### ONE Record API and Security Overview

#### Draft for Cargo Services Conference

December 7, 2018

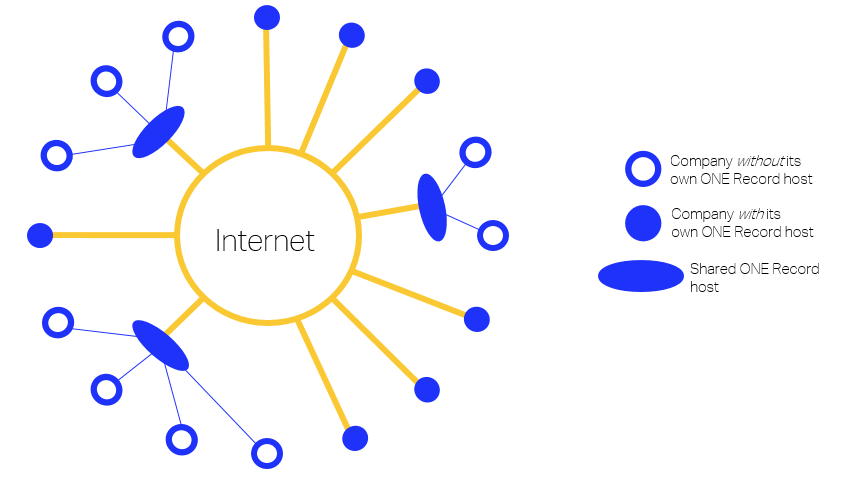
# Glossary

|  |  |
| --- | --- |
| Term | Description |
| Authentication | A process that validates the identity of a Trusted Party |
| Authorization | A process that determines whether a Trusted Party is allowed to access a specific Logistics Object |
| Identity Provider | A service that allows Parties to authenticate themselves and obtain a secure token that will allow them to identify themselves with ONE Record Hosts and get access to Logistics Objects |
| Host | The service that hosts Logistics Objects on a web server on behalf of one or more ONE Record Publishers |
| Logistics Internet | A network of Hosts that can share Logistics Objects over the internet using the ONE Record data model, API and security standards |
| Logistics Object | A data object that represents a meaningful entity in the logistics business. These may represent documents like air waybills but may also be more granular such as company details or a transport segment description.  Logistics Objects are specified in a common data model by IATA. |
| Party | Company that participates in the logistics business |
| Publisher | The Party that makes their Logistics Objects available through a ONE Record Host |
| Subscriber | The Party that subscribes to Logistics Objects in order to receive updates automatically |
| Trust Center | An organization that hosts registers trusted parties and operates an Identity Service. This organization must be accredited by IATA to provide this service. |
| Trusted Party | Party that has registered with an Accredited Identity Provider and has possession of a valid certificate to prove this |
| URI | In the web context, this is a URL that uniquely identifies a Logistics Object and a Host |

# Introduction

The purpose of ONE Record is to facilitate direct digital communication between air cargo stakeholders. Mature web technologies allow for such an objective to be reached supported by robust internet network infrastructure.

The basic premise of ONE Record, i.e. direct digital communication, is easily understood and achieved through the HTTP web standards. As shown below, any company that implements a ONE Record host or that uses the services of a shared host can share data with any other company that has done so as well.



Companies and shared servers that want to share data across the logistics internet will implement an API that meet the ONE Record API and security standards described in this document.

**Note:** It should be stressed that ONE Record is a standard is not a system or a service operated by IATA; it is a design guide for implementing systems that can share logistics data universally and independently.

# ONE Record API

#### ONE Record API for data sharing

The ONE Record API is a web API that allows parties to publish logistics objects through ONE Record hosts. Direct access is available to trusted parties that have been authenticated and authorized to access these resources.

To facilitate message flow, trusted parties can subscribe to logistics objects through the Publish/Subscribe pattern that allows them to subscribe to a specific publisher & logistics objects type channel.

#### Accessing logistics objects

Authenticated trusted parties may access logistics objects of publishers for which they are authorized through the Logistics Object URI with a GET request as follows.

Request header specifies accepted media types application/turtle or application/ld+json and the response header includes the corresponding content type.

If the HTTP response status code is 2XX (success) then the Logistics Object is returned in the response body.

If the HTTP response status code is 4XX (client error) or 5XX (server error) then an error description may be included in the response body.

#### Active data sharing

In addition to the need to access a logistics object of publishers, trusted parties also need the facility to push logistics objects to their partners. One mechanism that serves this purpose uses a publish & subscribe type design pattern.

Partners also need to be able to interact on the data within the logistics objects themselves. This requires mechanisms that allow them to notify the publisher of the logistics object that they wish to make a change to that logistics object and for the publisher to log that change and process it.

These data sharing patterns are being evaluated and the most commonly appropriate patterns will be elaborated on an API basis.

##### 

# Security

#### Overview

ONE Record provides a secure network for data exchange between parties. This security is ensured in several stages.

1. Parties need to register with an accredited Trust Center. This will give them Trusted Party status.
2. Before being able to access logistics objects, a Trusted Party needs to authenticate with an Identity Provider operated by the Trust Center that they registered with and who will provide them with a secure token once authenticated.
3. Using the secure token the Trusted Party can access logistics objects through the API of the relevant ONE Record host.
4. If the publisher has authorized the Trusted Party to access a logistics object, then its ONE Record host will serve that logistics object as per HTTP request.

This approach established the following requirements.

#### Trust Centers and Identity Providers

Trust Centers act as registrars of trusted parties and provide an Identity Provider service to facilitate access to ONE Record hosts.

The registration of a trusted party requires verification of their status as a reputable company in the logistics supply chain, their contact details and roles and permissions in the logistics internet.

#### Accreditation of Trust Centers

There may be multiple Trust Centers and a common standard will be defined for the registration and authentication of trusted parties. IATA will also establish an accreditation process for Trust Centers which will also established mutual acceptance of the trust status that these Trust Centers will confer on the parties registering with them.

#### ONE Record Identity

Trusted parties will be registered with a unique identity. This identity and other registration details will be included in the token following their authentication such that publishers can identify the trusted party and assess their trusted status.

#### Authorization

Access to Logistics Objects by authenticated trusted parties is at the discretion of the publisher and through its ONE Record host. Business processes will be established to prescribe a common approach to authorization of access to logistics objects by trusted parties and their roles within the logistics process.

#### Data security

HTTPS with TLS encryption must be used for any communication over HTTP of One Record hosts and technical components