

Interactive Cargo

Standard
Operating
Procedures
IoT data sharing



Standard Operating Procedure - Introduction

Shippers, cargo handlers and stakeholders of the air cargo supply chain wish to know with confidence the procedures and requirements for the IoT data sharing.

This Standard Operating Procedures (SOP) document contains the operational steps that stakeholders of the air cargo supply chain should follow when collecting data via IoT devices and sharing them with their stakeholders.



Standard Operating Procedure – Scope and framework

The scope of the Standard Operating Procedure is to outline the activities and responsibilities of the stakeholders of the air cargo industry related to IoT Data sharing.

The Standard Operating Procedure will introduce:

- Description of IoT devices & sensors used for data collection about shipments during transport
- Connectivity options for IoT devices
- Data sharing architecture for data collected from IoT devices
- Using ONE Record for data sharing and processing
- The ONE Record data model
- Data security and access control in ONE Record
- Use case to illustrate the use of ONE Record for data sharing

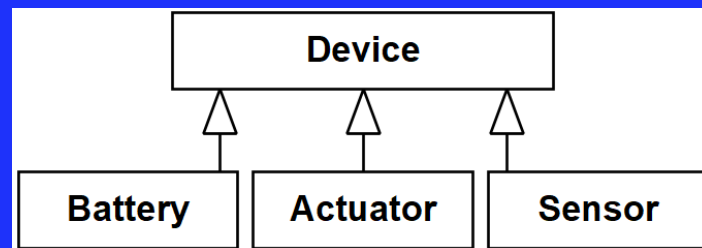


IoT Device

A tangible object that provides the technological interface to interact with or obtain information about physical and other digital entities in an Internet-of-Things (IoT) ecosystem. The IoT device extends physical entities and allows them to be part of the digital world.

Device composition

An IoT device may include (but is not limited to) one or more sensors, one or more actuators or one or more batteries. IoT devices may be able to observe or act, or both, one or more properties.

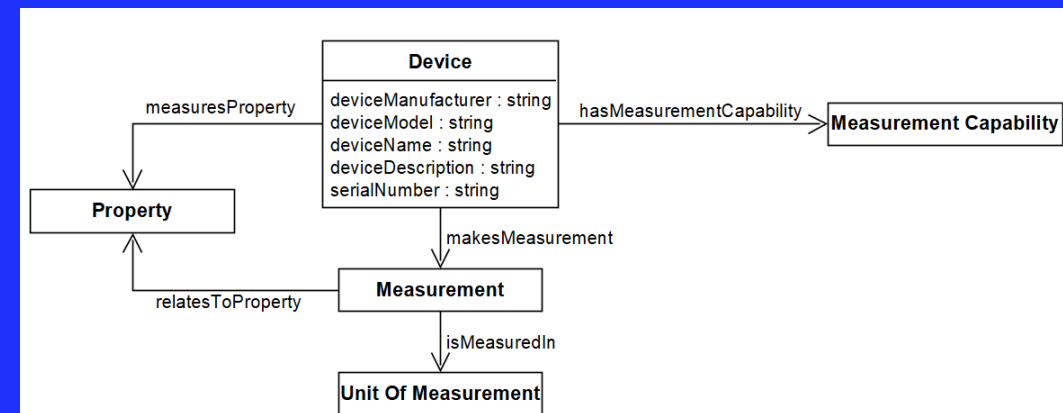


PROPERTY. A quality that can be measured.

MEASUREMENT. The measured value of a given property in a unit of measurement. A timestamp identifies when the measurement was taken.

UNIT OF MEASUREMENT. A definite magnitude of a quantity that is used as a standard for measurement of the same kind of quantity. The use of the International System of Units such as radian, hertz, pascal, degree Celsius, and lux, is recommended.

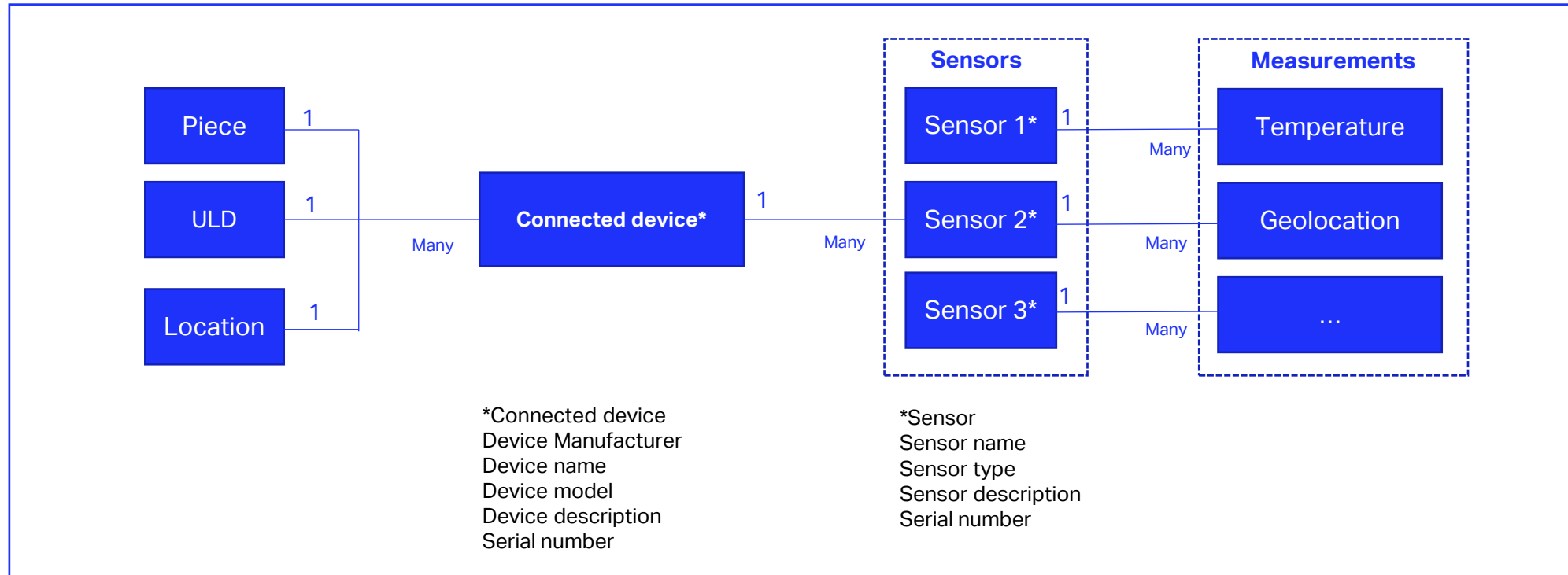
MEASUREMENT CAPABILITY. Specification of the device's capability in the environmental conditions.



NOTE: Please refer to Recommended Practice 1692 on IoT Device Data sharing in Air Cargo (RP1692)

Sensor

- They refer to a device that senses and reports physical or chemical properties from the physical environment and transforms them into digital data that can be transmitted over a network. The purpose of a sensor is to collect analog data from the physical world and translate it into digital data assets.
- Sensors contain information to identify them: name, description, serial number, type.
- The type gives information on the type of measurements (property) recorded by the sensor. The RP1692 explains multiple types of sensors such as geolocation, thermometer or humidity.
- Most observed properties have a datatype double and a unit of measurement. Only the geolocation differs as the geolocation contains a triplet of values latitude, longitude, altitude.
- An **IoT device** can be linked to multiple Sensor objects that record a single type Measurements.



NOTE: Please refer to Recommended Practice 1692 on IoT Device Data sharing in Air Cargo (RP1692)

Connectivity

Connectivity is the piece of the IoT puzzle which enables the “things” to communicate and exchange data.

The connection can be achieved via wired or wireless networks. However, wired network is unsuitable for most IoT applications due to the limited range determined by the wire. Most IoT applications require bigger range, hence wireless connectivity.

Connectivity Options for IoT



There are many connectivity options available for IoT, including but not limited to cellular, satellite, WiFi, low-power wide-area networks (LPWAN), and Bluetooth.



When selecting a connectivity option, there are many factors to take into consideration: range (maximum distance over which data can be sent), bandwidth (amount of data that can be sent), power consumption (battery lifetime), costs, reliability, and availability, for example.


As each IoT device may require a different option for connectivity, this SOP does not recommend any specific option of connectivity to communicate data.

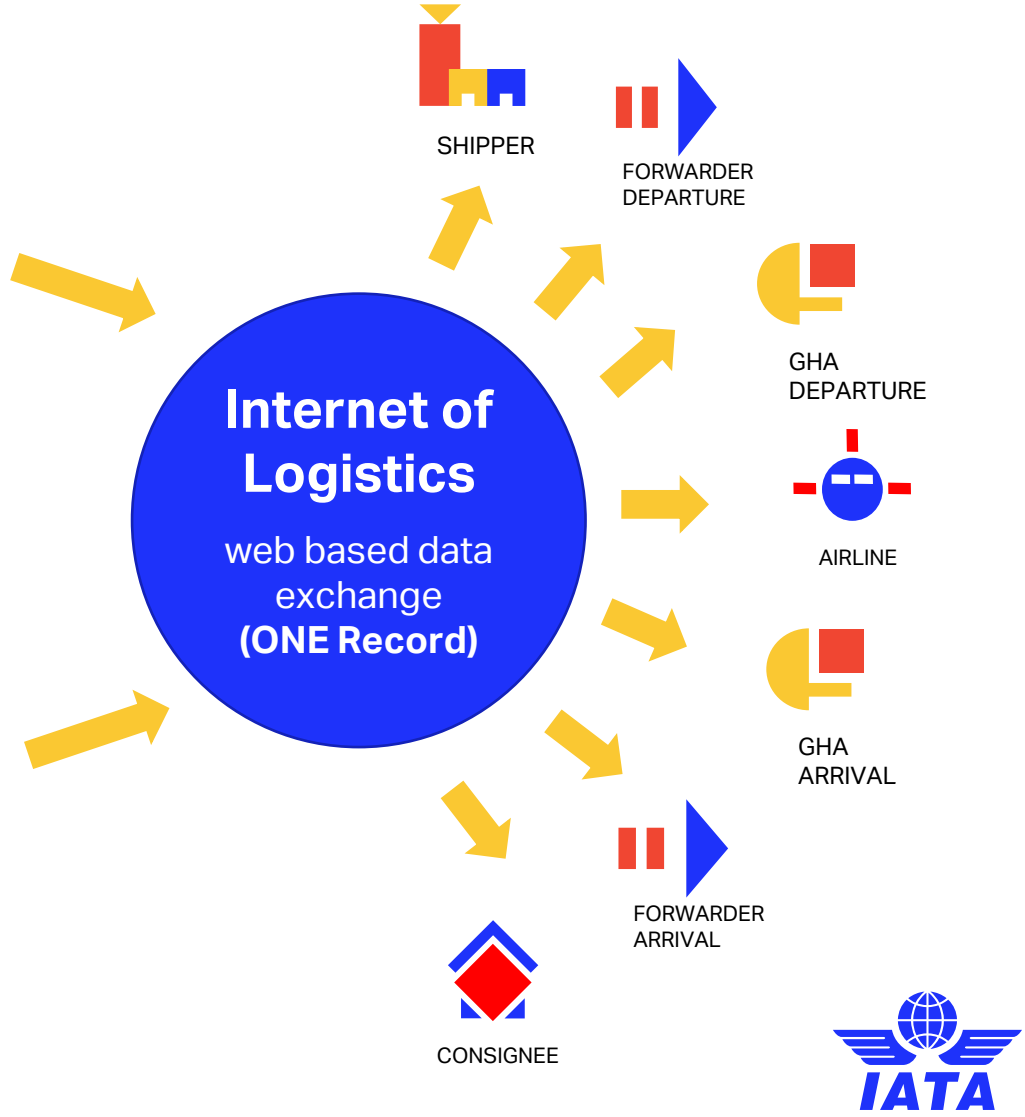


Data sharing architecture

1  direct connectivity to the IoT data platform (e.g., cellular, LPWAN) 

2  data collected via wireless readers (e.g., WiFi, BLE, RFID) to the local IoT data server 

3  data collected via wired connection to the local IoT data server



Data sharing architecture

1

Direct connectivity to the IoT data platform

1. Attribute(s) detected by sensors
2. Input from sensor recorded on IoT device
3. Data shared via connectivity to the IoT data platform (e.g., cellular, LPWAN)
4. Data owner shares data and allows access
5. Data is available to authorized parties of the data exchange

2

Data collected via wireless readers

1. Attribute(s) detected by sensors
2. Input from sensor recorded on IoT device
3. Data collected via wireless readers (e.g., WiFi, BLE, RFID)
4. Data stored on local IoT data server
5. Data owner shares data and allows access
6. Data is available to authorized parties of the data exchange

3

Data collected via wired connection to the local IoT data server

1. Attribute(s) detected by sensors
2. Input from sensor recorded on IoT device
3. Data collected via wired connection
4. Data stored on local IoT data server
5. Data owner shares data and allows access
6. Data is available to authorized parties of the data exchange

ONE Record data sharing – minimum requirements

In order to be able to implement IoT data sharing (either via gateways or connectivity options), the following minimum requirements are needed:

All concerned stakeholders signed the **Multilateral Data Agreement***

All concerned stakeholders **incorporate the ONE Record Ontology** into existing systems

All concerned stakeholders **implemented the ONE Record API**** for the purpose of data sharing

All concerned stakeholders have **secured the ONE Record API**

All concerned stakeholders **are connected to each other via ONE Record for the purpose of data exchange**

** To learn more about the Multilateral Data Agreement, please refer to the [MDA site](#)*

*** To start implementation, please refer to the [ONE Record Implementation Playbook](#)*

**** To read more about ONE Record Security, please refer to the [ONE Record API & Security specification](#)*

ONE Record

- ONE Record is the new **IATA standard for data sharing** and creates a single record view of the shipment.
- This standard defines a **common data model** for the data that is shared via standardized and secured web API.
- It aims to address the main challenges of e-freight and unlock the possibilities of a full digital air cargo industry and create opportunities for new value-added services and business models.

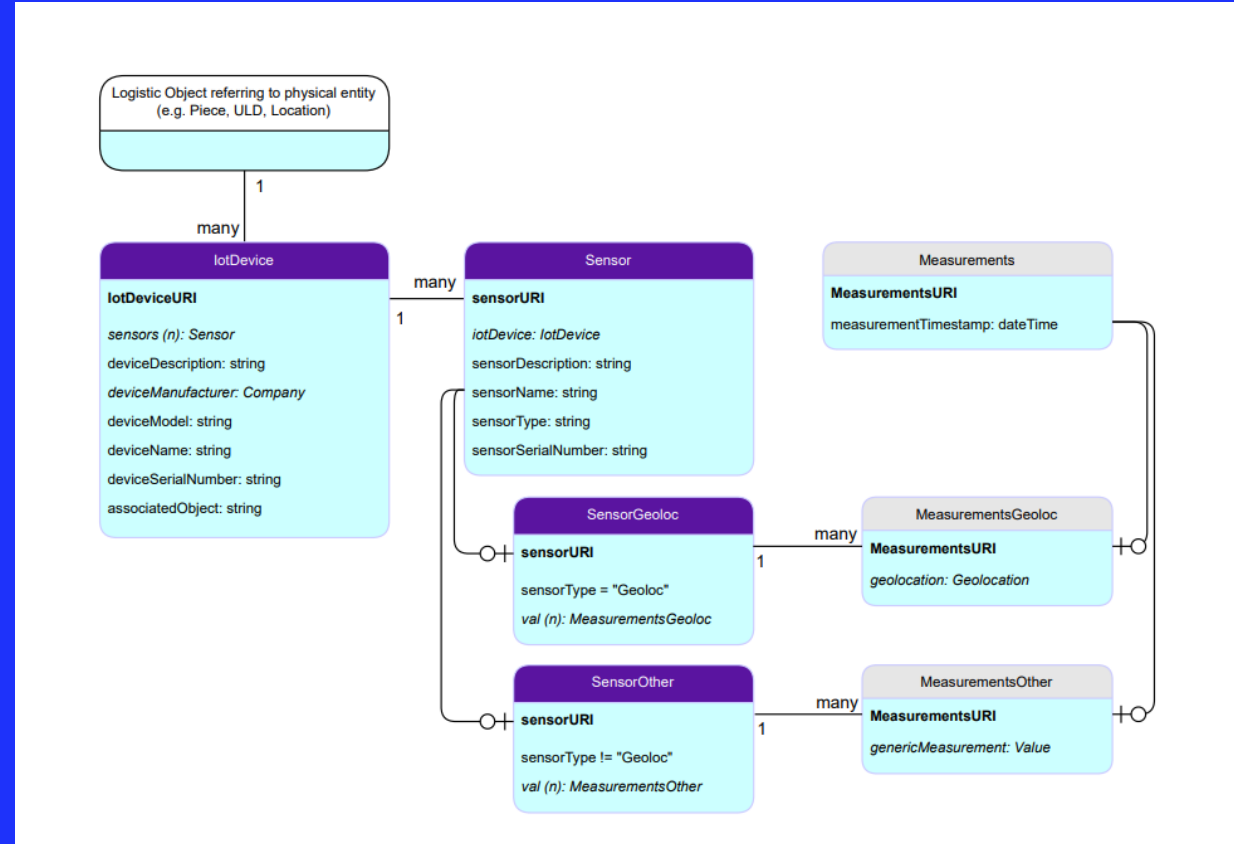
NOTE: Please read the [ONE Record implementation playbook](#) for details of the ONE Record Implementation Steps

The ONE Record data model

The Data Model is an essential part of ONE Record and aims to provide the air cargo industry with a standard data structure for data exchange using JSON-LD that facilitates data integration with existing and new data services.

The data model was first defined to cover the interaction of General Cargo between shippers and freight forwarders as well as between freight forwarders and Airlines, this refers to the Airline Core Ontology.

The latest progress made on the ONE Record data model, ontology and technical specifications can be found on the dedicated GitHub space: <https://github.com/IATA-Cargo/ONE-Record>



Logistic object

As part of the Internet of Logistics, the ONE Record data model is using Logistic Objects (LO). In the ONE Record context a LO can be defined as follows:

- It represents an essential element of the supply chain: physical objects, legal documents, etc.
- It has its own lifecycle and can have statuses or events;
- It can be shared and subscribed to by any stakeholder involved in the logistics supply chain;

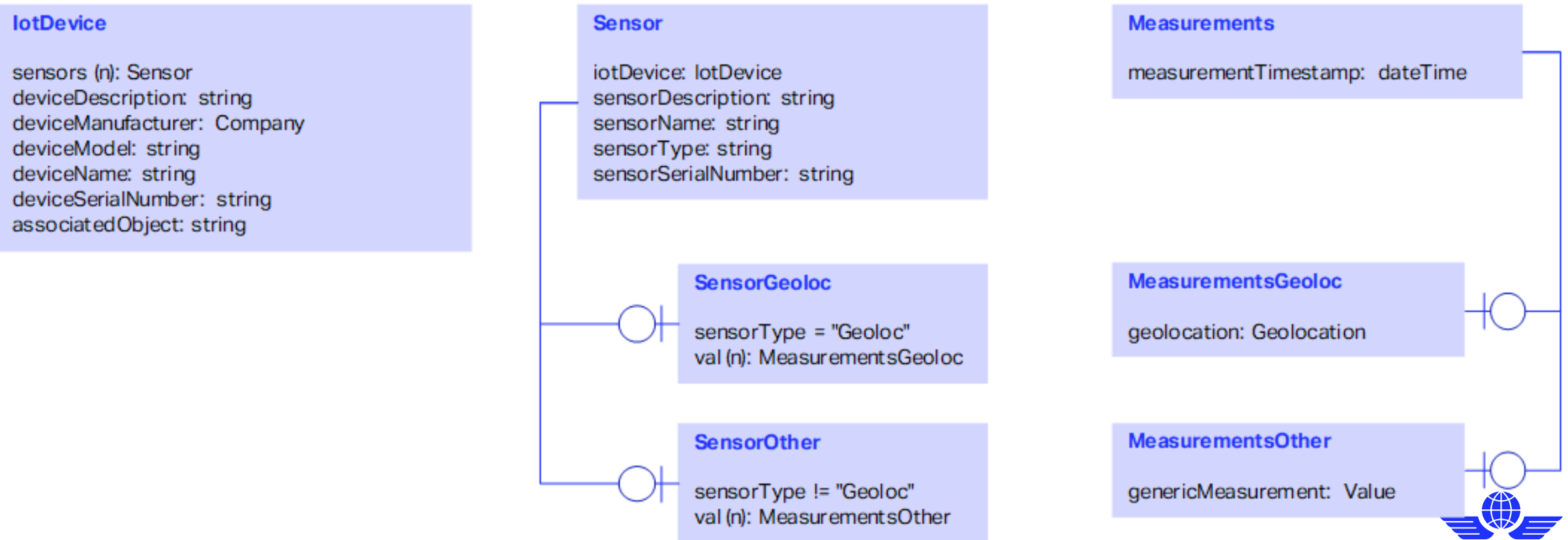
As a digital twin of a physical object, a LO can have IoT data. The Unique Resource Identifier (URI) of a LO contains its endpoint (c.f. API & Security specifications available on the Github space ONE Record) as well as an identifier that can be an existing unique identifier standardized among the industry (e.g., UPID for pieces or Airway bill numbers). Following the design principles defined above, we have defined a semantic data model, or conceptual data model, which focuses on the Logistic Objects of the data model.

For additional detail on the Logistic objects, please refer to <https://github.com/IATA-Cargo/ONE-Record>



Expected interactions with cargo

To consider the specificity of the Geolocation sensor type, subtypes of Sensor and Measurements have been added to ease the usage of the data model.



Data security in ONE record

ONE Record / Security

The security of ONE Record relies on 3 components:



IDENTIFICATION

Who are you?



AUTHENTICATION

Are you who you claim to be?



AUTHORIZATION

Do you have the right credentials?



ONE Record / Security

The security of ONE Record is managed through a Trust Network



ONE Record / Security

The security of ONE Record is managed through a Trust Network

IDENTIFICATION

- Register the ONE Record participant through a dedicated accreditation process
- Issue a ONE Record certificate as an identifier

AUTHENTICATION

- Verify the validity of the ONE Record certificate

AUTHORIZATION

- Managed by the data owners. Can grant access to specific companies or groups of companies



- ONE Record as a basis for data sharing on the Internet of Logistics needs to ensure that data sharing is secure, i.e., that the participants sharing data are known, identified, authenticated and authorized for data access.
- The security of ONE Record relies on three components:
 - Identification
 - Authentication
 - Authorization
- Every stakeholder is accountable for their own data, store data based on preference and control data access
- Security mechanism is in place for data access and data sharing via access controls

NOTE: Please refer to [ONE Record API & Security specification](#) for details



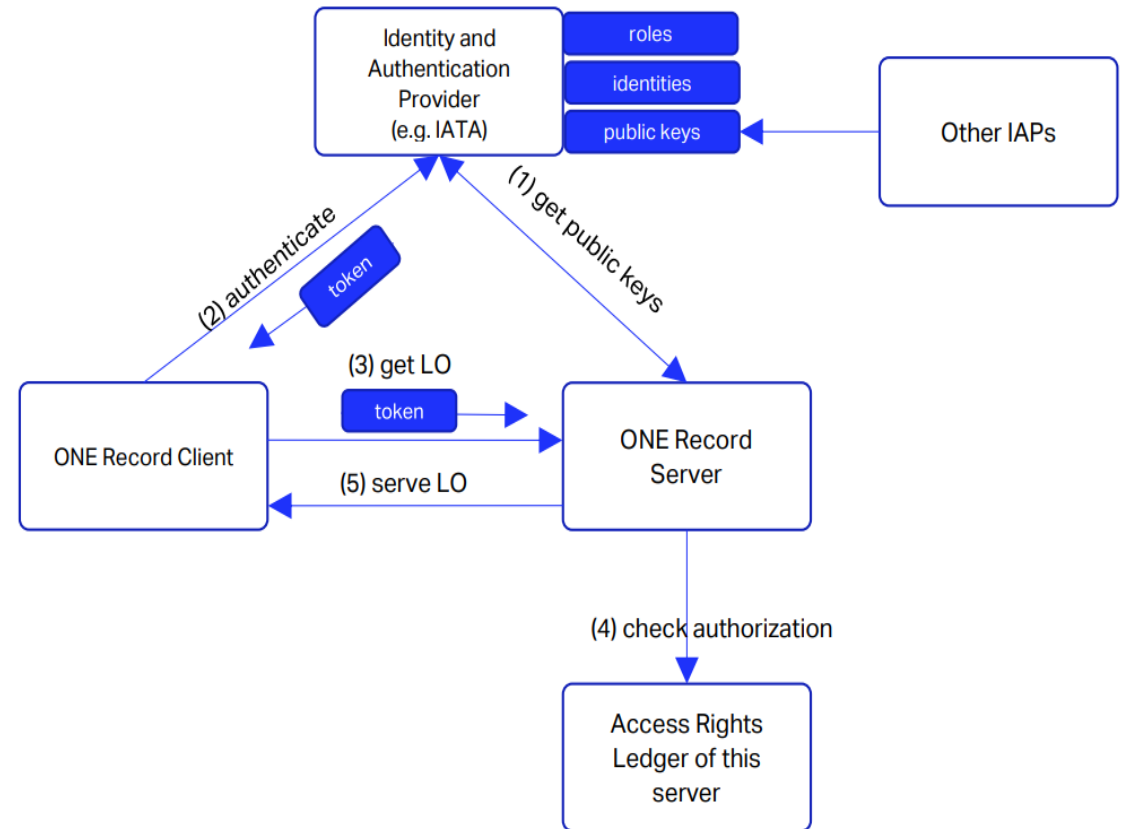
Data security in ONE Record

ONE Record, as a basis for data sharing in the Internet of Logistics needs to ensure that data sharing is secure, i.e., that the participants sharing data are known, identified, authenticated and authorized for data access.

Since the Internet of logistics is potentially vast and may cover many different stakeholder groups, there is a need for a network of Identity and Authentication Providers (IAP) that can ensure the validity of the Internet of Logistics participants for their respective stakeholder groups. Each IAP will also hold an inventory of public keys of other IAP's that they trust. Therefore, Internet of Logistics participants only need to interact with their own IAP and still be able to verify the validity of other participants even though they may be registered with another IAP.

The IAP's will use Public Key Cryptography to guarantee the authenticity of the Internet of Logistics participant whose identity and roles are in the payload of a signed Json Web Token. Once, validated, this is then used as a bearer token to access the Logistics Object.

Identity and Authentication Providers (IAP)



NOTE: Please refer to [ONE Record API & Security specification](#) for details



ONE Record – Access control

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.




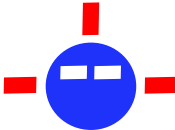

In ONE Record, access to resources can be specified by using Access Control Lists (ACLs) associated to specific Logistics Objects (LOs). Each LO resource possesses a related ACL containing a set of Authorization statements that describe:

- who has access to that resource;
- what types/modes of access they have.

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

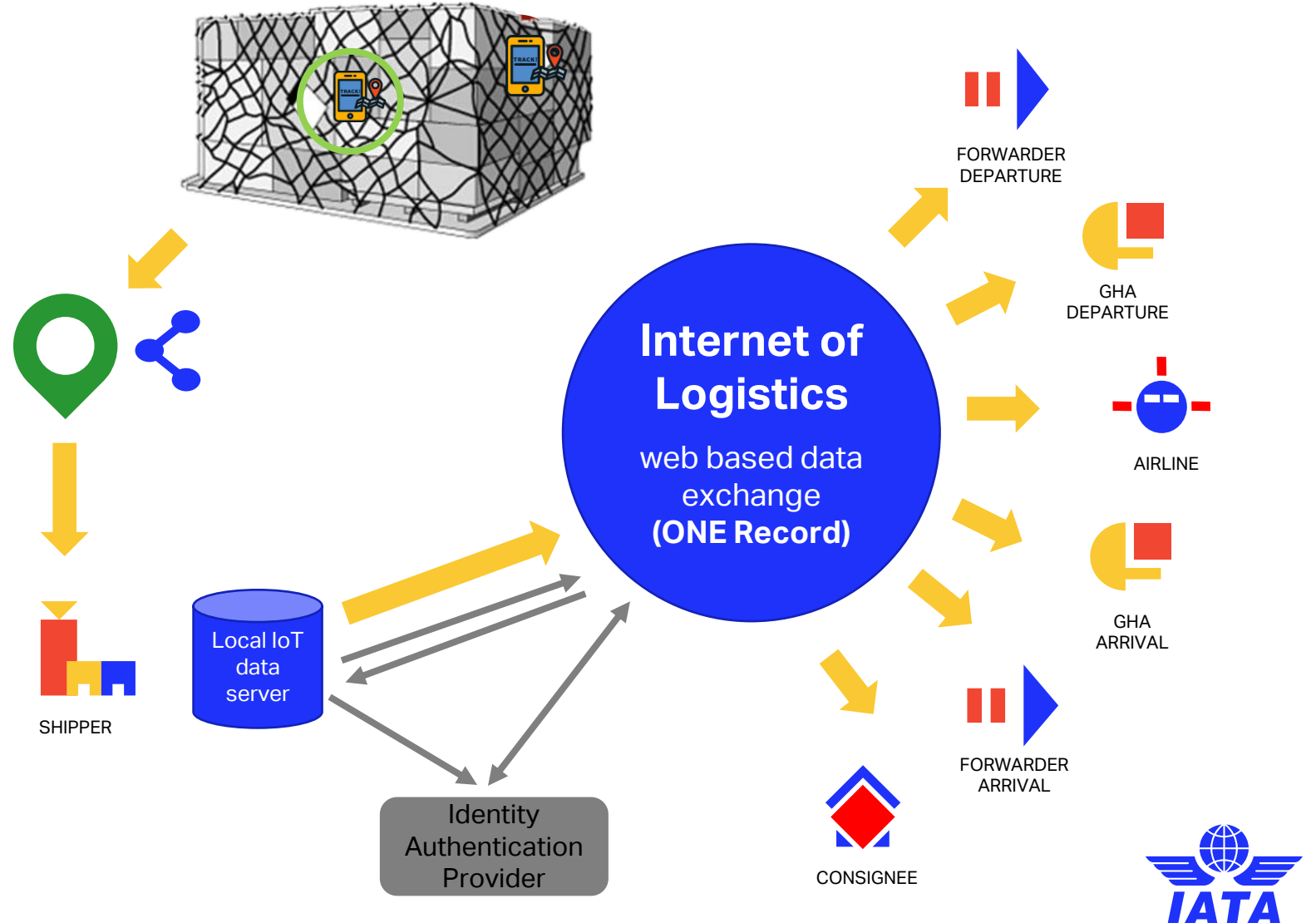
IoT data collection and sharing simplified use case

<p>Shipper includes tracking device to shipment to measure temperature and humidity</p> <p>Shipper needs data on shipment condition during the journey</p>	 <p>FORWARDER</p>	<p>Airline needs data on shipment location and condition</p>	 <p>GHA</p>	<p>Consignee needs information on shipment location and condition</p>
 <p>SHIPPER</p>	<p>Forwarder attaches tracking device to shipment to monitor location</p> <p>Forwarder needs data on shipment location</p>	 <p>AIRLINE</p>	<p>GHA needs data on shipment location</p>	 <p>CONSIGNEE</p>

Stakeholder level data collection & sharing



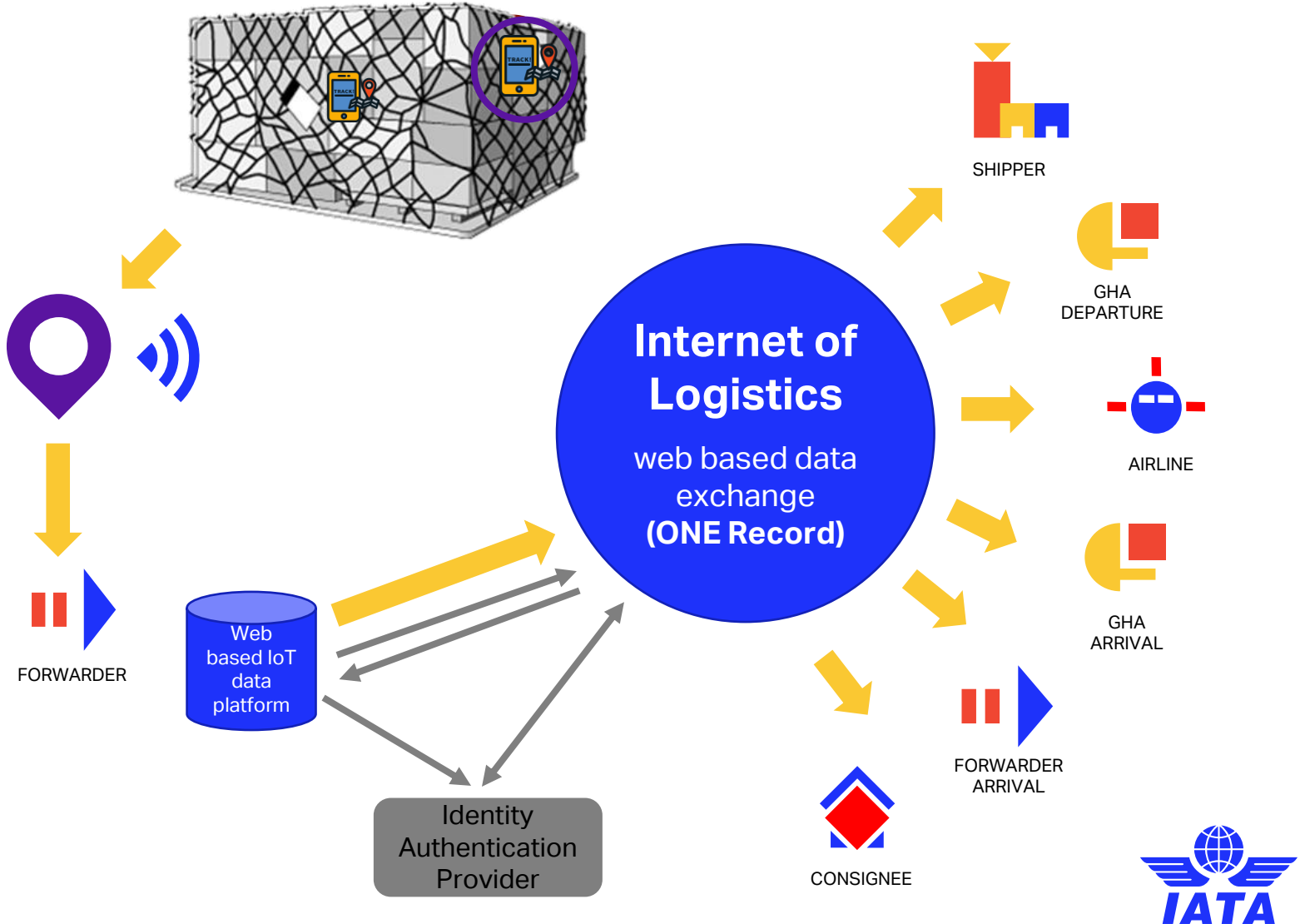
- Shipper collects data on the shipment condition using IoT devices placed in the shipment
- Data from IoT devices is collected via wireless readers (e.g., WiFi, BLE, RFID)
- Data is stored on local IoT data server of the shipper
- The shipper, as data owner shares data and allows access




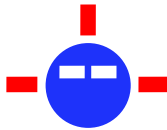

Stakeholder level data collection & sharing

FORWARDER

- Forwarder collects data on shipment location using IoT device attached to the shipment
- Data from the IoT device is shared via direct connectivity to the IoT data platform
- Data is stored on the data platform of the forwarder
- Forwarder, as the owner of the data, makes data available to other stakeholders



Stakeholder level data collection & sharing

 <p>GHA DEPARTURE & ARRIVAL</p>	<p>Airline reads data on shipment location and condition shared by other stakeholders via data exchange platform based on ONE Record</p>
<p>Airline reads data on shipment location and condition shared by other stakeholders via data exchange platform based on ONE Record</p>	 <p>AIRLINE</p>
 <p>CONSIGNEE</p>	<p>Airline reads data on shipment location and condition shared by other stakeholders via data exchange platform based on ONE Record</p>

