

Policy-based Authentication and Authorization based on the Layered Privacy Language

LPL

- Machine-readable representation of Legal Privacy Policies
- Purpose-based Access Control
- Representation of Privacy-Preserving Methods
- Concept: Sticky Policies with Raw Data



→ POLICY-BASED AUTHENTICATION AND AUTHORIZATION

- 1 Requesting Entity Uni Passau authenticates
- 2 Purpose research is valid
- 3 Requesting Entity Uni Passau authorized against Data Recipients
- 4 Data age and postal-code authorize
- 5 Data salary is invalid for 'Alice' ↴

LPL POLICY LPL1

- Purpose: research
- Data: age, postal-code
- Data Recipient: Uni Passau, TH Deggendorf

POLICY / DATA SOURCE / AGE / POSTAL-CODE / SALARY

• lpl1	• Alice	• 25	• 94032	• 36.000
• lpl2	• Bob	• 23	• 94469	• 35.500
• lpl3	• Charlie	• 24	• 18055	• 35.700

REQUEST

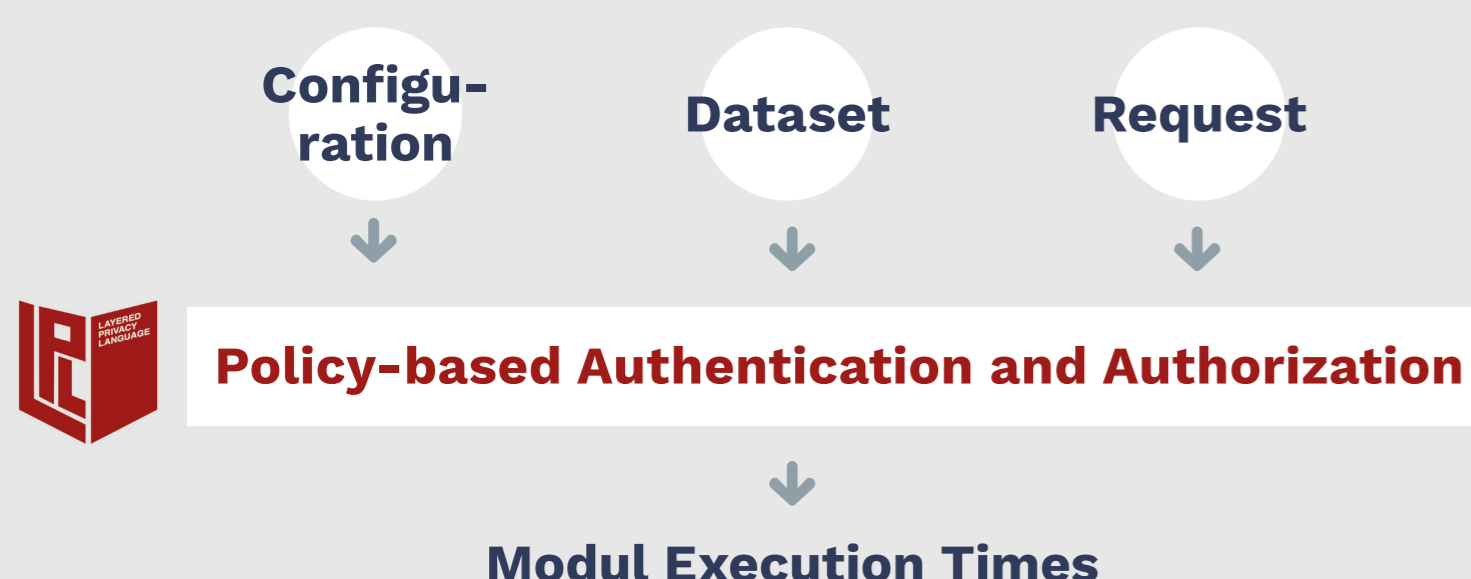
- Entity: Uni Passau
- Purpose: research
- Data: age, postal-code, salary
- Data Source: Alice, Bob

POLICY-BASED AUTHENTICATION AND AUTHORIZATION

AGE / POSTAL-CODE / SALARY

• 25	• 94032	• -
• 23	• 94469	• 35.500

EXPERIMENT SETUP



RESULT

Each of the benchmark parameters has maximal a linear effect on the execution time of the modules.

- Put all requested and inherited Purposes to the key-set ... < 1 ms
- Put the Data Sources to the relevant Purposes 11 ms
- Getting all not relevant Purposes of the key-set < 1 ms
- Remove all not relevant Purposes from the result map < 1 ms
- Total execution time (cleaned) ~ 11 ms