Access Control for HTTP Operations on Linked Data

Luca **Costabello**
Serena **Villata**
Oscar **Rodriguez Rocha**
Fabien **Gandon**

Outline

- Introduction
- Shi3ld Authorization Procedure
- Shi3ld for HTTP: Scenarios
- Response Time Evaluation
- Future Work

Outline

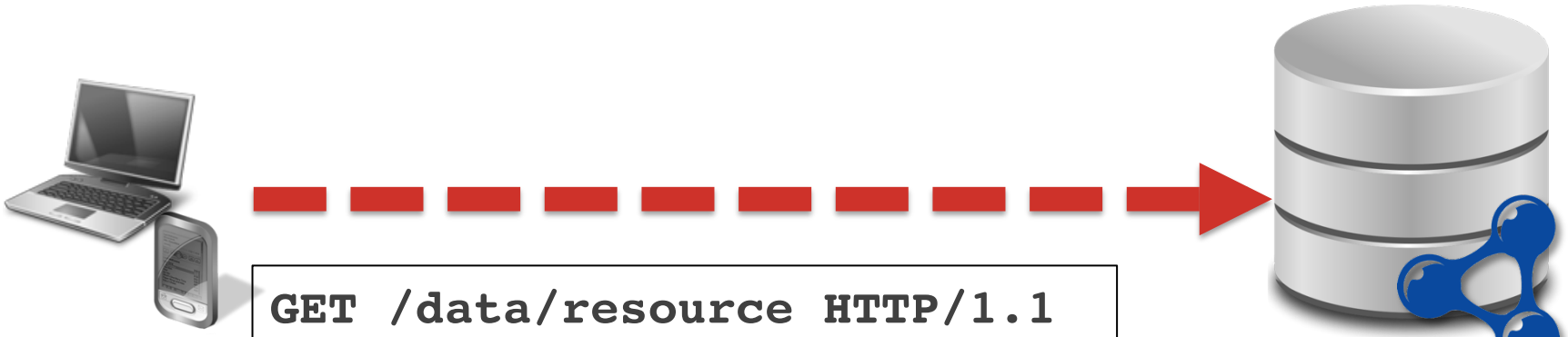
- **Introduction**
- Shi3ld Authorization Procedure
- Shi3ld for HTTP: Scenarios
- Response Time Evaluation
- Future Work

Accessing Linked Data

- HTTP URIs dereferencing
- SPARQL queries
- RDFa, search engines APIs

Accessing Linked Data

- **HTTP URIs dereferencing**
- SPARQL queries
- RDFa, search engines APIs



```
GET /data/resource HTTP/1.1
Host: example.org
...
```

Our Problem

How to design an **authorization** framework for **HTTP interaction** with Linked Data?

Access Control for Triple Stores

	HTTP Interaction	Attribute-Based AC Model	Policies in RDF/SPARQL	Resource-level Granularity	Context Awareness
Shi3ld-SPARQL [2012]	✗	✓	✓	✓	✓
WAC [2007]	✓	✗	✓	✓	✗
Proteus [2006]	✗	✓	✗	✗	✓
Abel et al. [2007]	✗	✓	✗	✓	✓
Finin et al. [2008]	✓	✓	✓	✗	✗
Flouris et al. [2010]	✗	✗	✗	✓	✗
PPO [2011]	✓	✓	✗	✓	✗

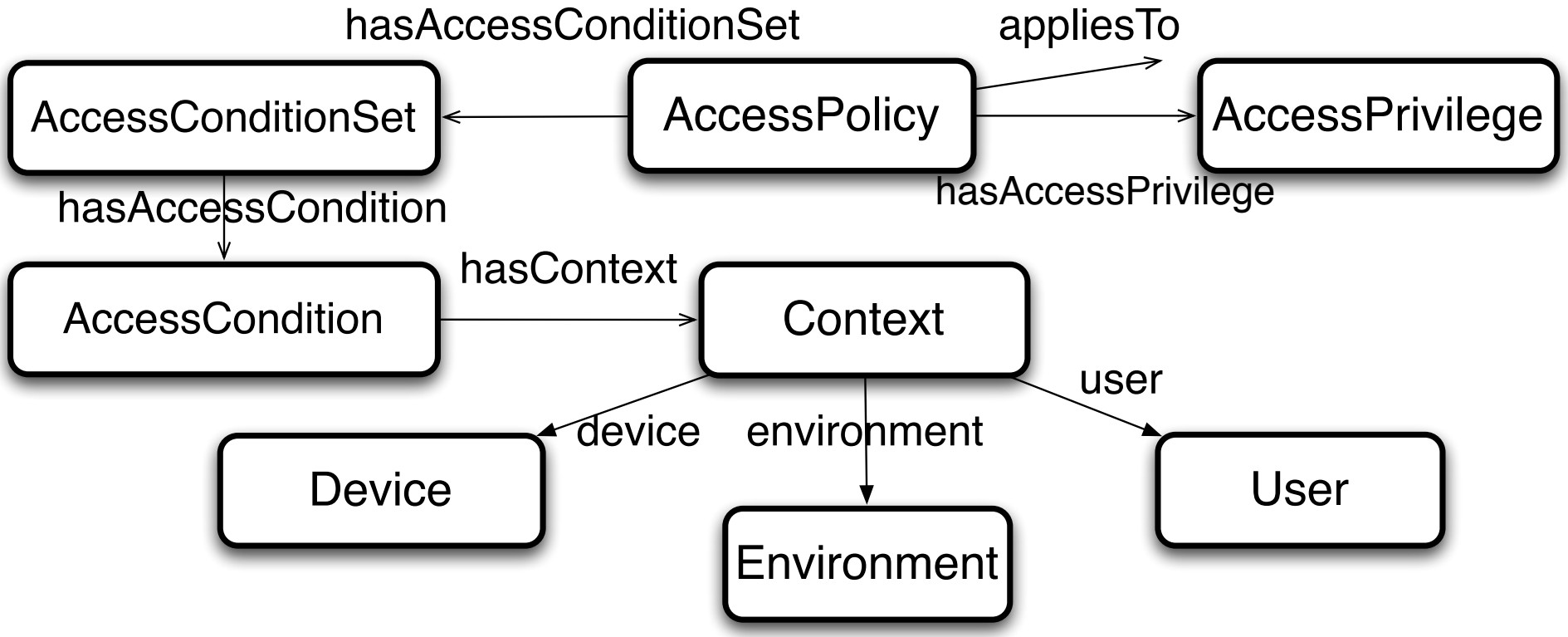
Our Proposal:
Adapting Shi3ld-SPARQL to HTTP

Our Proposal:
Adapting Shi3ld-SPARQL to HTTP

Outline

- Background
- **Shi3ld Authorization Procedure**
- Adapting Shi3ld-SPARQL to HTTP
- Response Time Evaluation
- Future Work

Shi3ld Access Policy



Two “Styles” for Access Conditions

- SPARQL-based
- SPARQL-less

Sample Access Policy (SPARQL-based)

```
:policy1 a s4ac:AccessPolicy;
         s4ac:appliesTo :resource;
         s4ac:hasAccessPrivilege s4ac:Read;
         s4ac:hasAccessConditionSet :acs1.

:acs1 a s4ac:AccessConditionSet;
       s4ac:hasAccessCondition :ac1.

:ac1 a s4ac:AccessCondition;
    s4ac:hasQueryAsk
   """ASK
       {?ctx a prissma:Context;
             prissma:environment ?env;
             prissma:user <http://example.org/john.rdf#me>.
       ?env prissma:currentPOI ?poi.
       ?poi prissma:based_near ?p.
       ?p geo:lat ?lat;geo:lon ?lon.
       FILTER(((?lat-45.8483) > 0 && (?lat-45.8483) < 0.5
       || (?lat-45.8483) < 0 && (?lat-45.8483) > -0.5)
       && ((?lon-7.3263) > 0 && (?lon-7.3263) < 0.5
       || (?lon-7.3263) < 0 && (?lon-7.3263) > -0.5 ))}""".
```

Protected resource

Access Condition to be verified:
«User must be John and request must come from a specific location»

Sample Access Policy (SPARQL-less)

```
:policy1 a s4ac:AccessPolicy;
         s4ac:appliesTo :resource;
         s4ac:hasAccessPrivilege s4ac:Read;
         s4ac:hasAccessConditionSet :acs1.

:acs1 a s4ac:AccessConditionSet;
       s4ac:hasAccessCondition :ac1.

:ac1 a s4ac:AccessCondition;
     s4ac:hasContext :ctx1.

:ctx1 a prissma:Context;
    prissma:user <http://example.org/john.rdf#me>;
    prissma:environment :env1.

:env1 a prissma:Environment;
      prissma:nearbyEntity <http://alice.org#me>.
```

Protected resource

Access Condition to be verified:

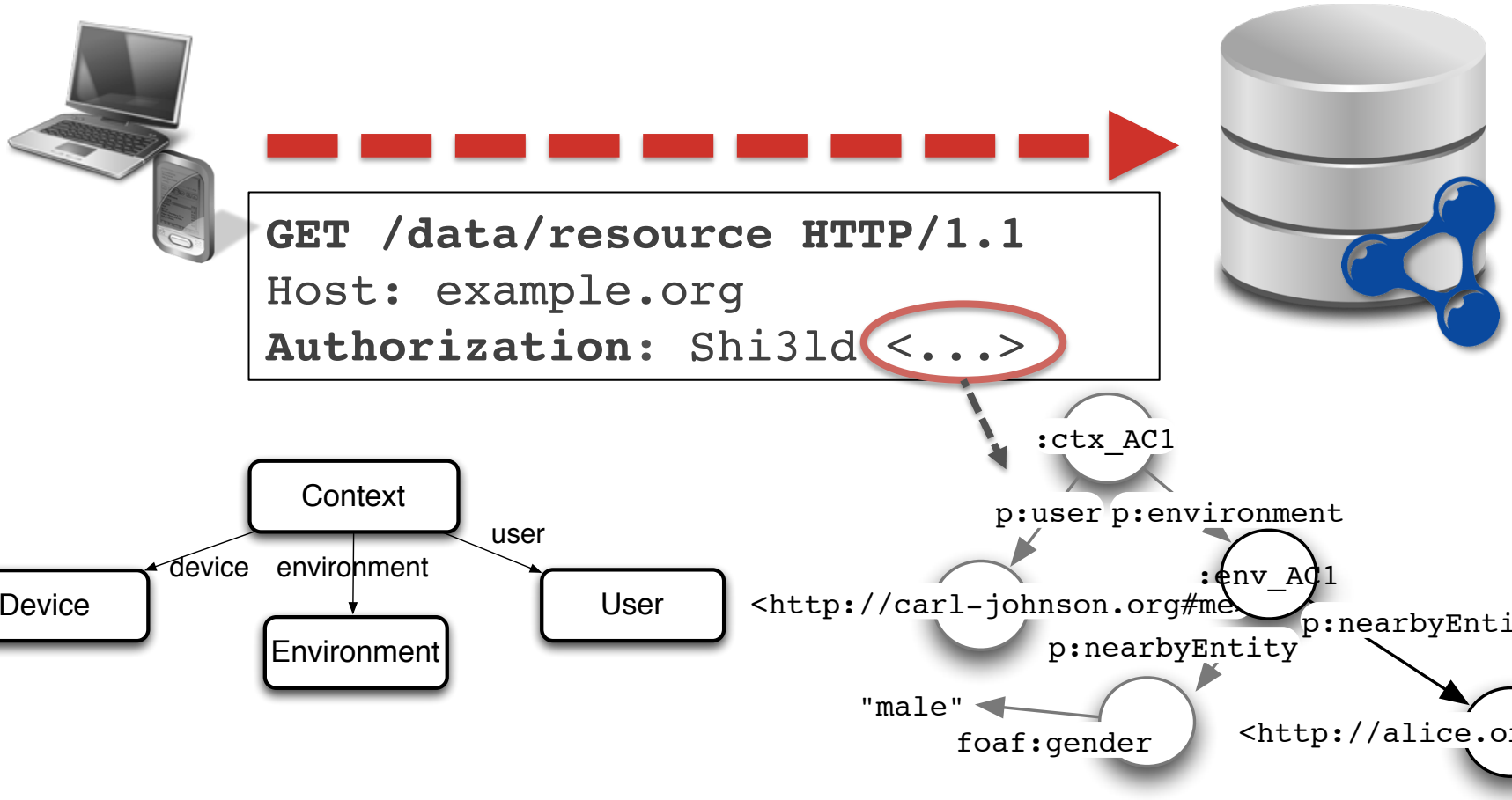
«User must be John and Alice must be nearby»

Authorization Procedure

1. Adding **Client Attributes** to HTTP operation
2. Access Conditions **Execution**
3. HTTP Response **Construction**

Authorization Procedure

1. Adding **Client Attributes** to HTTP operation
2. Access Conditions Execution
3. HTTP Response Construction



Authorization Procedure (SPARQL-based)

1. Adding Client Attributes to HTTP operation
2. Access Conditions **Execution**
3. HTTP Response Construction

```
ASK {?context
        a prissma:Context;
        prissma:user ex:john.}
```

= "false"

```
VALUES (?context) {(:client_attributes)}
```

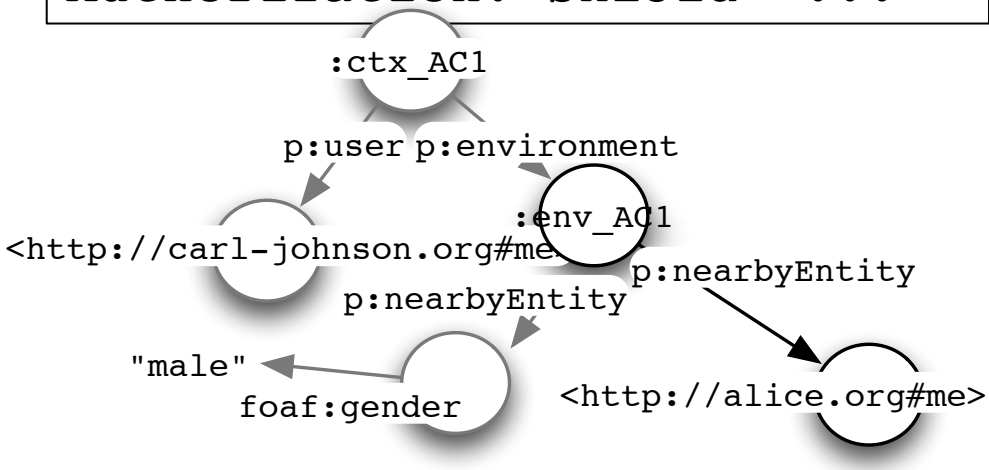
```
GET /data/resource HTTP/1.1
Host: example.org
Authorization: Shi3ld <...>
```

Authorization Procedure (SPARQL-less)

1. Adding Client Attributes to HTTP operation
2. Access Conditions **Execution**
3. HTTP Response Construction

```
:context a prissma:Context;
         prissma:user ex:john.
```

```
GET /data/resource HTTP/1.1
Host: example.org
Authorization: Shi3ld <...>
```



"no match"

Authorization Procedure

1. Adding Client Attributes to HTTP operation
2. Access Conditions Execution
3. HTTP Response **Construction**

Outline

- Introduction
- Authorization Procedure
- **Shi3ld for HTTP: Scenarios**
- Response Time Evaluation
- Future Work

HTTP Operations on Linked Data: Our Scenarios

- SPARQL 1.1 Graph Store Protocol (GSP)

```
GET /rdf-graph-store?graph=... HTTP/1.1
Host: example.com
Accept: text/turtle; charset=utf-8
```

```
CONSTRUCT { ?s ?p ?o }
WHERE { GRAPH <...>
{ ?s ?p ?o } }
```

- W3C Linked Data Platform (LDP) 1.0

  Best practices for a read-write HTTP-based Linked Data architecture.

HTTP Operations on Linked Data: Our Scenarios

- SPARQL 1.1 Graph Store Protocol (GSP)

  Shi3ld-GSP

- W3C Linked Data Platform (LDP) 1.0

  Shi3ld-LDP

  - **SPARQL-based**
  - **SPARQL-less**

HTTP Operations on Linked Data: Our Scenarios

- SPARQL 1.1 Graph Store Protocol (GSP)

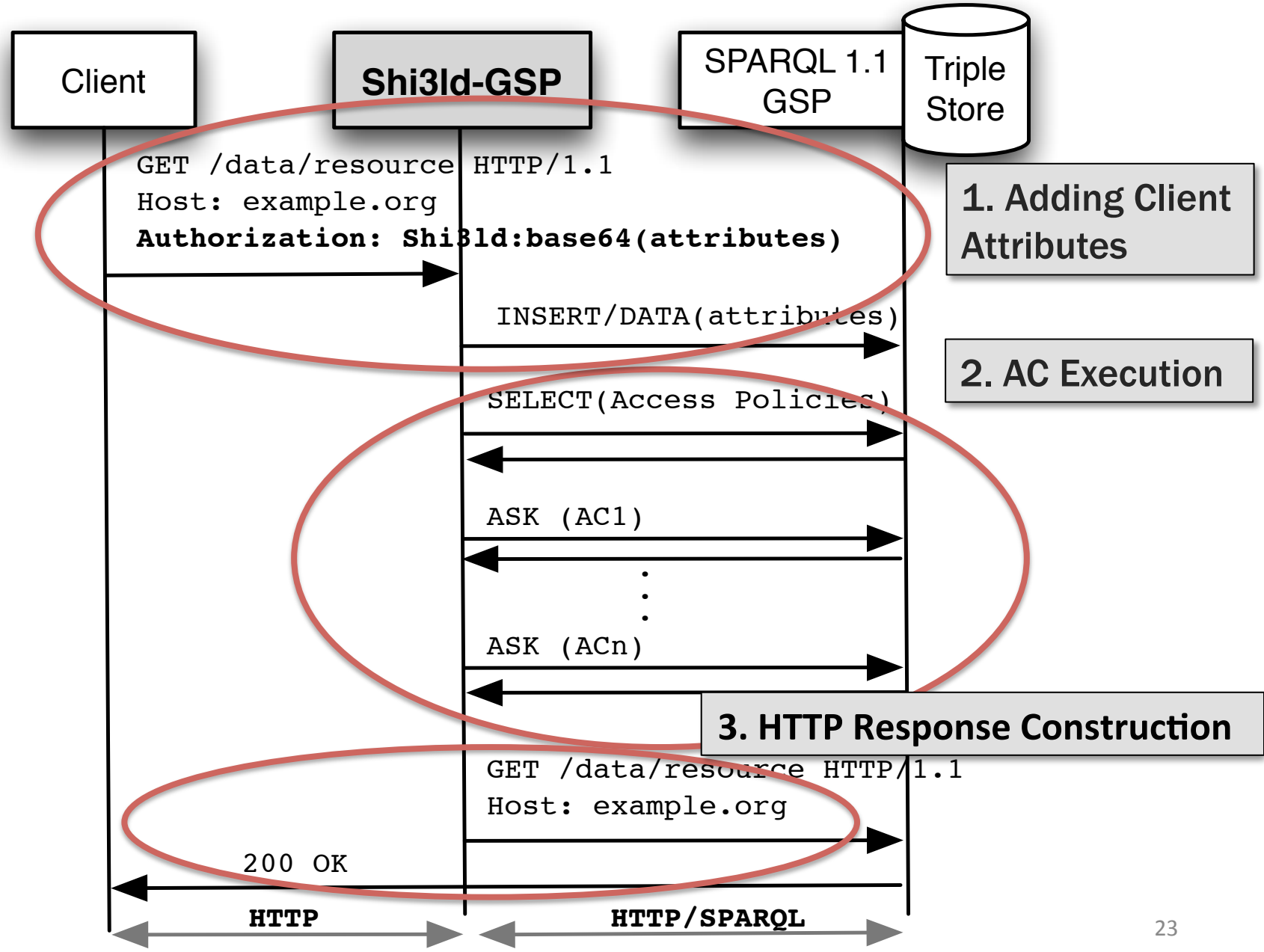
  Shi3ld-GSP

- W3C Linked Data Platform (LDP) 1.0

  Shi3ld-LDP

  - **SPARQL-based**
  - **SPARQL-less**

Shi3ld- GSP


Client
Shi3ld-GSP
SPARQL 1.1 GSP
Triple Store
GET /data/resource HTTP/1.1
Host: example.org
Authorization: Shi3ld:base64(attributes)
INSERT/DATA(attributes)
SELECT(Access Policies)
ASK (AC1)
ASK (ACn)
GET /data/resource HTTP/1.1
Host: example.org
200 OK
HTTP
HTTP/SPARQL
1. Adding Client Attributes
2. AC Execution
3. HTTP Response Construction

HTTP Operations on Linked Data: Our Scenarios

- SPARQL 1.1 Graph Store Protocol (GSP)

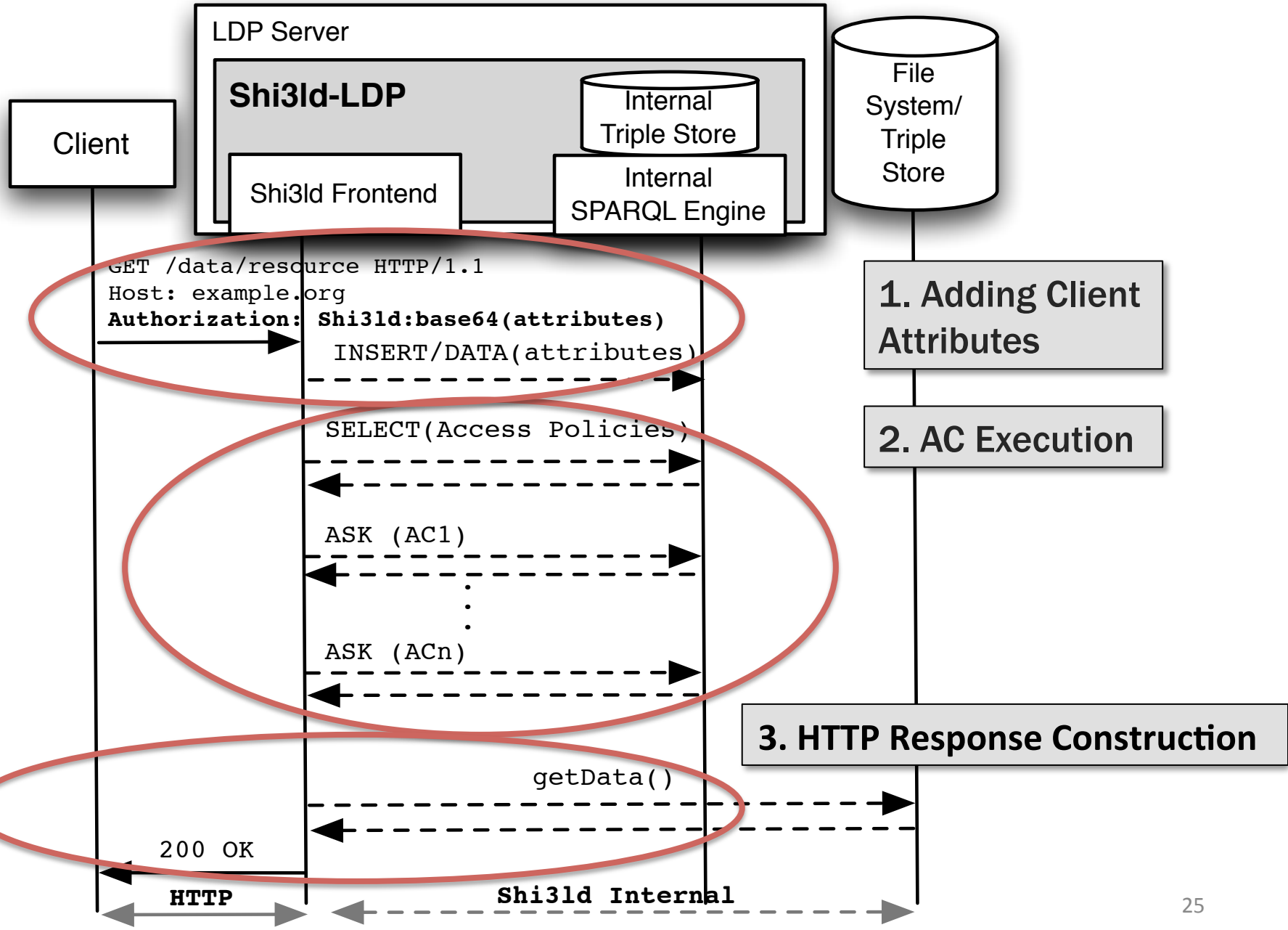
  Shi3ld-GSP

- W3C Linked Data Platform (LDP) 1.0

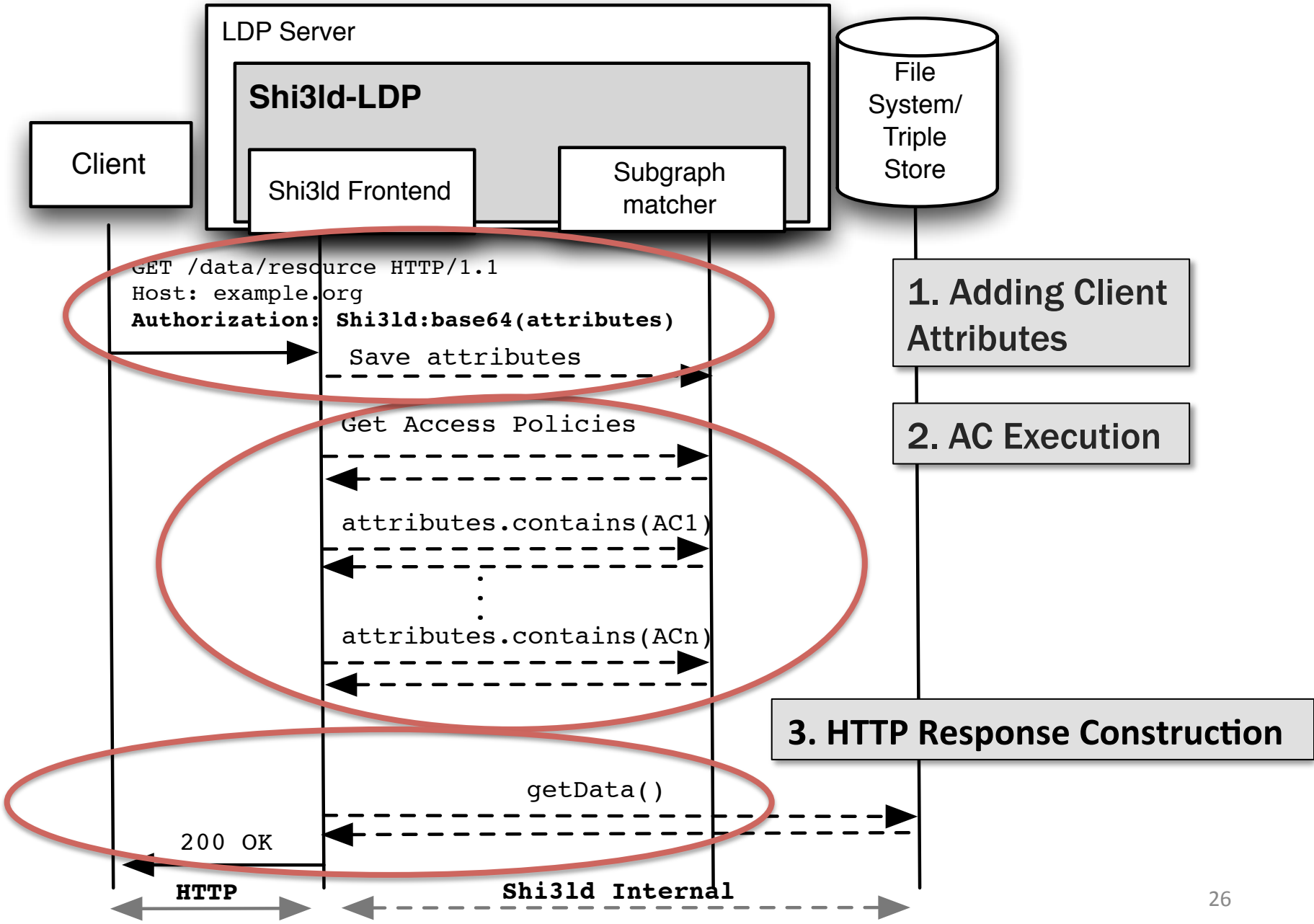
  Shi3ld-LDP

  - **SPARQL-based**
  - **SPARQL-less**

Shi3ld-LDP (SPARQL-based)



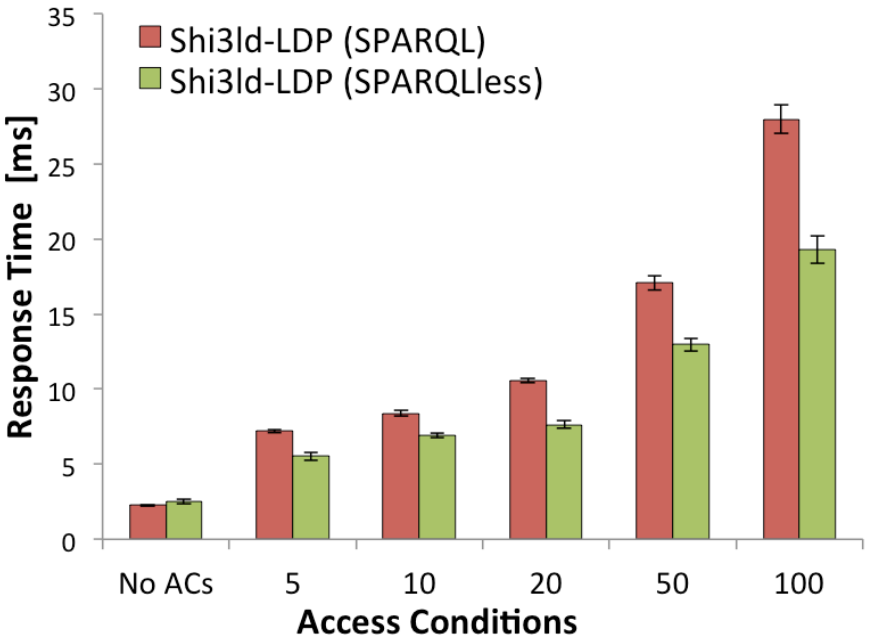
Shi3ld-LDP (SPARQL-less)

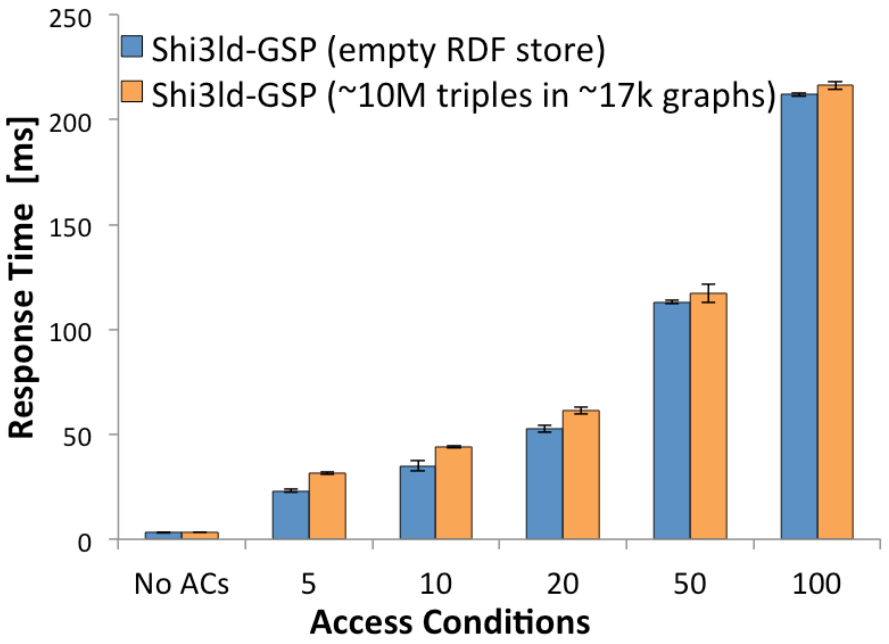


Outline

- Background
- Authorization Procedure
- Shi3ld for HTTP: Scenarios
- **Response Time Evaluation**
- **Future Work**

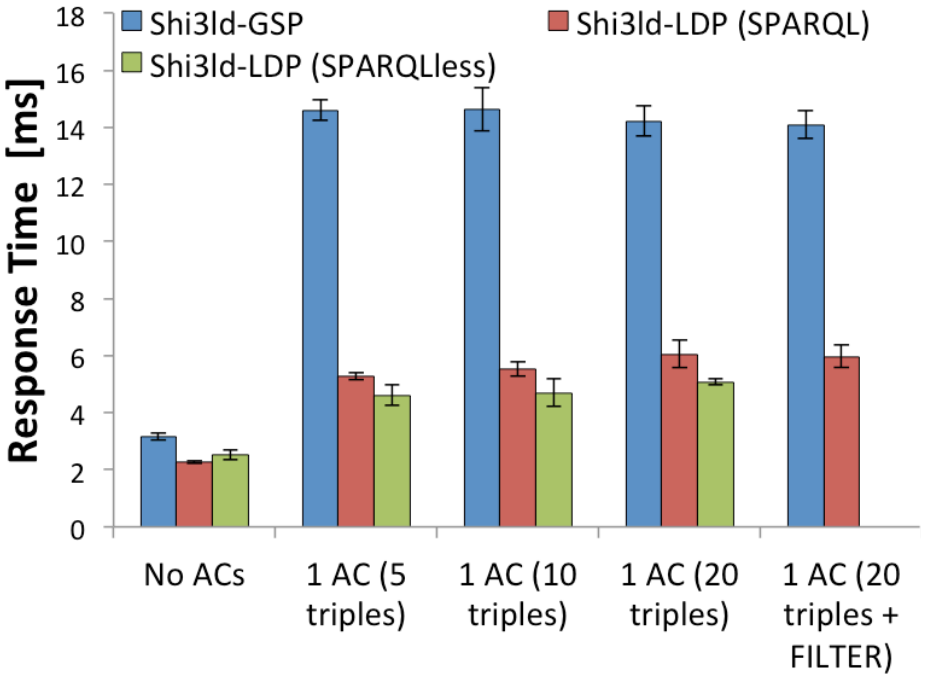
Response Time Evaluation

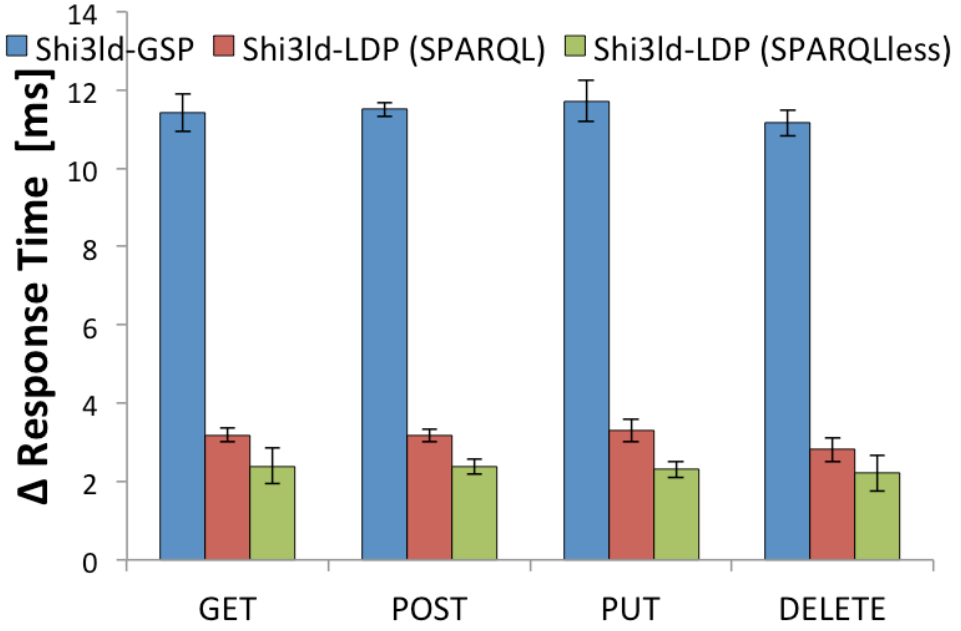




- Response time linear w/ AC #
- SPARQL-less: 25% faster
- Empty RDF Store: only 14% faster

Response Time Evaluation





- AC complexity does not affect response time
- Response time independent from HTTP method

Outline

- Background
- Authorization Procedure
- Shi3ld for HTTP: Scenarios
- Response Time Evaluation
- **Future Work**

bit.ly/shi3ld-http

Future Work

- Client Attributes Trustworthiness
- Client Attributes Caching
- Admin UI

Luca **Costabello**
@lukostaz

Serena **Villata**
@serena_villata

Oscar **Rodriguez-Rocha**
@orocha

Fabien **Gandon**
@fabien_gandon