



ONE Record – Access delegation

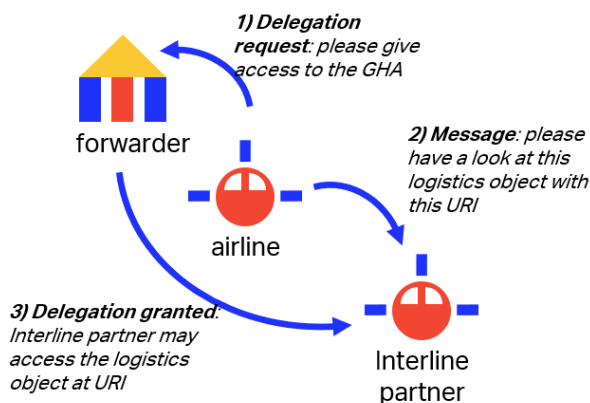
Sharing data downstream

One unique feature of transport and logistics chains is their sequential nature. Cargo is moved from the shipper to a forwarder to a ground handling agent to an airline etc. Each party along this chain has data that needs to be shared downstream and status or clarifications back upstream. The challenge is that in most cases, these parties along the transport chain don't always know each other but do need each other's data.

For example, an import customs agent may need information from the originating shipper between whom there is no relationship. Traditionally, each party copies data and carries it forwards so the issue doesn't exist. With data sharing however, data needs to stay at its source. This is solved by a mechanism where any party along a transport chain can delegate their own access to data from their upstream partner with one or more downstream partners and vice versa.

Access Delegation

Before a company can access a logistics object of another company, it needs to be authorized to do so and the server that hosts the logistics objects will determine whether to grant access. Typically, when a company creates a logistics object on a server, it will share the URI of that logistics object with another company and grant them access by default. For example, a forwarder creates a logistics object for a booking request and then sends the URI to the airline. When the airline then accesses the logistics object, the forwarder will usually grant access to the airline but only to that airline and no one else.



What if the airline sends the URI of the booking request to an interline partner? When the interline partner accesses the logistics object through the API, the forwarder will not grant access because only the first airline has been granted access. To avoid this situation, when the airline sends the URI to their interline partner, for example, then they also send a message to the forwarder that they would like their interline partner to get access to the logistics object. The forwarder will accept this because they trust the airline to only share with trusted partners. When the interline partner now tries to access the logistics object, they will be granted access.

Revoking access

In the same way, if the airline in this example wishes to revoke access to a certain logistics object from their interline partner, they can make a revocation request to the forwarder and from then on, the interline partner would no longer have access.

Trust Chains: trusting partners along the transport chain through

The concept of companies requesting a delegation of access to their partners can also be used by these partners themselves, who are now third parties. In the example above, the interline partner



can request that the forwarder gives access to their ground handler. The forwarder will grant the access on the basis that they trust the airline who has trusted their interline partner who trusts their ground handler.

These chains of trust are based on business partnerships and trust in the transport chain. It ensures that the company who has shared a logistics object on a server, always knows who may access this and at any time, it can revoke all or part of the chain of trust.

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

