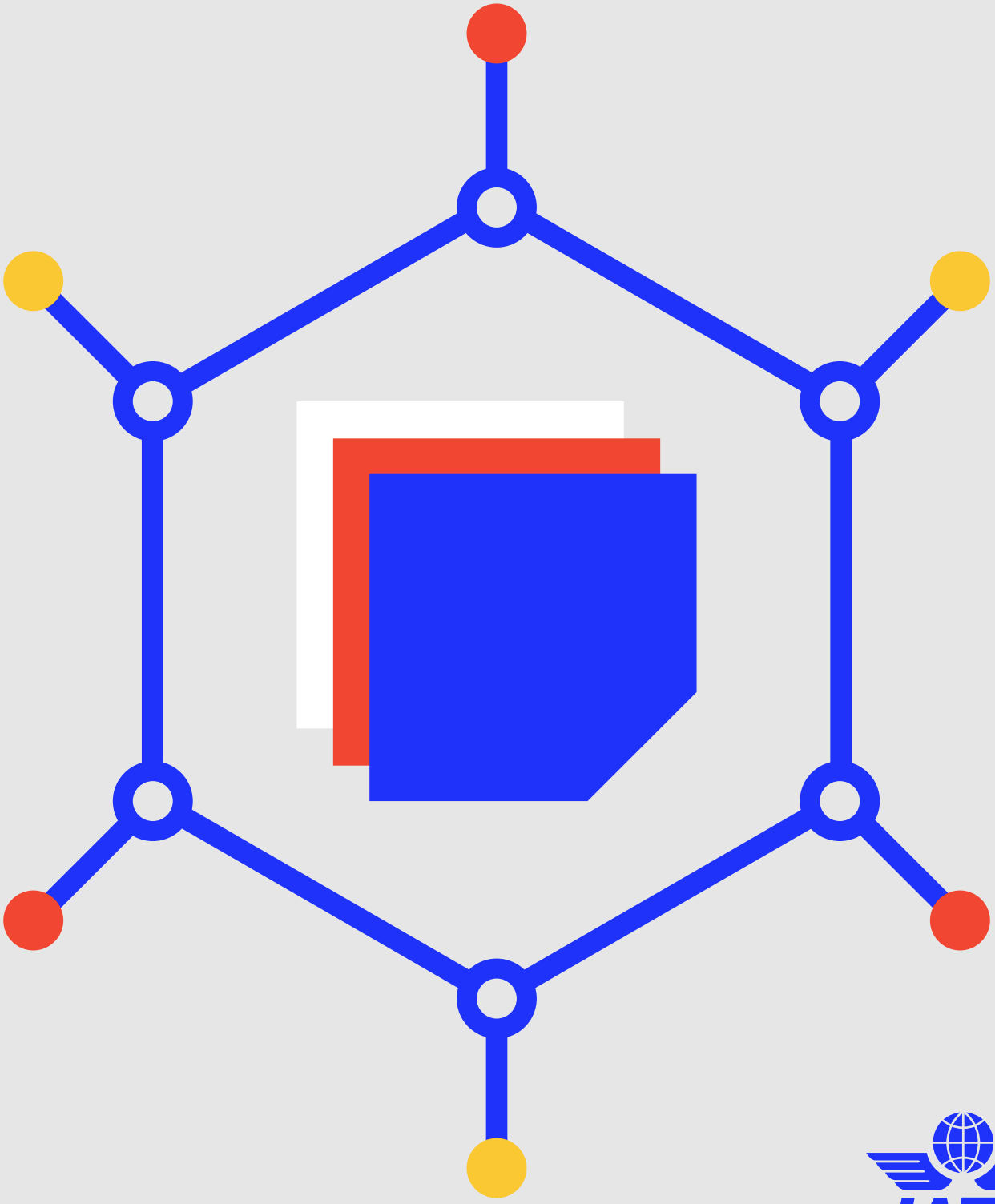
Securing the Digital Future of Air Cargo

Understanding IATA ONE Record Security



Summary

The IATA ONE Record initiative represents a fundamental shift in air cargo data sharing, moving from outdated, siloed systems to a modern, interconnected digital ecosystem. This transformation promises unprecedented efficiency, visibility, and enables the industry to innovate and design process-driven systems. However, sharing data requires robust security and trust. ONE Record incorporates a multi-layered, standards-based security framework designed to protect sensitive information, ensure data integrity, and facilitate secure collaboration across the supply chain. Understanding this framework is crucial for C-level executives evaluating the adoption and strategic benefits of ONE Record.

Ensuring Secure Collaboration in the Digital Air Cargo Supply Chain

Historically, air cargo data exchange relied on point-to-point messages (like EDI) or manual processes, creating information delays, inconsistencies, and security vulnerabilities. ONE Record introduces the concept of a shared, single "record" for each shipment, accessible via modern APIs (Application Programming Interfaces). While this unlocks immense value, it necessitates a security model where participants can confidently share data, knowing it's protected and accessed only by authorized parties.

ONE Record's Security Pillars

The ONE Record security model is built on established internet standards and modern principles, focusing on several key areas:

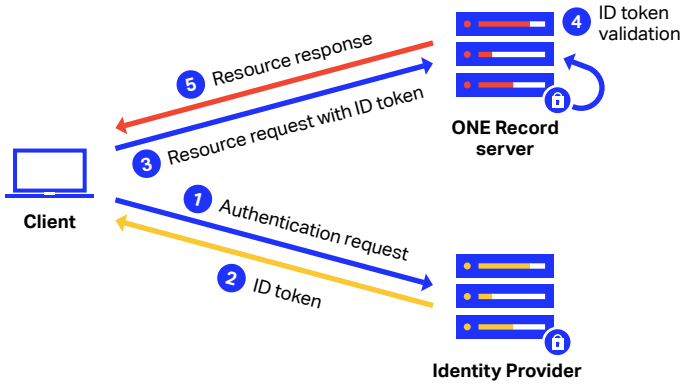
1. **Decentralized Control & Data Sovereignty:** Unlike a single central database, ONE Record promotes a decentralized architecture. Each participant (airline, forwarder, GHA) hosts their own ONE Record server and controls the data they create. They grant specific access permissions to their partners. This means **data owners retain control**, minimizing the risk associated with large, central data repositories.

   Think of it like sharing a document. Instead of putting all your sensitive files on one company-wide drive for everyone to see, you keep your documents on your own computer. When you need to share a specific file, you create a special link or "view" for just that document, granting only the necessary permissions (like "view only"). You remain the owner, deciding exactly who sees what. That's how ONE Record lets each party control their own data and share it precisely

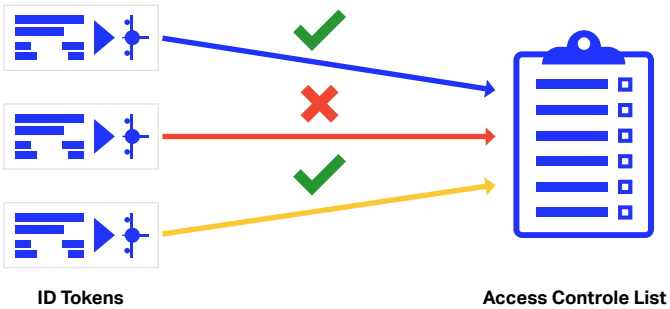
2. **Secure Access Management (Authentication & Authorization):** Knowing who is accessing data and what they are allowed to do is critical. This is handled in two steps:

   – **Authentication:** ONE Record leverages the industry-standard **OIDC (OpenID Connect)** framework for secure server-to-server authentication. This is the same robust technology used by major internet services for secure API access. It ensures that only verified systems can request access, establishing a strong foundation of trust for all data interactions within the ONE Record ecosystem.

   Think of OIDC as the digital passport for each system. Just as a passport verifies your identity when you travel, OIDC verifies that a system is who it claims to be before it's allowed to connect and request data.

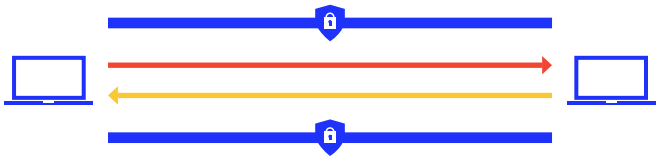


   – **Authorization:** Once authenticated, the data owner's server determines precisely which data objects and actions (read, create, update) the requesting party is permitted. Access is granted based on pre-agreed business relationships and specific data-sharing needs for a given shipment. Delegated access allows partners to interact securely without sharing primary credentials.



   Building on the passport analogy for authentication, think of authorization as your boarding pass. Your passport (OIDC authentication) gets you into the airport (the ONE Record ecosystem). But your boarding pass (authorization) specifies exactly which flight you're allowed on, your seat number, and whether you can access the lounge. Similarly, authorization in ONE Record dictates precisely which data (your "seat" or "flight") a verified system can access and what it can do with it (read, create, update—like checking in baggage or boarding).

3. **Data Protection (Confidentiality & Integrity):** Protecting data as it moves across the internet is paramount.
   - **Confidentiality:** All communication between ONE Record servers must use **HTTPS (TLS encryption)**. This is the standard for secure web traffic (like online banking), ensuring data is encrypted in transit and protected from eavesdropping. Think of HTTPS (TLS) as a sealed, opaque envelope for your digital messages. Even if someone intercepts it, they can't see what is inside.



TLS or mTLS

   - **Integrity:** TLS also helps ensure that data hasn't been tampered with during transmission. The structure of ONE Record, linking data pieces cryptographically, further enhances integrity. Imagine that sealed envelope also has a tamper-evident seal or a unique wax stamp. If the seal is broken or the stamp looks different when it arrives, you know the contents might have been changed along the way.

Business Benefits of ONE Record Security

- **Enhanced Trust:** Builds confidence among supply chain partners for digital collaboration.
- **Improved Data Control:** Companies retain sovereignty over their data assets.
- **Reduced Risk:** Mitigates risks associated with data breaches and unauthorized access compared to less secure or manual methods.
- **Streamlined Compliance:** Standardized security protocols simplify adherence to data protection regulations.
- **Foundation for Innovation:** Secure data sharing enables the development of new value-added services.

Conclusion

IATA ONE Record's security framework is integral to its design, enabling trusted digital collaboration in air cargo. By using clear rules for verifying identity (authentication) and controlling access (authorization), protecting data in transit, and keeping data control decentralized, it provides the necessary control and confidence for businesses to share data effectively and unlock the efficiencies of a truly digital supply chain. For more information, please consult the website ONE-Record documentation.

Frequently Asked Questions (FAQ)

General Information

Q: How is IATA storing industry data in ONE Record?

A: IATA itself DOES NOT store (nor even has access to) the operational industry data (like shipment details, AWB information, etc.) within the ONE Record framework. In the decentralized ONE Record architecture, each participating organization (airlines, freight forwarders, ground handlers, etc.) is responsible for hosting and managing their own ONE Record server and the data they create. IATA's role is to develop, maintain, and promote the ONE Record standard, which defines the data model, API specifications, and security framework that participants use to share data directly with each other, not through a central IATA-managed database of operational data.

Q: Is IATA ONE Record based on blockchain technology?

A: No, IATA ONE Record is not based on blockchain technology. While both concepts involve digital data sharing and security, they operate very differently:

- Data Location & Control: In ONE Record, each company hosts and controls its own data on its own servers. They grant specific access permissions to partners via secure APIs (like giving specific partners access to specific files on your company's secure server).
- Blockchain: Typically involves a single database (ledger) copied and shared across many participants' computers, often requiring complex agreement protocols (consensus) to make changes.
- Data Updates: ONE Record data represents the current state of a shipment and can be updated by authorized partners (it's a live, evolving record). Blockchain records are generally designed to be immutable—very difficult or impossible to change once recorded.

ONE Record uses standard web technologies focused on controlled, efficient data exchange between specific business partners, emphasizing data owner control over access. Blockchain is a different toolset often used for creating shared, tamper-proof historical ledgers.

Data Security & Protection

Q: How can I be sure my commercially sensitive data won't be seen by competitors using ONE Record?

A: You control your data. Access is granted explicitly by your ONE Record server based on your defined permissions for specific, authenticated partners and specific data elements. The robust authorization layer ensures that even authenticated systems can only access what you permit them to access. Competitors will not have access unless you deliberately grant it.

Q: Is ONE Record security better than traditional EDI messages or email?

A: Yes, significantly. ONE Record mandates modern, standardized security protocols (OIDC, HTTPS/TLS) designed for secure internet communication and API interactions. This provides stronger, verifiable system authentication, granular authorization controls, and mandatory encryption in transit, a major upgrade over often less secure methods like emails.

Q: Does ONE Record security cover data security within my own organization's network?

A: No. ONE Record security standards primarily govern the secure exchange of data between different organizations' ONE Record servers over the internet. Security inside your own network (protecting your server, internal access controls, etc.) remains your company's responsibility and should follow established IT security policies.

Q: How is the security implementation audited or verified between partners?

A: The ONE Record standard defines the security requirements. Verification that a partner has implemented these correctly often forms part of the technical onboarding process and bilateral agreements between connecting parties. Industry certifications or audits may emerge in the future, but currently, due diligence during partner integration is typical.

Data Breaches & Authentication

Q: Who is responsible if a data breach occurs within the ONE Record ecosystem?

A: Responsibility generally lies with the entity whose server was compromised or misconfigured. If your server securely manages authentication and authorization according to the standards, you have mitigated your risk. If a partner's system is compromised, the breach is contained to the access you granted them. The decentralized nature limits the blast radius. Robust internal security and proper implementation of ONE Record standards are key.

Q: What happens if the credentials (e.g., Client Secret) used for authentication are compromised?

A: The owner of the server that issued the credentials can revoke them immediately, preventing the compromised credentials from being used to gain access tokens. This highlights the importance of secure credential management practices, including regular rotation and secure storage, for all participants.

Data Sharing & Accessibility

Q: As a Freight Forwarder, when I provide access to an airline, how does the Ground Handling Agent (GHA) gain access to my Air Waybills (AWBs)?

A: As the Freight Forwarder (FF), you are generally the owner and holder of the Logistics Objects, which include your House Waybills (HAWBs) and Master Waybills (MAWBs), as well as associated Shipment and Piece objects. A fundamental principle of ONE Record is that only the Holder of a Logistics Object has full control over access rights. When you, as the Holder, grant access to an Airline, you are delegating specific permissions to them to access (e.g., read) these Logistics Objects. At this stage, typically only you (the FF) and the Airline have access.

If a Ground Handling Agent (GHA) requires access to these same Logistics Objects, the process involves the mechanism of Access Delegation. Since the Airline has received access from you, the Airline MAY request an access delegation for the GHA. This request is made to you, the Freight Forwarder, as you are the Holder of the Logistics Object.

This request results in an **AccessDelegationRequest**, which is a type of Action Request that requires approval. You, as the Holder of the Logistics Object (the Waybill, Shipment, Pieces), decide about the **AccessDelegationRequest** and change the GHA's permissions if you approve it.

The sources highlight the concept of Trust Chains in this scenario. The reason you, the Freight Forwarder (the Delegator in this context), would potentially grant access to the GHA (the Delegate) is based on business partnerships and trust. You would grant the access because you trust the Airline who trusts their ground handler.

In essence, this ensures that organizations can track and review access to their data, a capability that analogue data-sharing methods (i.e.: Cargo IMP) do not provide.

Q: As an airline, when I re-route a shipment from Frankfurt (FRA) to Munich (MUC), how is data authorization granted to the Ground Handling Agent (GHA) in MUC?

A: As an airline, when you re-route a shipment from Frankfurt (FRA) to Munich (MUC), the Ground Handling Agent (GHA) at the new destination in MUC requires digital access to the shipment's information.

You, as the airline, already possess access to this digital shipment data, known as Logistics Objects, which was granted by the party who holds or originally created the data (often the Freight Forwarder for core shipment details, based on conversation history). To enable the MUC GHA to access this data, you initiate an Access Delegation Request within your company's ONE Record system. This formal request asks for access to the relevant Logistics Object(s) to be granted to the specified GHA (an "Organization").

The request is directed to the party who is the data "Holder" of those specific Logistics Objects. The data Holder receives and reviews your Access Delegation Request. If approved, the ONE Record system grants the designated GHA in MUC the necessary Authorization to access the required digital shipment data, allowing them to handle the re-routed cargo efficiently.

These processes can be fully automated within the cargo management system. Once the airline user defines the reroute of a shipment, the system will automatically generate an Access Delegation Request and request the revocation of access for the previous Ground Handling Agent (GHA). Meanwhile, the freight forwarder system can be configured to automatically accept all requests from the designated airline for the specified shipment.

Q: How does Customs receive authorization to access my House Air Waybill (HAWB) or pieces, and how do they retrieve this information once access is granted?

A: The Freight Forwarder is generally the party who controls the digital information for your House Air Waybill (HAWB) and its individual pieces within the ONE Record system. This Freight Forwarder, acting as the data Holder, is the only party who can decide who else gets to see that specific data.

The Freight Forwarder, as the Holder, can directly grant the necessary Authorization to Customs for accessing this data by updating the Access Control Lists (ACLs). Alternatively, another authenticated party, such as the Airline, can request an Access Delegation Request from the Freight Forwarder to ask for Customs to be granted access to the data. It is ultimately the Freight Forwarder, as the Holder, who decides about the Access Delegation Request and grants the permissions by setting the ACLs accordingly.

An Event may be created and linked to the shipment or waybill data to specifically tell Customs that the HAWB or piece data is ready for them to access or has been updated.

After Customs has been granted permission and is logged into the ONE Record system as an approved user, they can retrieve the authorized information. They do this by directly accessing the specific digital records for your HAWB and the associated pieces from the server where the data is hosted.

Authorization & Access Management

Q: How can my organization manage authorization once ONE Record is implemented?

A: After implementing ONE Record specification, it's important to focus on the business rules for authorization. This is crucial because:

- Authorization decisions, including accepting or rejecting Access Delegation Request and Change Request instances, are made by the Holder based on business or technical reasons.
- Analysing industry processes, like the Master Operating Plan (MOP), helps define what ONE Record actions (including accessing/sharing data) are required by whom for each activity. This analysis directly feeds into determining the necessary permissions and access rights for different stakeholders at various points in the process.
- Implementing processes like PLACI relies on events triggering notifications to selected stakeholders. The "chosen setup" for who gets notified automatically is based on pre-defined business rules about access and information flow.
- Sharing planning data, like for pickups, involves the Forwarder managing data access to relevant stakeholders, which requires defining rules for relevance and access.
- The implementation of access control means that each company's ONE Record server MUST deny access by default if permission is not explicitly set. When an operation is attempted without granted permissions, the server MUST return a 403 Forbidden HTTP error. The definition of the business rules determines when permission should be granted, and thus when a 403 is appropriate.
- Implementing authorization requires establishing a mechanism to verify the legitimacy of parties requesting access or updates, particularly in scenarios involving third parties. This mechanism is guided by business rules.

Q: Can access permissions be changed easily if a business relationship changes?

A: Yes. Since each organization controls the authorization rules on its own server, permissions can be updated, modified, or revoked relatively easily through server configuration changes. This allows data access to accurately reflect current commercial agreements and relationships.

Data Retention & Compliance

Q: How long will the data be stored in ONE Record?

A: ONE Record serves as a data-sharing standard, but it does not establish specific data retention guidelines. You can think of ONE Record like an email system—it provides a standardized way to share data, just like email protocols ensure messages can be exchanged between different platforms. However, just as email providers don't dictate how long users must keep their emails, ONE Record doesn't establish specific data retention rules. Instead, each organization using ONE Record must follow the legal and regulatory requirements for data retention in their respective jurisdictions, much like how businesses must comply with email archiving laws based on their industry and location.

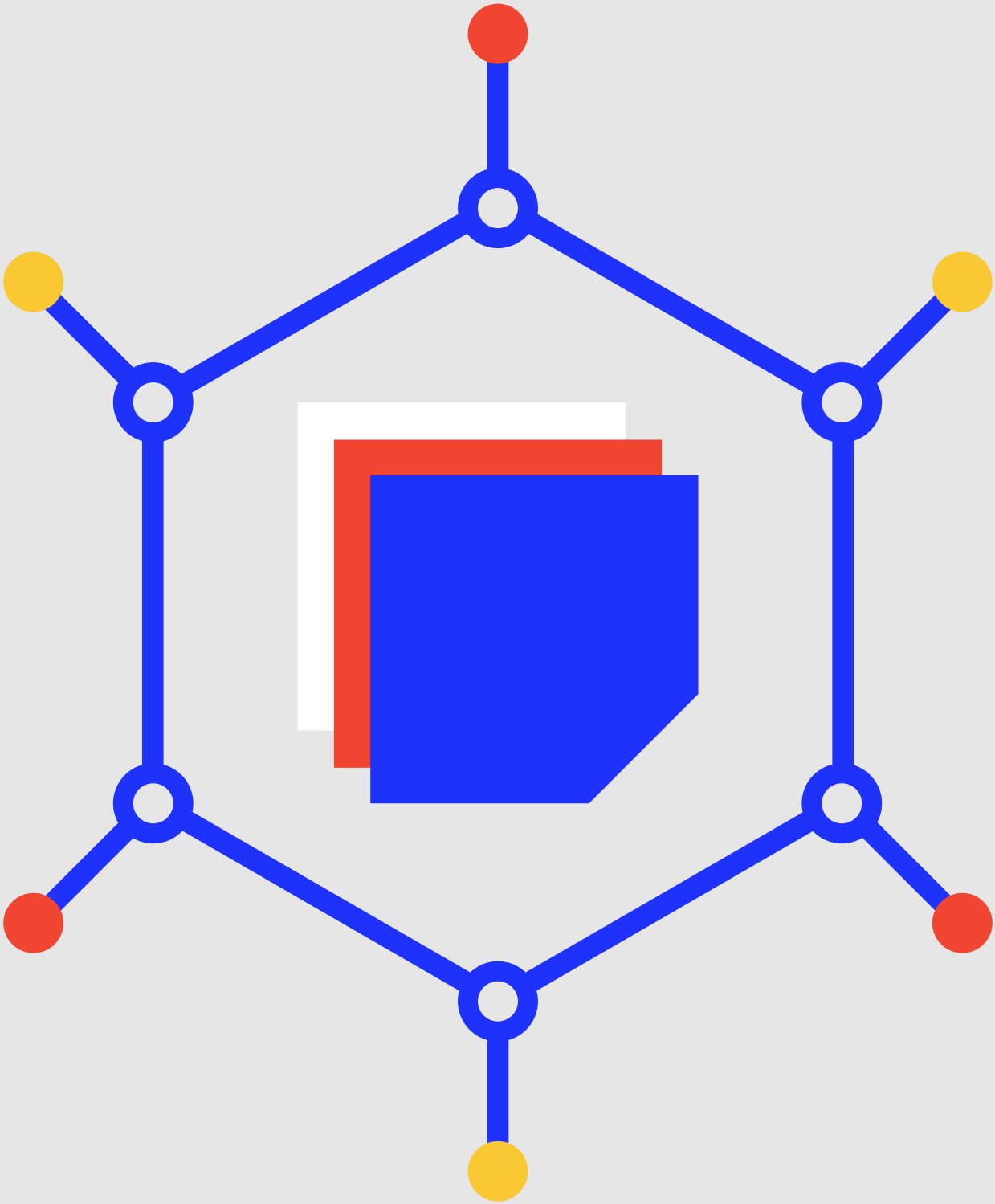
Each organization must ensure its logistics object URLs remain active for a duration set by its business rules and have a mechanism in place to archive them once that period concludes.

Q: What are the best practices for securely deleting data after the retention period has expired?

A: ONE Record does not provide specific guidelines for securely deleting data once the retention period has expired. Organizations that implement ONE Record must adhere to the applicable regulatory frameworks and data retention policies enforced within their respective jurisdictions to ensure compliant data disposal practices.

Q: How should I provide data to governmental authorities upon request?

A: If governmental authorities support ONE Record, you can grant them access and proactively notify them about the availability of logistics objects through the designated notification endpoint. Alternatively, you have the option to extract relevant data from ONE Record and provide it to the authorities in the required predefined format, ensuring compliance with applicable regulations and procedural standards.



International Air Transport Association
800 Place Victoria, PO Box 113
Montreal, Quebec, Canada H4Z 1M1
Tel +1 (514) 874 0202

iata.org