

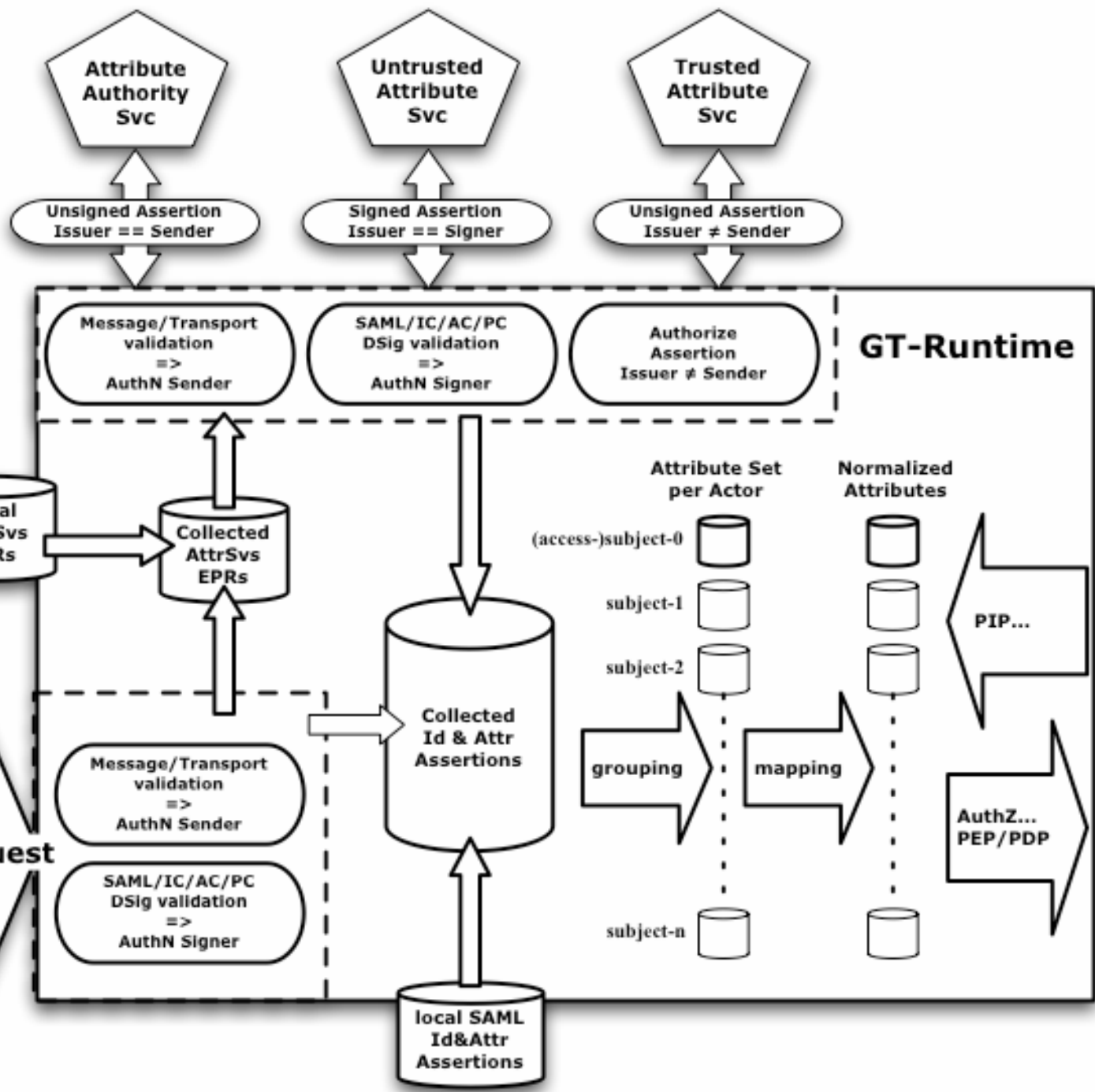
# Overview of Attribute & Authorization Processing in GT4 (With GridShib for GT)

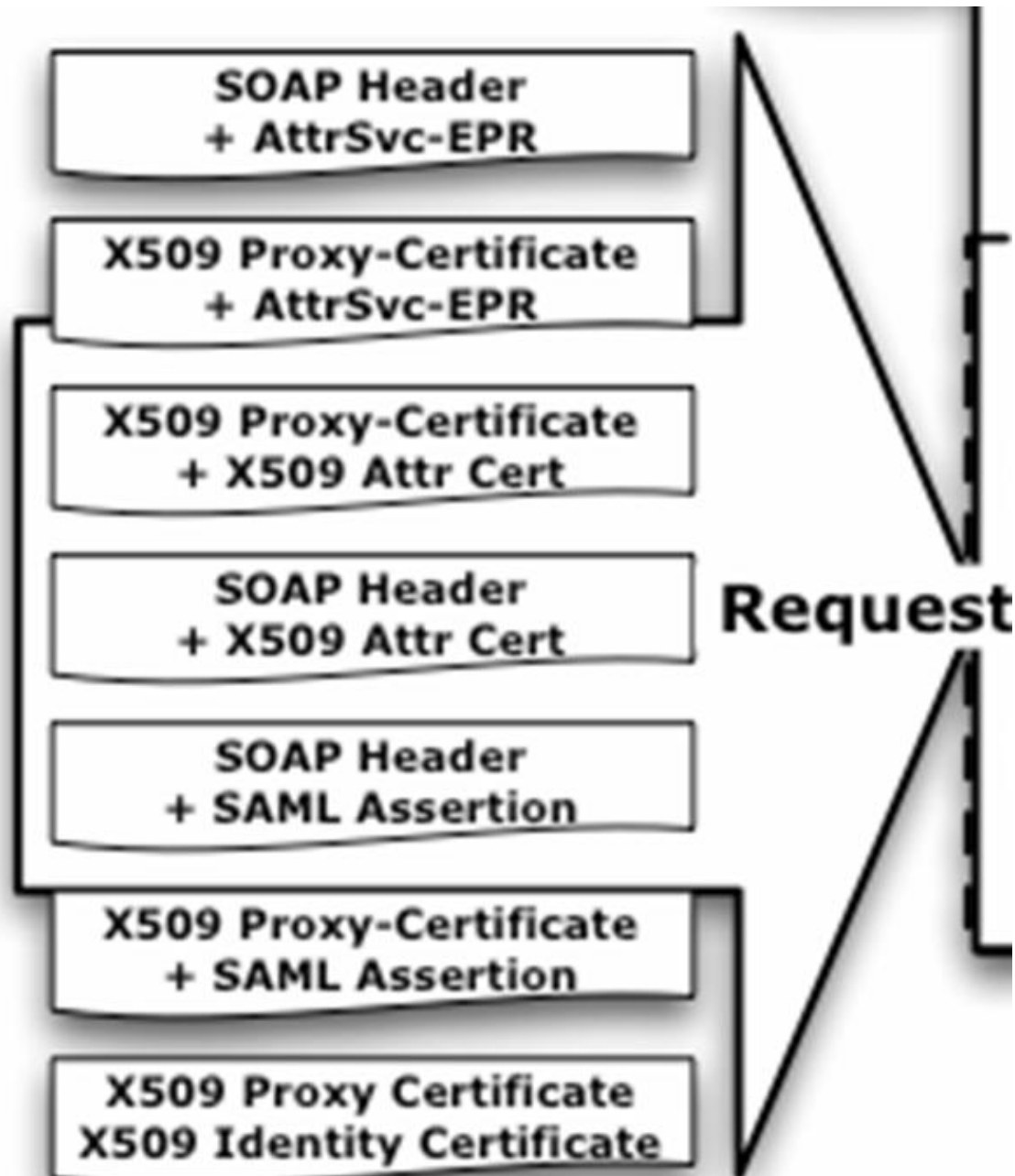
Tom Barton  
University of Chicago

Thanks to Tim Freeman, Rachana  
Ananthakrishnan, and Frank Siebenlist

# GT4 Attribute Collection

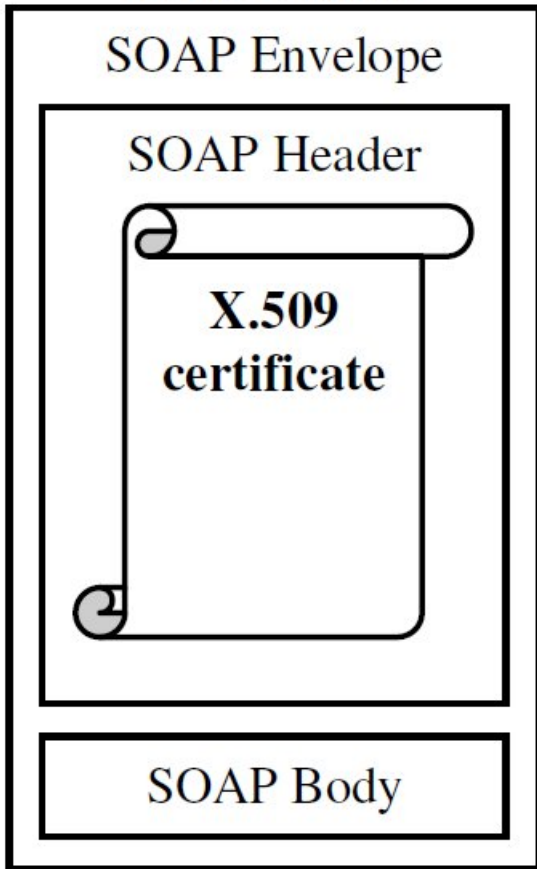
Attribute  
Services



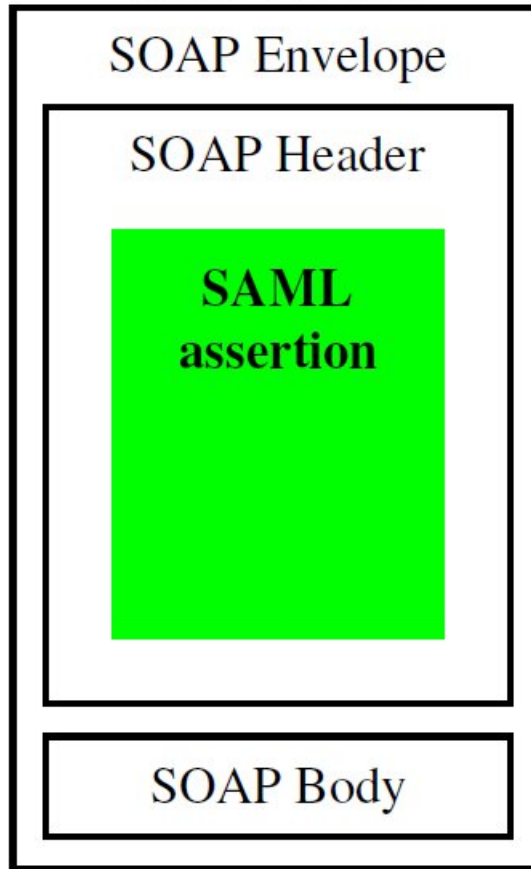


# WS Security Tokens

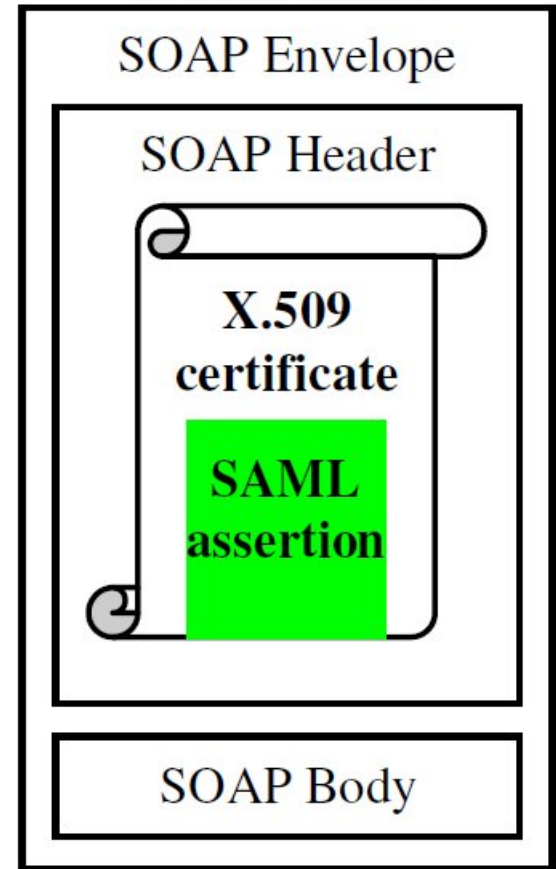
## X.509 Token

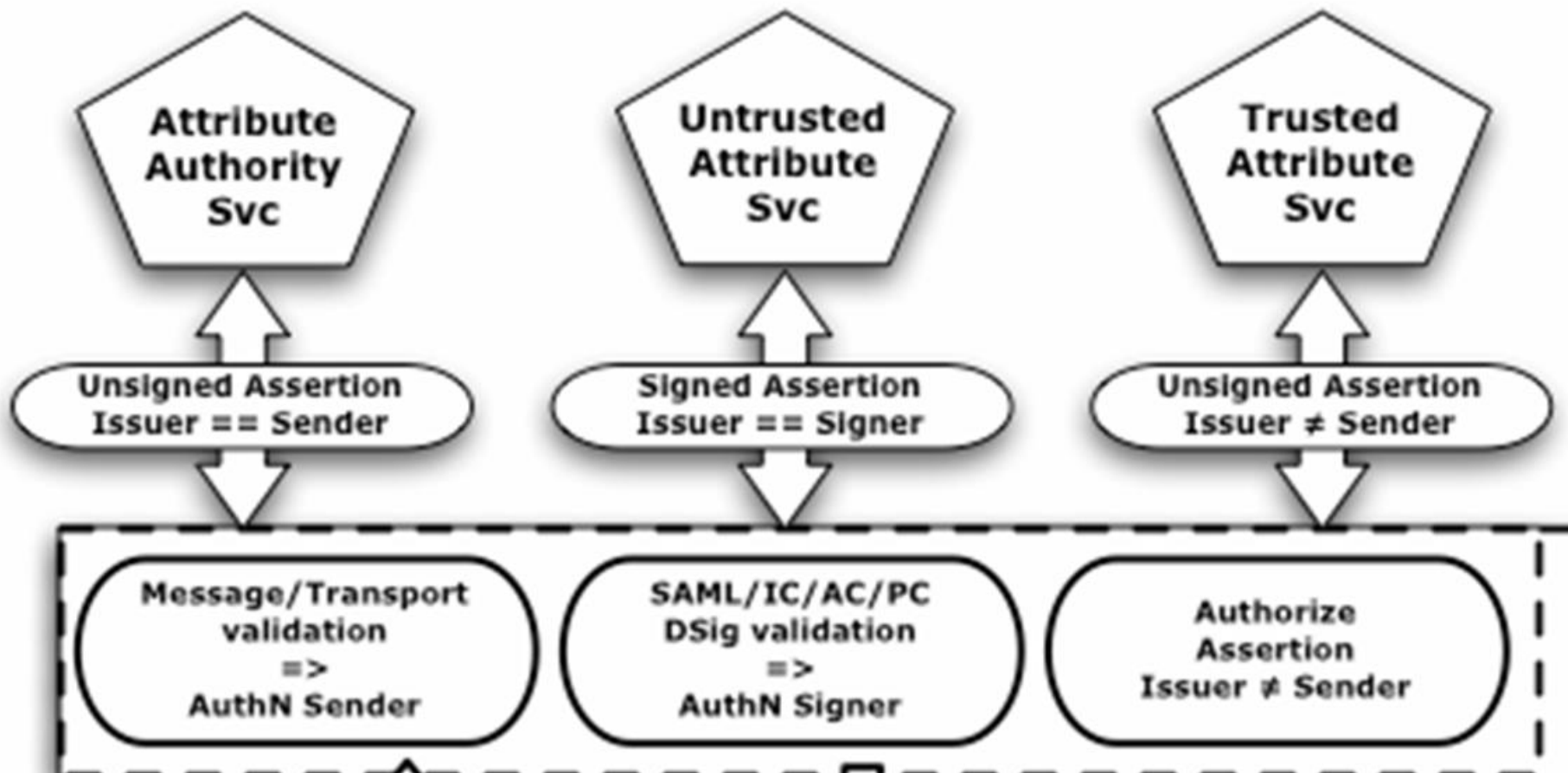


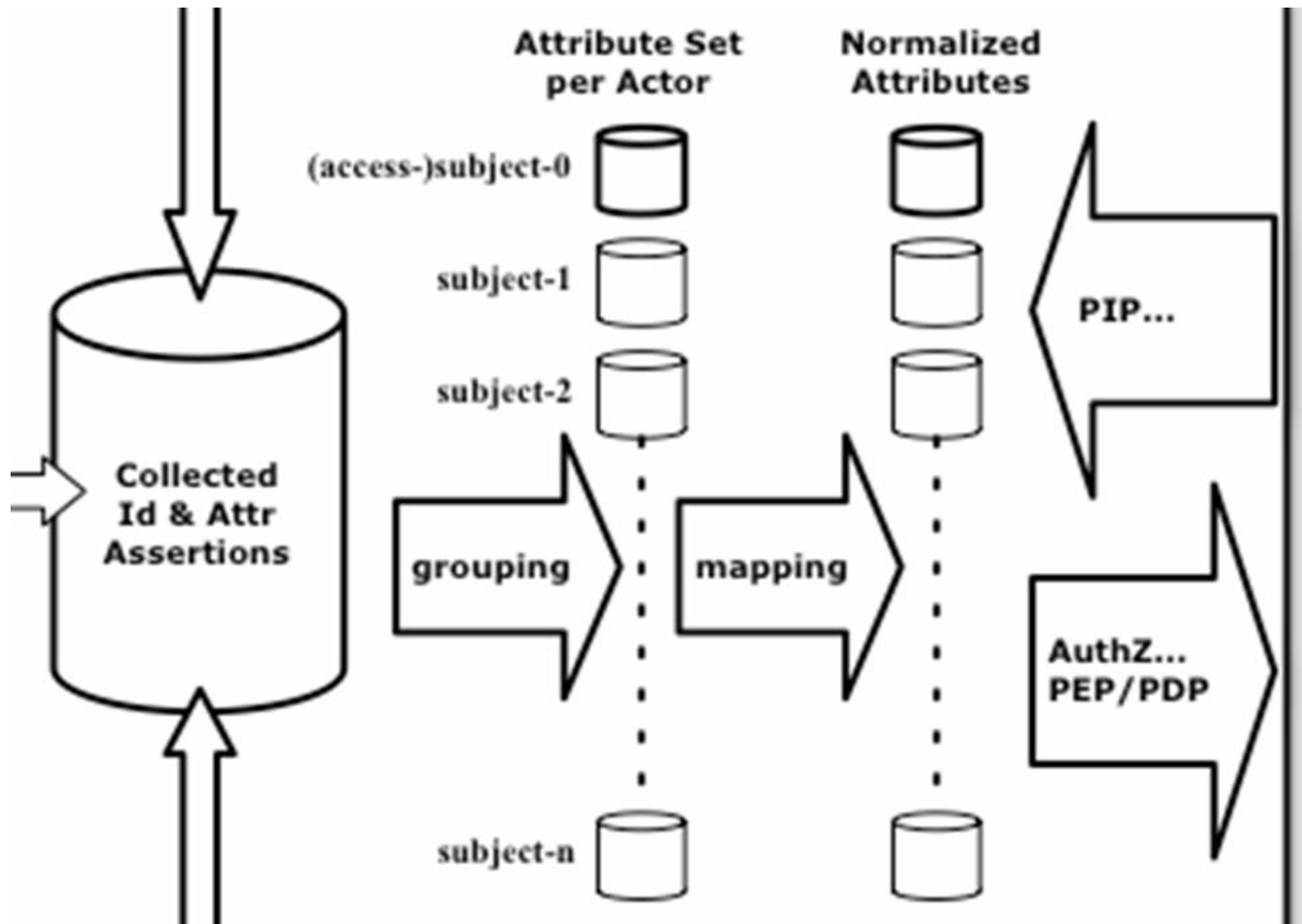
## SAML Token



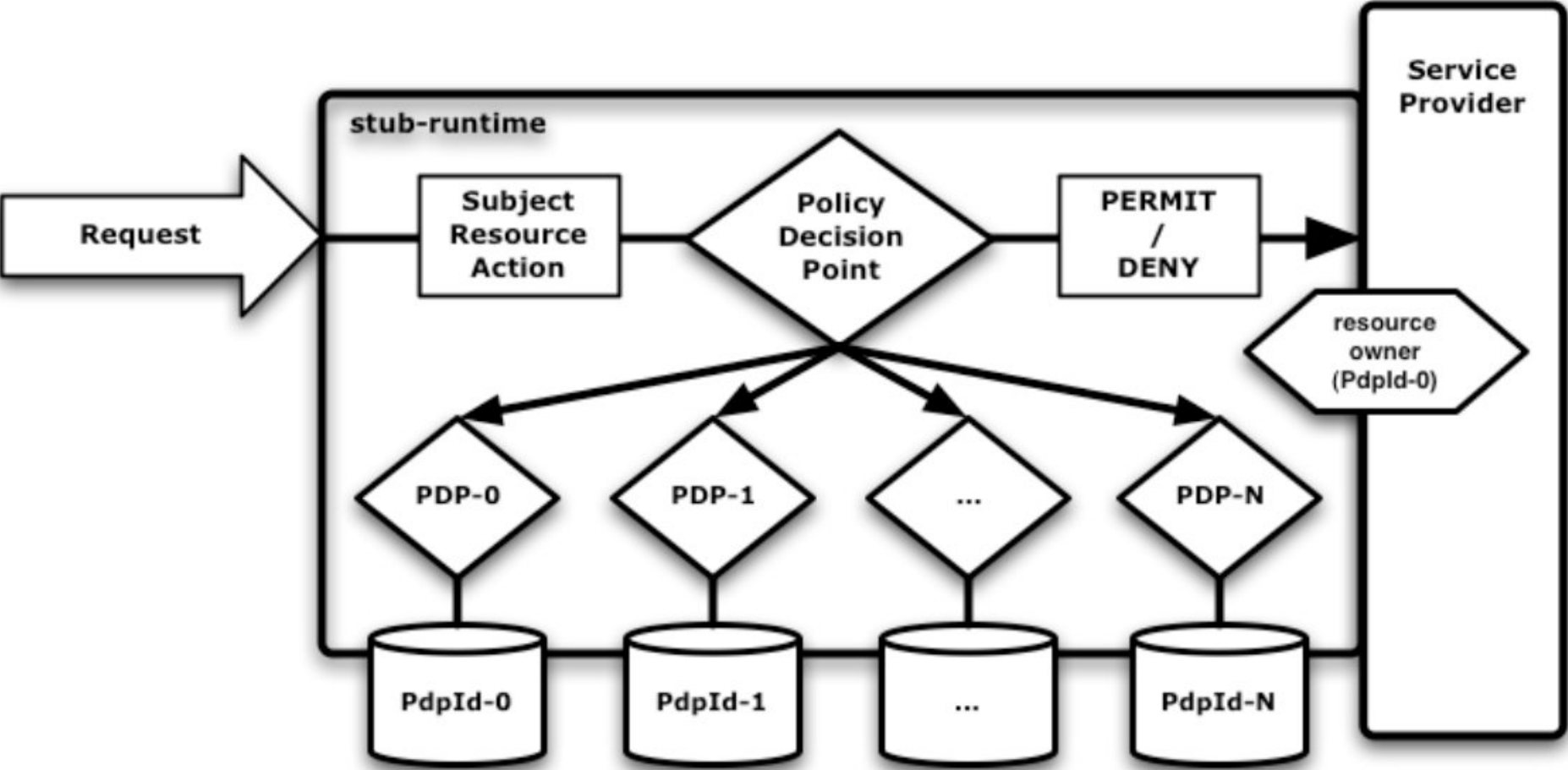
## X.509-bound SAML Token







# GT4 Authorization Framework



# Resultant Decision

- PDP decisions: canAccess, canAdmin
  - Permit, Deny, Not Applicable, error
- PDP combining algorithms
  - First Deny denies
  - First Permit permits
  - Permit over-ride with delegation
- PIP-PDP chain configurable per-container, per-service, and per-resource

# Attribute Notables

- Query SAML AAs
- SAML attributes from cert chain
- VOMS attributes
- Attribute Acceptance Policy
- Map SAML, VOMS attributes to accounts
  - Enables attribute-based GRAM
- Map attributes to dynamic accounts
  - Enables attribute-based GridFTP

# Some Things I Don't Know

- Policy administration interfaces
- Framework for accounting/reporting uses of attributes
- All of the add-ons to administer access rights
  - VOMS, CAS, PERMIS, GridGrouper, ... ?