Complex Cyber Infrastructure

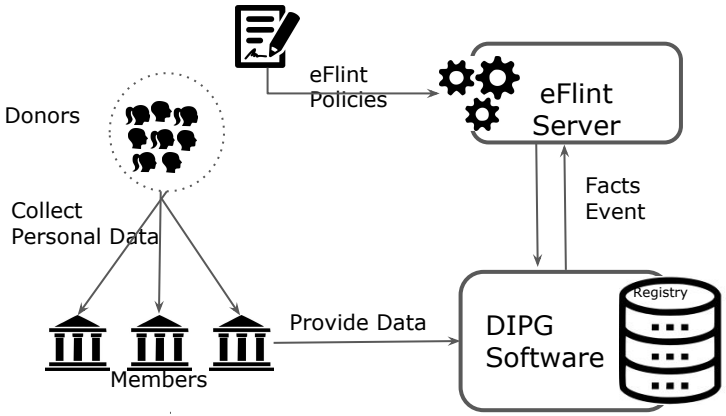
RQ5: Automating regulatory constraints and data governance

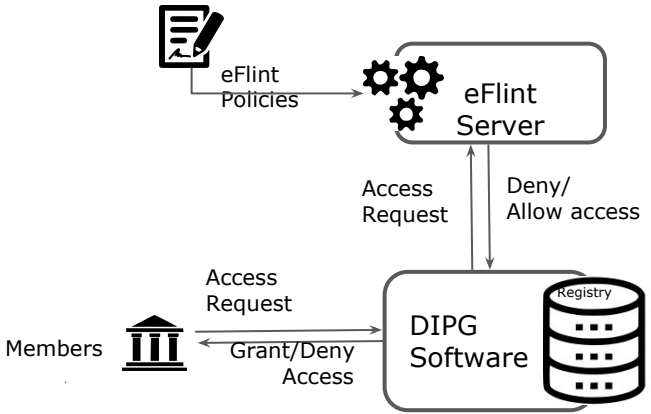
EPI Quarterly Meeting

Milen G. Kebede . 17/01/2022

Dynamic generation of access control policies from social policies

- A prototype for a Policy Decision point(PDP) or a Policy Administration point (PAP) for the AMdEX project
  - eFLINT reasoner as PDP
    - As both PAP and PDP
  - eFLINT as PAP
    - Extensions for the XACML reference model
  - Decentralized approach

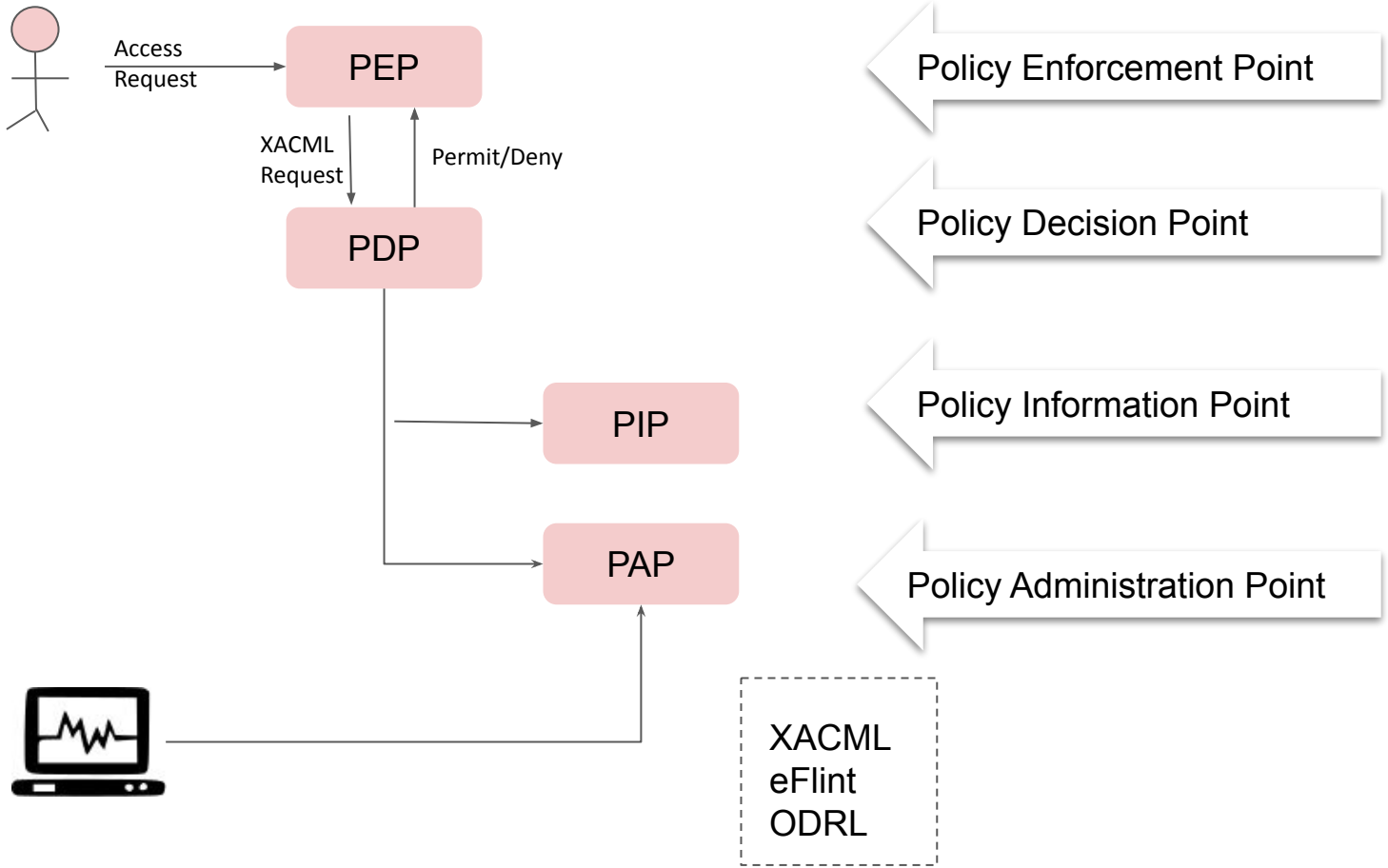




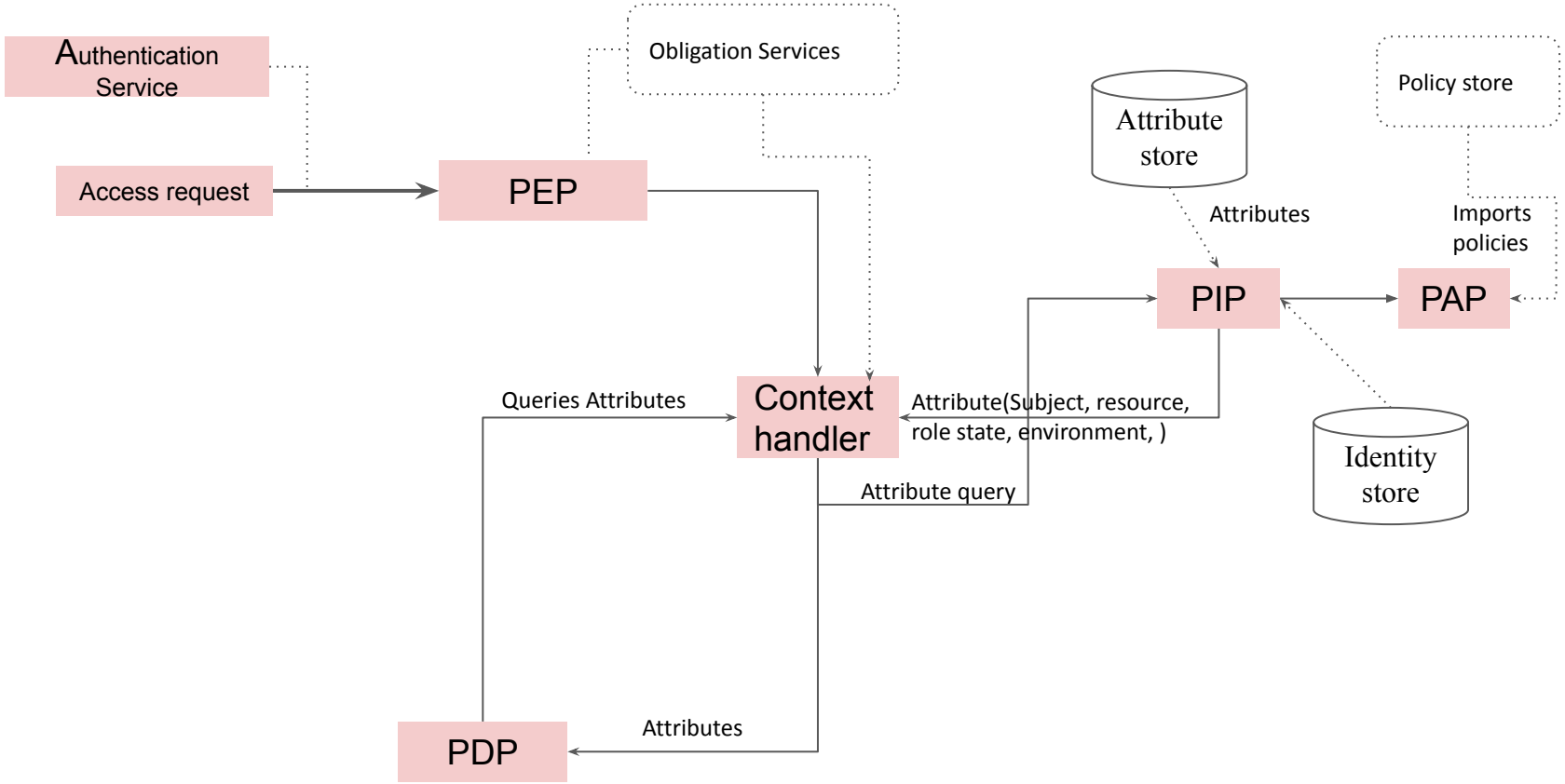
The XACML ABAC model

- XACML policy language
  - Specifying access control requirements using rules, policies and policy sets , expressed in terms of subject, resource , action and environmental attributes and set of algorithms for combining policies and rules
- XACML request/response protocol
  - For querying a decision engine that evaluates subject access requests against policies and returns access decision in response
- XACML reference architecture
  - For deploying software modules to policies and attributes and computing and enforcing access control decisions based on policies and attributes

XACML Request/Response protocol



XACML Reference Architecture



Obligation in XACML

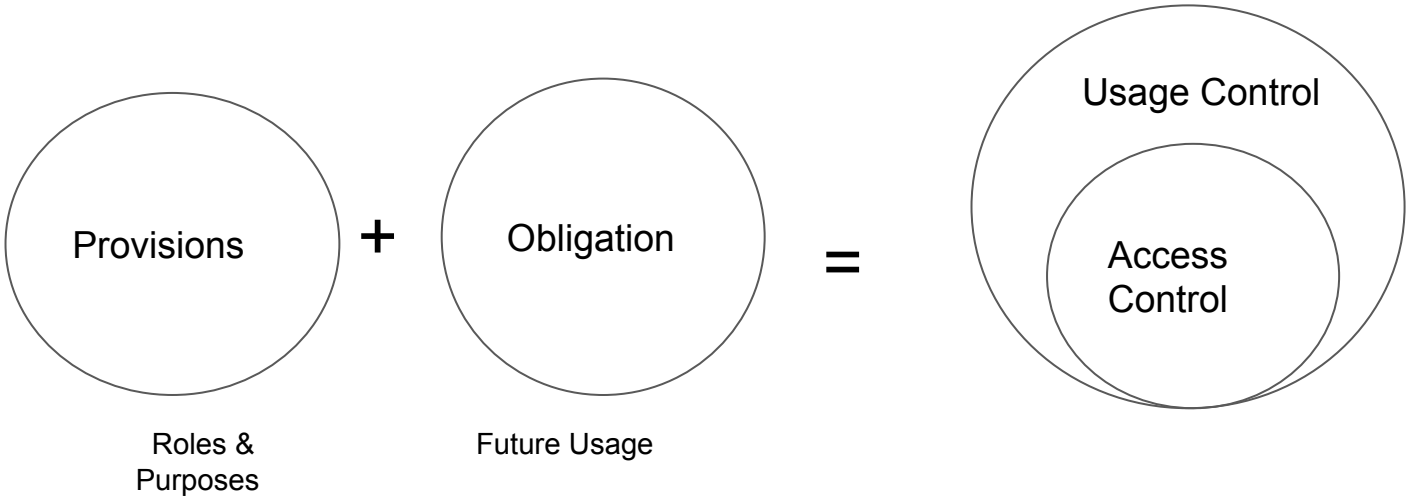
Obligation services - obligation optionally specified in a rule, policy and policy set is a directive from the PDP to the PEP on what must be carried out before or after an access request is approved

Obligations must be fulfilled in conjunction with the policy enforcement after the access decision has been made(which is the result of a rule that is to permit or deny)

When a PDP evaluates a rule that is containing obligation expressions, it evaluate the obligation expressions into obligations and return certain of those obligation to the PEP in the response context

Obligation extensions to XACML

- Enforce before the user action is performed
  - E.g get the consent of owner
- Enforce after the user action is performed
  - E.g email data owner that his data is accessed
- Simultaneously with the performance of the user's action
  - E.g write to the log the activities the user is performing



Authorization model decisions

Pre-authorization models
- The authorization decision is made before the action is allowed

Ongoing authorization models
- Authorization decisions are made continuously while the action is taking place

Pre-conditions model
- Certain environment conditions have to be fulfilled before the resource usage

Ongoing conditions model

- Environmental conditions that needs to be satisfied while the resources usage is taking place

Ongoing work & other activities

- eFlint ontology with Triply
- Flint ontology with TNO
- The design of eFLINT 3.0
- Collaboration with Amdex on the design and development of a prototype PDP & PEP
- Data sharing Winter school | Next mobility - smart data sharing to move goods & people