Carrier Implementation Process
March 2023
Carrier Implementation Process Overview
EES – ETIAS Carrier Implementation Process

Sys2Sys Channel

Step 1:
eu-LISA Rollout to Carriers
- European Commission
- Carriers
- Security Convention
- EU regulations
- Objectives Process

Step 2:
Carriers Registration
- ConnectivityManager
- Connectivity Details
- Service provider ...
- EU regulations
- Objectives Process

Step 3:
Testing
- Pre-Compliance Phase
  - Connectivity Configurations
  - eu-LISA Cloud Simulator
  - eu-LISA System
  - Carriers Service Providers
  - Carrier Test Environment
  - Pre-defined Carriers Test Cases (TDD)
- Compliance Phase
  - Connectivity Configurations
  - eu-LISA Test Environment
  - Carrier Test System connected to eu-LISA Test environment
  - Pre-defined Carriers Test Cases (TDD)

Step 4:
Go live
- eu-LISA
- Go Live
- Carriers
- Carrier Prod configurations
Carriers using the web portal and mobile application channel test their ability to connect and perform the testing of the interface.

When the testing is finalized, carriers need to send to eu-LISA a testing declaration and readiness for the go live and confirm that their staff are trained.

Access to the production is provided to authorised carrier’s staff.
Step 1: Rollout to Carriers

- According to the EES and the ETIAS regulations, carriers will have to query EES and ETIAS and receive answers regarding the status of travellers.

- With the introduction of the EES, which replaces the manual stamping of passports with an electronic record of entries and exits, carriers will verify if a third-country national travelling to the EU with a single or double entry visas has already used the number of entries authorised by their visa.

- Once ETIAS enters into operation, carriers will have to verify, prior to boarding, that their eligible ETIAS passengers have a valid travel authorisation.

Air carriers, sea carriers and international carriers transporting groups overland by coach can now register with eu-LISA using the forms published on eu-LISA Working Group for Carriers web page.
Step 2: Carrier Registration

a. Carriers provide Information for the registration as per the EES and ETIAS regulations

b. Carriers complete the registration forms with authorized contacts to be involved during the implementation, and after the entry into operation. A Carrier Contact is not necessarily a person that is an employee of the same company as the Carrier SPOC. The carrier may have contracted responsibility to another company, e.g. a Service Provider.

c. Each Carrier Contact needs to complete a Security Convention in order to receive a decryption key for encrypting or decrypting documents being shared via secured e-mail communication of authorised contacts during the Manual On boarding.

d. Carriers complete the registration with the channel of choice: Sys2Sys or web portal and mobile application

e. For carriers using the Sys2Sys channel, contacts managing their system could be requested. It may be a Service Provider contact for Carriers that have outsourced the relevant system, or a Carrier contact for carriers that operate an in-house system.
Step 3: Testing
Pre-Compliance phase – Sys2Sys links

Both eu-LISA and the carriers shall provide **communication means and technical details** during the implementation phase using the carrier interface simulator.

The carriers must implement the underlying security protocols as listed below:

- **UN/EDIFACT**: Messages are sent through the **IBM MQ** over an Internet Protocol Security (IPsec) Virtual Private Network (VPN);

- **JSON or XML**: Messages are sent over mutual Transport Layer Security (mTLS) authentication.

To ensure data privacy and integrity between eu-LISA and the carriers, **TLS 1.3** shall be used as the communication standard.
Step 3: Testing
Pre-Compliance phase – Connectivity links and tests

- The carrier or carrier service provider performs tests to ensure that messages are correctly received and processed by the carrier interface simulator according to the connectivity configurations.

- When the connectivity link is validated, the carrier is authorized to proceed with tests according to the Pre-defined Carriers Test Cases (TDD), the Carrier technical Guidelines (CTG) and specific sets of data.

- When the testing is finalized, carriers need to send to eu-LISA a testing declaration and readiness for the compliance phase.
Step 3: Testing
Compliance phase – Sys2Sys links

Both eu-LISA and the carriers shall provide the communication means and technical details during the implementation phase (including IP addresses/URLs to be contacted and certificates).

The carriers must implement the underlying security protocols as listed below:

- **UN/EDIFACT**: Messages are sent through the IBM MQ over an Internet Protocol Security (IPsec) Virtual Private Network (VPN);

- **JSON or XML**: Messages are sent over mutual Transport Layer Security (mTLS) authentication.

To ensure data privacy and integrity between eu-LISA and the carriers, **TLS 1.3** shall be used as the communication standard.
Step 3: Testing
Compliance phase – Connectivity links and testing

- The carrier or carrier service provider performs tests to ensure that messages are correctly received and processed using the eu-LISA test environment.

- When the connectivity link is validated, the carrier is authorized to proceed with further tests according to the Pre-defined Carriers Test Cases (TDD), the Carrier technical Guidelines (CTG).

- Compliance tests are mandatory for each carrier and the eu-LISA support team will verify the acceptance of the Pre-defined Carriers Tests.

- When eu-LISA test manager provides the green light for the pre-defined Carriers tests, then the carrier is authorized to establish the connection to production.
Step 4: Go live

- Both eu-LISA and the carriers shall provide the communication means and technical details for connecting production environments (including IP addresses/URLs to be contacted and certificates). Same as during the compliance phase, the carriers must implement the underlying security protocols as listed below:

  ✓ **UN/EDIFACT**: Messages are sent through the IBM MQ over an Internet Protocol Security (IPsec) Virtual Private Network (VPN);

  ✓ **JSON or XML**: Messages are sent over mutual Transport Layer Security (mTLS) authentication.

To ensure data privacy and integrity between eu-LISA and the carriers, **TLS 1.3** shall be used as the communication standard.
Carrier Certification and Testing Strategy
**Pre-Compliance Phase**

**Sys2Sys**

**Recommendations**

The Pre-Compliance (Pre-CT) phase is not expected for carriers requesting to use only the Web Portal and Mobile Application to check the traveler status.

The Pre-Compliance is the phase in which the carrier can perform free testing using the Carrier Interface Simulator and following Test guidelines as per the Predefined Carrier Test Cases (TDD) document.

Not all carriers requesting a Sys2Sys connection need to perform the Pre-Compliance Tests.

It is recommended that at least one carrier per Service Provider/System performs a testing with the Carrier Interface Simulator using mocked data.
# Compliance Phase

## Sys2Sys

<table>
<thead>
<tr>
<th>Recommendations</th>
<th>The Compliance phase is not expected for carriers requesting to use only the Web Portal and Mobile Application to check the traveler status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All carriers requesting a Sys2Sys connection need to perform the Compliance Tests</td>
</tr>
<tr>
<td></td>
<td>The Compliance (CT) is the phase on which the carrier need to run a set of minimum scenarios to get certified and ready for production</td>
</tr>
<tr>
<td></td>
<td>The environment used for compliance testing is similar to production</td>
</tr>
<tr>
<td></td>
<td>eu-LISA will provide to each registered carrier, testing guidelines and a predefined list of use cases to get a successful result for the certification</td>
</tr>
</tbody>
</table>
Carrier User Roles
Carrier User Roles

Carrier User

SPOC or Backup SPOC role
(Recommended functional mailbox is recommended to be used)

- Manage all the administrative tasks for the registration or deregistration of the carrier
- Main Point of contact for the Technical Impossibility
- Administer the user access and role allocation under the Security Convention
- Authorized from the Carrier SPOC to request assistance
- Authorized from the Carrier SPOC to access the Carrier Interface System as per the authentication schema and the Security Convention

Support assistance role

Authorized system access role

Carrier (Functional mailbox is recommended to be used)
Thank you!

eu-LISA
European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

www.eulisa.europa.eu