# Delegated attribute-based access control (DABAC) for contextual Linked Data

R. Stojanov, S. Gramatikov,
M. Jovanovik, D. Trajanov

# Introduction

- Security is cross-cutting concern that affects every part of the system
  - It is constant trade-off between a **secured system** and **convenient security management**
- Delegation of the security management makes this process more convenient
  - Multiple individuals can contribute
- In this work we have defined a **policy language** that extends the SPARQL query language with constructs that describe whether a data portion is allowed or denied for a certain Intent

# Motivation

- Our goal is
  - to provide **context-aware**, **attribute-based** access control of the Linked Data, by using complex and diverse policies
    - Solved in [1] by using extension of the SPARQL query language for the Semantic Wb
  - simplifying the task of policy definition
    - Design-time validation [1]
    - Delegation of access rights
      - Each user defines new policies that are combined with all the inherited policies up to that level

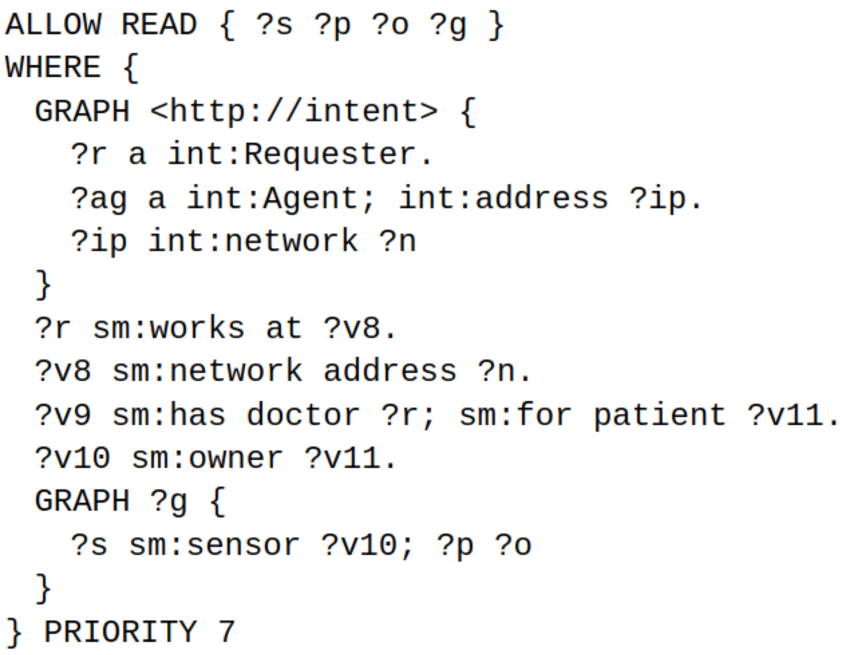
[1] Stojanov, Riste, et al. "Linked Data Authorization Platform." IEEE Access 6 (2018): 1189-1213.

# Research Question

- The policy management process requires
  - a flexibility to protect an **arbitrary part** of the data, for every **particular user** or **group of users** in a **specific context** [1]
  - design-time security rules validation [1]
  - convenient delegation of access rights
- The main challenge in this work is to provide a **convenient delegation** of access rights for **attribute based policies**

[1] Stojanov, Riste, et al. "Linked Data Authorization Platform." IEEE Access 6 (2018): 1189-1213.

# Linked Data Authorization (LDA) Platform [1]



```
ALLOW READ { ?s ?p ?o ?g }
WHERE {
  GRAPH <http://intent> {
    ?r a int:Requester.
    ?ag a int:Agent; int:address ?ip.
    ?ip int:network ?n
  }
  ?r sm:works at ?v8.
  ?v8 sm:network address ?n.
  ?v9 sm:has doctor ?r; sm:for patient ?v11.
  ?v10 sm:owner ?v11.
  GRAPH ?g {
    ?s sm:sensor ?v10; ?p ?o
  }
} PRIORITY 7
```

**Listing 1: Example Policy**

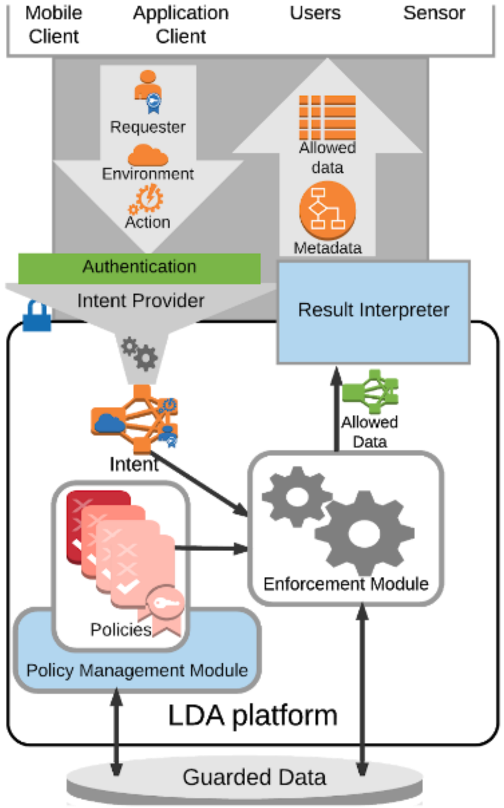


**Figure 1. The LDA platform architecture**

[1] Stojanov, Riste, et al. "Linked Data Authorization Platform." IEEE Access 6 (2018): 1189-1213.

# LDA Platform with Policy Delegation

- Extended policy management system
  - Uses the same interface as previously
  - Modified policy storage
    - each delegated policy is stored by **removing the data that is not allowed** for the given user

# Delegated policy transformation

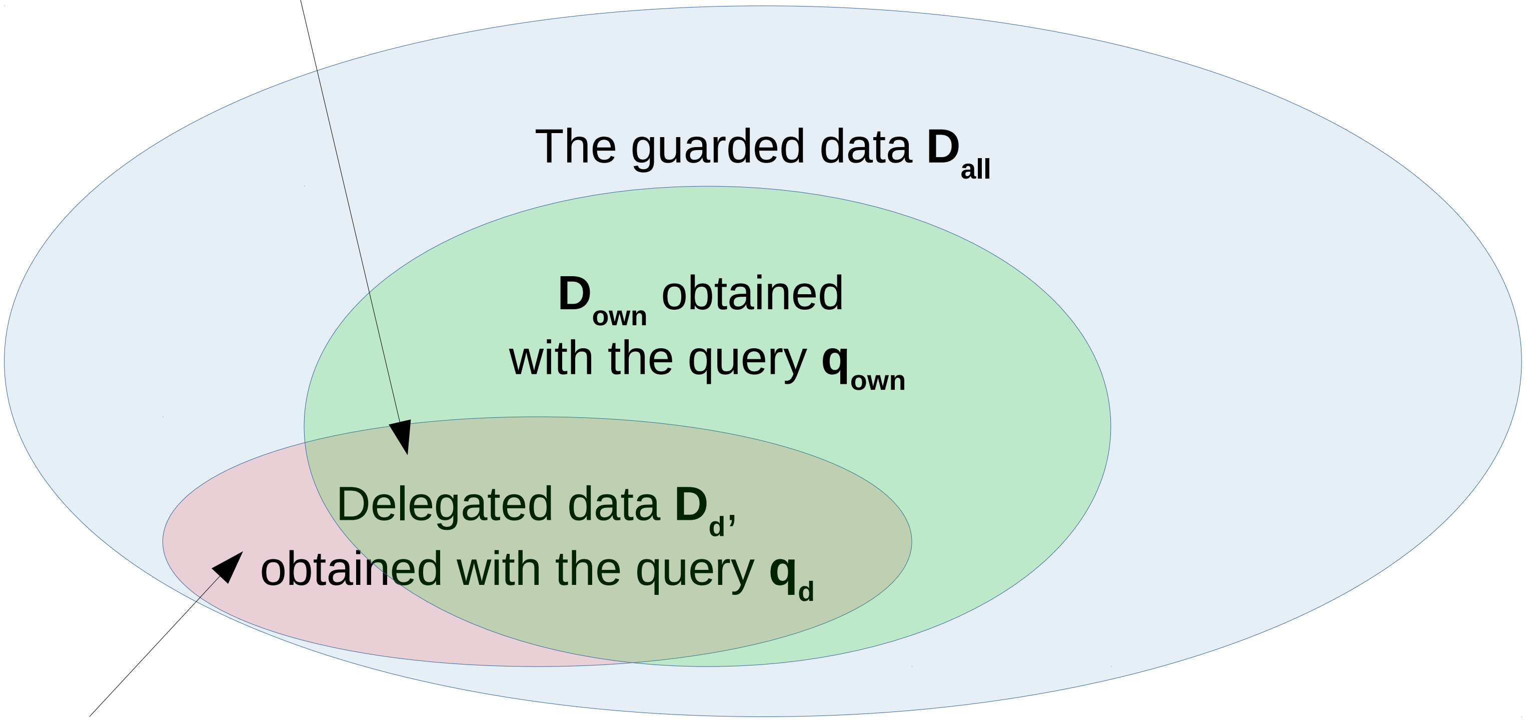
- Users can delegate rights to their data to other entities
- Allowing each user to define a policy that delegates the access of its allowed data to other users using the standard interface and policy syntax
  - Some user may try to give access to data that is not allowed for him/her
  - The system removes the data that is not allowed for the given user when the policy is stored

# Delegated policy transformation

$D_d \cap D_{own} \Leftrightarrow D_d \setminus (D_{all} \setminus D_{own})$

Implemented with the following SPARQL construct:

**… WHERE {$i_d$ . $q_d$ MINUS { $q_{all}$ MINUS { $q_{own}$ } } }**



The guarded data **$D_{all}$**

**$D_{own}$** obtained with the query **$q_{own}$**

Delegated data **$D_d$**, obtained with the query **$q_d$**

Portion from $q_d$ that should not be delegated

# Conclusion

- Flexible policy language
  - Protection to arbitrary data parts in relation to the requester and its context
- **Convenient delegation** of the authorization
- Design-time policy validation
- Ensures that the data owner can only specify policies for a **subset of its owned data**
- Activation and combination of the defined policies
  - convenience to protect multiple parts data
  - separate policies