ONE Record Insights

Data Security: Securing the Internet of Logistics

Pedro Fuentes
CSO & Product Manager Trust Services WISeKey

Andra Blaj
Developer, ONE Record IATA

Henk Mulder
Head, Digital Cargo IATA
Your hosts today

Pedro Fuentes
CSO & Product Manager
Trust Services
WISeKey

Andra Blaj
Developer, ONE Record
IATA

Henk Mulder
Head, Digital Cargo
IATA
ONE Record Insights

Episode 1
ONE Record: One step closer to digital cargo
Tuesday, 23rd June 11:00 – 12:30 (CEST)

Episode 2
The data model: a digital twin of the air cargo industry
Tuesday, 30th June 11:00 – 12:30 (CEST)

Episode 3
Crafting ontologies: from physical freight to machine readable data
Tuesday, 7th July 11:00 – 12:30 (CEST)

Episode 4
The ONE Record API: an overview of the key features
Tuesday, 14th July 11:00 – 12:30 (CEST)

Episode 5
Data security: securing the Internet of Logistics
Tuesday, 21st July 11:00 – 12:30 (CEST)

Episode 6
Pilot testing: engaging with the cargo community
Tuesday, 28th July 11:00 – 12:30 (CEST)
ONE Record Insights

Episode 1
ONE Record: One step closer to digital cargo
Tuesday, 23rd June 11:00 – 12:30 (CEST)

Episode 2
The data model: a digital twin of the air cargo industry
Tuesday, 30th June 11:00 – 12:30 (CEST)

Episode 3
Crafting ontologies: from physical freight to machine readable data
Tuesday, 7th July 11:00 – 12:30 (CEST)

Episode 4
The ONE Record API: an overview of the key features
Tuesday, 14th July 11:00 – 12:30 (CEST)

Episode 5
Data security: securing the Internet of Logistics
Tuesday, 21st July 11:00 – 12:30 (CEST)

Episode 6
Pilot testing: engaging with the cargo community
Tuesday, 28th July 11:00 – 12:30 (CEST)
Data Security: securing the Internet of Logistics

Part 1
Why do we need data security?

Part 2
Security overview in ONE Record

Part 3
Deep-dive into the security approach

Part 4
How to be ONE Record security compliant?

Part 5
Demo & next steps

Part 6
Q&A
How to participate during the meeting?

• You can only hear the presenters

• Your microphones are disabled

• Use the questions box to interact

• Simply enter your questions in the chat box on the right
This meeting is recorded for future use

The entire recording along with questions will be available shortly after this webinar finishes.

Simply click on the link in the invite for the live event to access it.

The presentations shown today will be available for download on our website:

www.iata.org/one-record
Part 1

Why do we need data security?
What is the Internet of Logistics?
How does the Internet of Logistics work?

**Internet of Logistics (Iol)** - contains ONE Record Servers and Clients representing all types of stakeholders from the supply chain and it is governed by the ONE Record API and Security specifications.
ONE Record Pillars
The ONE Record concept is based on **3 pillars** enabling to define:

**WHAT, HOW, with WHOM** data can be shared.
The ONE Record concept is based on 3 pillars enabling to define:

WHAT, HOW, with WHOM data can be shared
When exchanging data, each party needs to know with certainty the true identity of the other party and that they have the authority to receive or share the data. They also need to be certain that the data being shared is private, secured and confidential and cannot be intercepted or changed by any unauthorized third party. The ONE Record security framework has to work globally and for all stakeholders in the full logistics and transport supply chain, and in compliance with corporate and local data security requirements.

What is the purpose of the ONE Record data security framework?
Part 2
Security overview in ONE Record
ONE Record Nodes

SINGLE NODE
A node that can receive and transmit data via the ONE Record API. It can act both as a Client & Server or as a Client only. Typically, a Single Node is operated by a single company.

MULTI-COMPANY NODE
A node that may be shared by multiple companies and is operated by a “ONE Record as a Service” service provider. This allows small and medium sized companies to exchange data without the need to implement their own node.

MULTI-USER NODE
A node that is shared by many users, possibly from different companies. Typically, this would be an app server that allows users to interact via a mobile app and retrieve or send data via ONE Record.

MULTI-DEVICE NODE
In addition to multi-company and multi-user nodes, there will be nodes that regroup devices such as trackers and that may connect via ONE Record.
ONE Record Security Architecture

Certificate Authority Compliance
Certificate Profile
Registration procedures
Service Level Agreements

Certificate Authority and Verification Services
Signed ONE Record Certificates
ID accounts + tokens

Identity & Authentication Service Provider

ONE Record Federation Security Agreement

Single Node
User: Password:

Multi-company Node
User: Password:

Multi-user Node
User: Password:

Multi-device Node
User: Password:
**Mutual TLS (HTTPS)**
- Mutual TLS secures the Node-to-Node channels
- Ensures PKI encrypted data channel
- Ensures that only ONE Record recognized servers are used

**Certificate Authorities (CA)**
- Issue and authenticate valid ONE Record certificates
- Must be internationally accredited to issue public certificates
- Meets ONE Record requirements for registration and service levels
- Is federated with other certificate authorities and identity & authentication services
OAuth 2.0 and Open ID Connect
• Framework for identification and authentication
• Open ID Connect facilitates user based accounts
• Ensures identity & authenticity of users, companies and devices
• Ensures identity & authenticity of the IAP that issues the token for data exchanges
• Provides signed & encoded encryption of token (JWT) and payload

Identity & Authentication Providers (IAP)
• Meets ONE Record requirements for registration and service levels
• Is federated with other IAP’s and CAs
• Can register companies, users and devices and provide user accounts
• Must hold a signed certificate issued by a ONE Record Certificate Authority
• Authenticates users and issues token for secured data exchange
WISeKey Test Certificate Authority (CA)

WISeKey is a Certificate Authority service provider

- Build a **portal** where ONE Record pilots can create and download **digital certificates** for their servers
- Provide NodeJS / JAVA / .NET **sample code** for authentication handshake
- Develop **CA policy and registration process** for ONE Record
- Develop **OAuth process** for testing
- In the future, IATA and/or other organizations must implement a **permanent CA**
ONE Record Insights

Part 3

Deep dive into the security approach
Definitions & Acronyms

1R-ID
URI that refers to a 1R service, with the form https://<FQDN>/<COMPANYID>

1R-SERVER
Application that accepts ONE Record API requests from a 1R-CLIENT

1R-CLIENT
Application that sends ONE Record API requests to a 1R-SERVER

TRUSTED CA
Certificate issuer that is approved by IATA

ENDPOINT
Either a 1R-CLIENT or a 1R-SERVER application

END USER
Entity that uses a 1R-CLIENT application

TOKEN
Authorization token, refers to the OAuth2 standard

IAP
Identity & Authentication Provider. Authentication service that implements OAuth2
Use cases & Available tools

In order to authenticate in the Internet of Logistics, **two use cases** were identified:

**MACHINE-TO-MACHINE AUTHENTICATION**

- **Use Case**: TLS Cert in the 1R-CLIENT and 1R-SERVER
- **Tools**:
  - Registration Portal
  - SDK and code samples

**USER-TO-APPLICATION AUTHENTICATION**

- **Use Case**: OAuth tokens to authorize users consuming ONE Record services
- **Tools**:
  - Identity Provider
  - SDK and code samples
Machine-to-Machine Security
Digital Certificates and PKI: Integrated solution to Information Security

Digital Certificates provide a full solution except to manage the Authorization, that requires to apply business logic or a complementary technology.

- **Identify** the entities (persons, applications or objects) connecting to an application, as a stronger authentication solution than username/password.
- **Encrypt** the data, to ensure the confidentiality, either during the communication, or permanently.
- **Digitally sign** the data, to ensure both:
  - the authenticity, and
  - the integrity of the data.
TLS Authentication

TLS Standard defines a **handshake procedure** to **authenticate** the parties and **encrypt** the communication channel.

**Key points to consider:**

- TLS Authentication can be used with certificates only on server side or in both client and server sides.
- The same certificate can allow an application to act as client and as server.
- The same certificate can be used for other purposes, like digitally signing the messages.
- All is standardized and supported out of the box by server applications and development frameworks.
TLS in Client & Server

1. The 1R-Client Initiates the request using HTTPS

2. The 1R-Server presents its certificate, and requests a Client certificate

3. The TLS connection is established if the 1R-Server and 1R-Client are properly configured to require TLS authentication with Client certificate, and the CA issuing the certificate is included in the CA list of the Server

4. The 1R-Client accepts the connection if:
   - The Server certificate comes from a Trusted CA, AND it is not expired/revoked

5. The 1R-Server accepts the connection if:
   - The Client certificate comes from a Trusted CA, AND it is not expired/revoked
   - The Client certificate contains a 1R-ID that is allowed to make ONE Record requests

ONE Record uses a Publish/Subscribe approach:
- The Client sends a request to the Server including a callback URL
- The Server will process asynchronously the request and will send the request to the Client using the callback URL

This means that when the response from the Server is ready, it will be sent to the Client as a new TLS flow, initiated by the Server, but in fact acting as a TLS Client, so using its own 1R-CLIENT certificate.
Client certificate request

The user can request Client certificates for any 1R-ID that has been approved by IATA.

The user can select one or more 1R-ID and this will generate a single certificate that contains multiple SAN containing an URI for each 1R-ID.

The portal will always generate a PFX containing the keys and certificate, protected with a password defined by the user when doing the request.

WISkey

IATA
Server certificate request

The user can request Server certificates for any 1R-ID that has been approved by IATA and that contains a domain that is validated.

The user can select one or more 1R-ID and this will generate a single certificate that contains multiple SAN containing an FQDN for each 1R-ID.

The user selects multiple 1R-IDs:
- https://servername.domain1.com/companyid1
- https://servername.domain1.com/companyid2
- https://servername2.domain1.com/companyid3
- https://servername.domain2.com/companyid4

The portal will generate a TLS Server certificate that contains three SAN:
- SAN1: DNS = servername.domain1.com
- SAN2: DNS = servername2.domain1.com
- SAN3: DNS = servername.domain2.com

The user can only select these 1R-IDs if all are approved by the admin and the user has validated the domains DOMAIN1.COM and DOMAIN2.COM
Account enrolment

The IATA admin creates an account, entering:

- **Entity name**
- **Main email address** (the email acts a username to access the portal)
- **Contact person** name and details (contact name and person, alternate email)

**Account validation**

When the account is created, the user is notified to the main email, receiving an invitation to activate the account and define the password.
1R-ID activation request

The user must register:

• One or more 1R-ID (URI). Examples:
  – https://servername.domain1.com/companyid1
  – https://servername.domain1.com/companyid2
  – https://servername2.domain1.com/companyid3
  – https://servername.domain2.com/companyid4

• For each URI the user must specify if it will be used for client and/or server
## Domain validation process

<table>
<thead>
<tr>
<th>When a new 1R-ID is approved to be used for a server access, before issuing a server certificate it is required that the user demonstrates control on the included domain in the URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a server URI is approved by the admin, the portal will check if the domain was already validated. If not, it will send to the user a random value that needs to be added as a TXT record in the DNS server</td>
</tr>
<tr>
<td>The domain validation must be done on a yearly basis and during that period unlimited certificates with FQDN in that domain can be used</td>
</tr>
<tr>
<td>Only after the portal verifies that the domain is validated, it will be allowed to request server certificates</td>
</tr>
</tbody>
</table>
User-to-Machine Security
Claim-based authentication

How OAuth2 works...
- Once the end user is authenticated, it can get an **Access Token**
- The application servers can take authorization decisions based on the Access Token

What this implies to ONE Record?
- The implementation must be **homogeneous**
- The application servers must be aware of the end user, not only of their organization
Using OAuth2 Tokens

This allows to identify the 1R-Server and 1R-Client, and enables the 1R-Server to take authorization decisions based on the end user.
OAuth Authentication in Multi-IAPs Env

- **Challenge**
  - ONE Record API may have to authenticate OAuth tokens from various IAPs
  - ONE Record API works with trusted IAPs only

- **Solution**
  - Using OpenID Connect IAPs
  - ID Tokens must be signed with Trusted x509 certificates
  - ID Tokens must be verified by ONE Record API to ensure that they come from a Trusted IAP
What is a Trusted IAP?

An IAP is considered a Trusted IAP for ONE Record API if ID Tokens are signed by trusted x509 Certificates issued by IATA Certificate Management System (CMS).
 Calling ONE Record API over OAuth & TLS

• 1R API requires SSL Mutual Authentication
• 1R API requires OAuth Authentication using OpenID Connect Code Flow
• 1R API validates SSL Client Authentication
• 1R API validates ID Token to check if the Token is signed by a Trusted IAP
OAuth – OpenID Connect Code Flow

1. Client (App-X) prepares an Authentication Request containing the desired request parameters.

2. Client sends the request to the Authorization Server (IAP-A).


7. The Server receives a query that contains an ID Token and an Access Token in the response body.

8. The Server validates the ID Token and retrieves the End User's Subject Identifier.
How to be ONE Record security compliant?
PKI Compliance

Certificate characteristics and compliance approach
Certificate profile 1

Client

- Key usage: DIGITAL SIGNATURE
- EXTENDED KEY USAGE: clientAuthentication
- SUBJECT NAME: CN=<COMPANY_ID>
- SUBJECT ALTERNATIVE NAME:
  - URI1=<1R_ID1>
  - URI2=<1R_ID2>
  - URI3=<1R_ID3>

WISeKey recommends using client certificates with only the clientAuthentication EKU, in order to simplify the issuance process and reduce audit complexity.
Certificate profile 2

Server

• Key usage: DIGITAL SIGNATURE, KEY ENCIPHERMENT

• EXTENDED KEY USAGE: serverAuthentication, clientAuthentication

• SUBJECT NAME: **CN=<FQDN1>**

• SUBJECT ALTERNATIVE NAME:
  - DNS1=<FQDN1>
  - DNSn=<FQDNn>

It’s mandatory to have at least one FQDN in a SAN. It’s possible to add several FQDN in a Server Cert, provided that all domains are validated. IMPORTANT: URIs CANNOT appear as SAN in a trusted TLS certificate.

WISeKey recommends using TLS certificates of type “Domain Validated”, that don’t contain company name or other identity attributes, in order to simplify the issuance process and reduce audit complexity.
Requirements for CAs

CERTIFICATE POLICY
IATA provided a Certificate Policy that regulates the details of the certificates used for 1R Clients and Servers.

1R-COMPLIANT
Any CA willing to issue 1R-compliant certificates must adopt this Policy and ensure that the identity validation are performed as expected.

INDEPENDENT AUDIT REPORT
IATA expects the participating CAs to be compliant with the industry standards, and in order to demonstrate it, the CA should present an independent audit report conforming to Webtrust or similar criteria.

TRUST LIST
Once the CA has been approved to participate as ONE Record CA, IATA will include it in a Trust List, which will be used by the applications to determine if a certificate can be trusted.
Trusted IAP
OAuth Auth – Trusted IAP validation

- Find the **iss** claim

  jwt.ms

  |-----|-----------------------------------------------------------------------------|

- Loading **OpenID Connect Configuration**
  

- Load the **IAP’s public key** at
  
OAuth Auth – Trusted IAP validation

Validate if RSA algorithm is being used

Calculate SHA1 Hash of the IAP's public key

Looking up certificate in IATA CMS by Subject Key Identifier (SKI)

If the certificate is found, then the IAP is Trusted.
Demo
Next steps
Implement test code in ONE Record Sandboxes available on GitHub

Get pilots to implement security specifications into their servers

Validate the proposed security architecture

Next steps:
- Validate the WISeKey test CA
- Implement test code on ONE Record sandboxes, both for mutual TLS and OAuth
- Get pilots to generate certificates and implement security on their servers
- Validate mutual TLS architecture
- Validate OAuth approach for platform authentication
Would you like to know more?
ONE Record API & Security specifications

ONf Record API & Security specifications document

Ontology of the API models

JSON-LD examples & Postman collection

The standard is publicly and freely available on GitHub
ONE Record White Papers

Don’t miss our series of three white papers coming this summer!

ONE Record Data Model
ONE Record API
ONE Record Security

https://www.iata.org/one-record/#tab-2
Advance your ONE Record knowledge & skills

Three great events to mark in your calendars

IATA WEBINAR
ONE Record Insights
Series of 6 webinars, every Tuesday from 23 June to 28 July, 11:00 to 12:30 CEST

SPONSORED BY
Riege Software

Hackathon
11-13 September

Digital Cargo Conference 2020
Week of 14-18 Sept.

All digital! All action packed! All Complimentary!

Brought to you by IATA Digital Cargo team
More info: onerecord@iata.org
ONE Record Insights

Save the date

ONE Record Webinar
From June 23 to July 28
Every Tuesday 11:00-12:30

Hackathon
11-13 September

Digital Cargo Conference 2020
Week of 14-18 September
Thank You

More info

www.iata.org/one-record