policy