# Defining Access Control in ONE Record

## Manage access to API operations with ontologies

**The main goal of access control is to minimize the risk of unauthorized operations on resources. Access control is a fundamental component of security compliance that ensures security technology and access control policies are in place to protect the data.**

**In ONE Record, access to resources can be handled by using Access Control Lists (ACLs) stored in the backend systems of the ONE Record Servers and defined using the Web Access Control standard from W3C.**

## What is Web Access Control (WAC)?

According to W3C WebAccessControl specifications page, "Web Access Control is a decentralized system for allowing different users and groups various forms of access to resources where users and groups are identified by HTTP URIs". It enforces access control based on the **Access Control List (ACL)** RDF resource associated with the requested resource. ACL allows access to agents (users, groups, etc.) to perform various kinds of operations (read, write, control, etc) on the respective resource.

## How can I define to whom I give data access?

In ONE Record, access to resources can be specified by using Access Control Lists (ACLs) associated to specific Logistics Objects (LOs). Each LO resource possesses a related ACL containing a set of **Authorization** statements that describe:

- **who** has access to that resource;
- **what types** (or **modes**) **of access** they have.

Each Authorization is a single rule for access, such as "`entities one and two may write to LO logisticObjectRef`", described with a set of RDF properties.

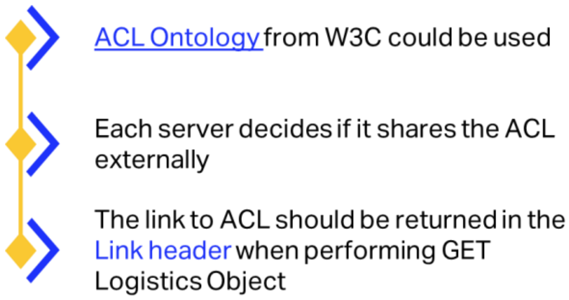
ONE Record recommends the use of the ACL ontology in order to express the Authorizations. As the ACL is specific to each ONE Record Server and it is not a mandatory requirement to make it available to external entities, any other kind of data model/ontology can be used instead.

Given an URI for an individual LO, a ONE Record Client can discover the location of its corresponding ACL by performing a `GET` request and parsing the `rel="acl"` **Link** header.

GET `http://myServer/myAirline/logisticsObject` would return the headers:

```
HTTP/1.1 200 OK
Link:
<http://myServer/myAirline/logisticsObject/acl>; rel="acl"
```

Example of GET LO returning an ACL



ACL Ontology from W3C could be used

Each server decides if it shares the ACL externally

The link to ACL should be returned in the Link header when performing GET Logistics Object

Access Control overview

**Note**: ONE Record Clients must not assume that the location of an ACL resource can be derived from an LO's URI.

## What types of Authorizations can be defined?

ONE Record recommends the definition of three types of Authorization:

1. **Single Authorization** – when a single company identifier from the Internet of Logistics has access to the LO;
2. **Group Authorization** – when a group of company identifiers has access to the LO. The ONE Record Server can define internally groups of access such as Airlines, Ground Handlers, Customs, etc.
3. **"Public" Authorization** – when every authenticated company identifier accessing the LO URI can retrieve the data.

## What modes of access ONE Record recommends?

ONE Record specifies three modes of access on LOs:

READ / **GET**
Read the contents (including querying it)

WRITE / **POST** and **PATCH**
Write contents or modify part of it

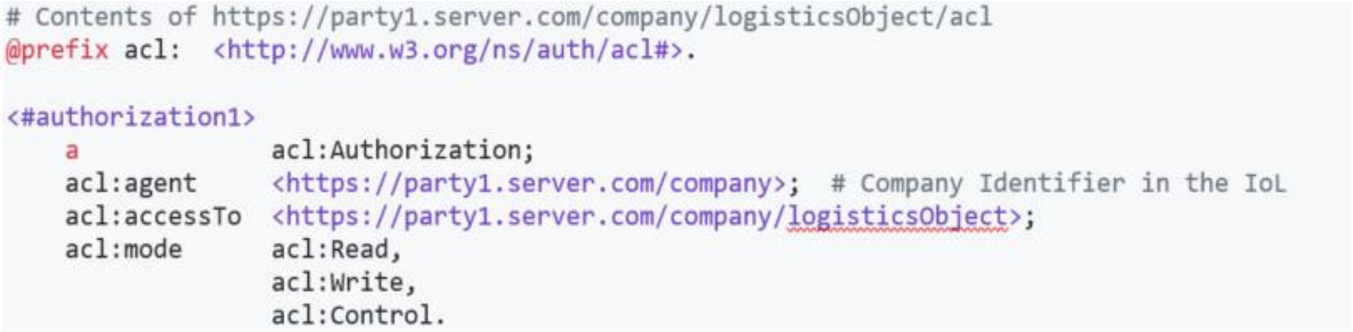
CONTROL / **GET**, **POST** and **PATCH**
Read and Write

**Note**: In a delegation scenario, when delegating access to a resource to a third party, a new Authorization element should be added to the ACL.

## Conclusion

In ONE Record, access control is achieved by using a dedicated Access Control List associated to each LO. ONE Record Servers might choose to share or not the ACLs to external parties and they can use the data model they desire for defining the access control rules. However, the usage of standard ontologies such as W3C ACL is recommended in scenarios in which ACLs are shared publicly.

More info at https://www.iata.org/one-record/.



```
# Contents of https://party1.server.com/company/logisticsObject/acl
@prefix acl:  <http://www.w3.org/ns/auth/acl#>.

<#authorization1>
    a             acl:Authorization;
    acl:agent     <https://party1.server.com/company>;  # Company Identifier in the IoL
    acl:accessTo  <https://party1.server.com/company/logisticsObject>;
    acl:mode      acl:Read,
                  acl:Write,
                  acl:Control.
```

Example of Authorization