Distr.: General
12 August 2021
Original: English

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

Group of Experts on Conceptual and Technical Aspects of Computerization of the TIR Procedure

Second session
Geneva, 25–28 May 2021
Item 6 (d) of the provisional agenda
eTIR conceptual, functional and technical documentation version 4.3: eTIR technical specifications

eTIR technical specifications

Table of contents

I. Mandate 3

II. General introduction 3

A. Purpose 3
B. Scope 3
C. Target audience 4
D. Prerequisites 5
E. Applicable documents 5
F. Definitions 5
G. Abbreviations 7
H. Availability 8

III. The eTIR international system 9

A. Guiding principles 9
B. Overall architecture of the eTIR system 11
C. Detailed architecture of the eTIR international system 16
D. Technical requirements 20
E. Development processes 31

IV. Security of the eTIR system 47

A. Security objectives and principles 47
B. Security requirements 49
C. Security of the eTIR international system 56
D. Security of exchanges with the eTIR international system 59
E. Security of exchanges between other eTIR stakeholders 63

V. Annexes 65

A. Diagram notation 65
B. Technical glossary 65
C. Analysis to determine the needs in terms of capacity and scalability of the eTIR international system 68
D. Error codes 74

List of tables 79

List of Figures 80

I. Mandate

1. The Inland Transport Committee (ITC), at its eighty-second session (23–28 February 2020) approved (ECE/TRANS/294, para. 84[1]) the establishment of the Group of Experts on Conceptual and Technical Aspects of Computerization of the TIR Procedure (WP.30/GE.1) and endorsed its ToR[2] (ECE/TRANS/WP30/2019/9 and ECE/TRANS/WP.30/2019/9/Corr.1), pending approval by the United Nations Economic Commission for Europe (ECE) Executive Committee (EXCOM). EXCOM during its Remote informal meeting of members of the Executive Committee (20 May 2020) approved the establishment of the Group of Experts on Conceptual and Technical Aspects of Computerization of the TIR Procedure (WP.30/GE.1) until 2022, based on the terms of reference included in document ECE/TRANS/WP.30/2019/9 and Corr.1, as contained in document ECE/TRANS/294 (ECE/EX/2020/L.2, para. 5(b)).[3]

2. The terms of reference of the Group stipulate that the Group should focus its work on preparing a new version of the eTIR specifications, pending the formal establishment of the Technical Implementation Body (TIB). More specifically, the Group should (a) prepare a new version of the technical specifications of the eTIR procedure, and amendments thereto, ensuring their alignment with the functional specifications of the eTIR procedure; (b) prepare a new version of the functional specifications of the eTIR procedure, and amendments thereto, ensuring their alignment with the conceptual specifications of the eTIR procedure; (c) prepare amendments to the conceptual specifications of the eTIR procedure, upon requests by WP.30.

3. This document presents the currently available parts of the eTIR technical specifications: a general introduction, the eTIR international system, the security of the eTIR system and a few annexes.

II. General introduction

A. Purpose

4. The purpose of the eTIR technical specifications is to translate the eTIR functional specifications into technical requirements, architectures, guidelines, procedures and detailed descriptions of all messages exchanged between the eTIR international system and the eTIR stakeholders.

5. This document is relevant for all eTIR stakeholders (customs authorities, guarantee chains and holders) which need to interconnect their information systems with the eTIR international system. All aspects of these specifications must be considered as mandatory, unless specified otherwise.

6. The main purpose of this document is twofold: to define the technical aspects of the eTIR international system and to define unambiguously how information is exchanged between the eTIR international system and the eTIR stakeholders.

B. Scope

7. This document is divided in five parts: the present general introduction, the eTIR international system, the communication between eTIR stakeholders and the eTIR

[1] Decision of the Inland Transport Committee para. 84 / ECE/TRANS/294 www.unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294e.pdf

[2] Terms of reference of the newly established Group approved by the Inland Transport Committee and the Executive Committee (EXCOM) of ECE

[3] Decision of EXCOM, ECE/EX/2020/L.2 / para. 5(b) www.unece.org/fileadmin/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/Item_4_ECE_EX_2020_L.2_ITC_Sub_bodies_E.pdf

international system, technical fallback procedures and annexes and appendices. This section defines the scope and content of these parts.

1. The eTIR international system

8. The eTIR international system is the cornerstone of the eTIR procedure as it receives and records information exchanged with customs authorities, guarantee chains and, possibly, holders. The eTIR international system is developed, maintained, hosted and administered under the auspices of ECE.[4]

9. This part starts by defining the three principles that were selected to guide the development activities of the eTIR international system, the rationale for the selection and the implications. It then details the overall architecture of the eTIR system[5] and the detailed architecture of the eTIR international system, including its components and interfaces. It also details the technical requirements of the eTIR international system i.e. several aspects that are not directly linked with its functionality but that are at least as important to ensure that the system functions well. The development procedures including various guidelines and the list of environments and related procedures are also described to explain the methods followed by ECE for the development and maintenance of the eTIR international system. Finally, the last section is dedicated to the technical requirements related to information security and details the security model of the eTIR system.

2. Communication between eTIR stakeholders and the eTIR international system

10. In the eTIR system, information systems of the eTIR stakeholders exchange information with the eTIR international system.

11. This part details the technical requirements of the interfaces between the information systems as well as several aspects that the information systems of the eTIR stakeholders will have to follow. It then describes the web services provided by the eTIR international system and the technical details needed to use them. It elaborates on the architecture and design principles of the implementation of the messages exchanged in the context of the eTIR procedure and provides all technical details. Finally, it explains the interconnection projects that have to be launched by the eTIR stakeholders to connect their information systems with the eTIR international system.

3. Technical fallback procedures

12. This part details the technical aspects of the fallback procedures, already detailed in the eTIR functional specifications, and that have to be followed in case of a problem with one or more components of the eTIR system.

4. Annexes and appendices

13. This final part features the technical glossary and details the notation used for the architecture diagrams. It also presents an analysis to determine the needs in terms of capacity and scalability of the eTIR international system. Finally, it introduces the structure and conventions used for the XSD files and the code lists used in various attributes of the eTIR messages.

C. Target audience

14. This document is prepared for the IT department and IT experts of the eTIR stakeholders that wish to use the eTIR procedure. In particular, this document contains all information needed for the eTIR stakeholders to interconnect their information systems with the eTIR international system.

[4] As per paragraph 1 of Article 11 of Annex 11 of the TIR Convention.

[5] See the definition of the «eTIR system» in section I.F

D. Prerequisites

15. This document should be read after having studied the other documents of the eTIR specifications namely: the introduction, the eTIR concepts and the eTIR functional specifications. In addition, while several key terms and considerations are recalled in this document, a good understanding of the TIR Convention and, in particular, of its Annex 11 is important.

16. It is also assumed that readers have a good understanding of the IT concepts and terminology used in this document, especially related to software engineering. They should also know how web services work and be familiar with SOAP and XML.

E. Applicable documents

17. The following table lists and describes all documents that work in conjunction with the present document to guide the reader on where to find additional information.

Table 1
Applicable documents

Title	*Description*	*Version or date*
The TIR Handbook	This document contains the complete text of the TIR Convention, including its annexes (except Annex 11).	2018
Consolidated eTIR legal framework	Annex I of the report of the seventy-second session of the AC.2 details the adopted changes to the TIR Convention and the text of the new Annex 11 which describes the eTIR procedure.	17 Feb. 2020
Introduction to the eTIR conceptual, functional and technical documentation	This document introduces the conceptual, functional and technical documentation for the eTIR procedure.	4.3a
The eTIR concepts	This document describes the approach and core concepts used to support the business logic, and to implement the eTIR system.	4.3a
The eTIR functional specifications	The purpose of this document is to translate the eTIR concepts into specifications that enable software developers and message designers to further design the eTIR system.	4.3a

F. Definitions

18. The following table provides the definitions of several key terms used in this document.

Table 2
Definition of key terms

Term	*Definition*
Accompanying document	The printed document electronically generated by the customs system, after the acceptance of the declaration, in line with the guidelines contained in the eTIR technical specifications. The accompanying document can be used to record incidents en route and replaces the certified report pursuant to Article 25 of the TIR Convention and for the fallback procedure.
Actor	See “eTIR stakeholder”
Advance amendment data	The data submitted to the competent authorities of the country in which an amendment to the declaration data is requested, in accordance with the eTIR specifications, of the intention of the holder to amend the declaration data.

Term	*Definition*
Advance TIR data	The data submitted to the competent authorities of the country of departure, in accordance with the eTIR specifications, of the intention of the holder to place goods under the eTIR procedure.
Customs office of departure	Any customs office of a contracting party where the TIR transport of a load or part load of goods begins.
Customs office of destination	Any customs office of a contracting party where the TIR transport of a load or part load of goods ends.
Customs office of entry	Any customs office of a contracting party through which a road vehicle, combination of vehicles or container enters this contracting party in the course of a TIR transport.
Customs office of exit	Any customs office of a contracting party through which a road vehicle, combination of vehicles or container leaves this contracting party in the course of a TIR transport.
Customs union	A customs or economic union is composed of two or more member states and form a unique customs territory in the context of the eTIR procedure, provided those member states are contracting party to the TIR Convention and apply Annex 11.
Customs union system	The central information system of the customs union which interconnects the national customs systems of its member states.
Declaration	The act whereby the holder, or his or her representative, indicates, in accordance with the eTIR specifications, the intent to place goods under the eTIR procedure. From the moment of acceptance of the declaration by the competent authorities, based on the advance TIR data or the advance amendment data, and the transfer of the declaration data to the eTIR international system it shall constitute the legal equivalent of an accepted TIR Carnet.
Declaration data	The advance TIR data and the advance amendment data which have been accepted by the competent authorities.
eGuarantee	In the context of the eTIR procedure, the electronic version of the guarantee described in the TIR Convention and represented by a TIR Carnet in the TIR procedure.
eTIR international system	The Information and Communication Technology (ICT) system devised to enable the exchange of electronic information between the actors involved in the eTIR procedure
eTIR procedure	The TIR procedure, implemented by means of electronic exchange of data, providing the functional equivalent of the TIR Carnet. Whereas the provisions of the TIR Convention apply, the specifics of the eTIR procedure are defined in Annex 11.
eTIR service desk	One of the roles of ECE is to assist the eTIR stakeholders to interconnect their information systems to the eTIR international system.
eTIR specifications	The conceptual, functional and technical specifications of the eTIR procedure adopted and amended in accordance with the provisions of Article 5 of Annex 11.
eTIR stakeholder	An entity being part of the eTIR system and using the eTIR procedure as described in the Annex 11 of the TIR Convention. An eTIR stakeholder uses its information systems to be part of the eTIR system and can be any of the following entities: • ECE, with the eTIR international system; • Guarantee chains, with their information systems; • Customs authorities, with their information systems; • Holders, with their information systems.
eTIR system	The set of all eTIR stakeholders, along with their information systems which apply the eTIR procedure as described in Annex 11 of the TIR Convention.

Term	*Definition*
Holder	TIR Carnet holders no longer hold a TIR Carnet in the context of the eTIR procedure, as the goal is precisely to replace the paper TIR Carnet by an electronic guarantee or eGuarantee. However, the term "holder" is retained in the context of the eTIR procedure and represents the same person as described in Article 1, paragraph (o) of the TIR Convention.
National customs system	The central information system of the customs authorities of a contracting party to the TIR Convention. In the context of Annex 11, this system should be connected to the eTIR international system.
Pre-declaration	Data sent by the holder to the appropriate customs office, prior to presenting the road vehicle, combination of vehicles or container. This can be the advance TIR data, the advance amendment data or the cancellation of previously sent advance TIR data or advance amendment data.
Query mechanism	Set of messages that can be used by eTIR stakeholders (I5/I6 for customs authorities and E5/E6 for guarantee chains) to retrieve information stored in the eTIR international system, related to an eGuarantee, its holder and TIR operations.
Technical Implementation Body	The Technical Implementation Body shall monitor the technical and functional aspects of implementing the eTIR procedure, as well as coordinate and foster the exchange of information on matters falling within its competence.

G. Abbreviations

19. The following table describes all abbreviations used in this document. The definition of several of these terms and expressions can be found in the technical glossary, available in the appendices of this document.

Table 3
Abbreviations

Abbreviation	*Description*
AC.2	Administrative Committee for the TIR Convention, 1975
API	Application Programming Interface
BGP	Border Gateway Protocol
CA	Certification Authority
CD	Continuous Deployment
CI	Continuous Integration
CL	Code List
CPU	Central Processing Unit
DBMS	Database Management System
DMR	Data Maintenance Request
DOD	Definition Of Done
ECE	United Nations Economic Commission for Europe
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
GB	Gigabyte
HDD	Hard Disk Drive
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ID	Identifier
IDE	Integrated Development Environment
IT	Information Technology
ITDB	International TIR Data Bank

Abbreviation	*Description*
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
KB	Kilobyte
KMS	Knowledge Management System
MB	Megabyte
MTO	Maximum Tolerable Outage
MTTR	Mean Time To Recovery
OSS	Open Source Software
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PRD	PRoDuction
PRINCE2	PRojects In Controlled Environments 2
RAID	Redundant Array of Independent Disks
SAN	Storage Attached Network
SSD	Solid-State Drive
SIT	System Integration Testing
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SPOF	Single Point Of Failure
TB	Terabyte
TCO	Total Cost of Ownership
TIB	Technical Implementation Body
TIRExB	TIR Executive Committee
TOGAF	The Open Group Architecture Framework
WSDL	Web Service Description Language
UAT	User Acceptance Testing
UI	User Interface
UN	United Nations
UPS	Uninterruptible Power Supply
UTC	Coordinated Universal Time
UTF	Universal Character Set Transformation Format
VCS	Version Control System
WCO	World Customs Organization
XML	eXtensible Markup Language
XSD	XML Schema Definition

H. Availability

20. This document is available from the ECE web site and from the web site[6] devoted to eTIR where the reader can always find the latest versions of all documents related to the eTIR system, including all technical guides used in the context of the interconnection projects.

[6] See www.etir.org/documentation

III. The eTIR international system

21. This part describes all the technical aspects of the eTIR international system, and the necessary information is provided to the reader to understand how this system is implemented, managed, hosted and maintained and how it should behave technically.

22. The level of details depends on the aspects being described and not all technical details may be provided for the following two reasons:

- As this document is publicly accessible, certain technical details are voluntarily not mentioned for security reasons. While ECE acknowledges that security through obscurity[7] should not constitute the only security measure in place, it nonetheless does not wish to divulge too much information that could be used against the security of the eTIR system. Contracting parties wishing to learn more about these additional details can contact the TIR Secretary to organize a study visit of the ECE premises;
- Certain aspects related to the software or hardware products, frameworks or libraries used, as well as implementation facets are subject to regular changes as technology quickly evolves. Flexibility should be given to ECE to be able to freely change these aspects, so that it can address evolving technical requirements (e.g. capacity, scalability, performance) without having to provide an updated version of the technical specifications.

23. Given the fact that several technical details are not mentioned in this document, ECE wishes to remain transparent and demonstrate its professionalism to the contracting parties by detailing its ways of working, its guiding principles and development procedures.

A. Guiding principles

1. Introduction

24. The principles described in this section define the underlying general rules and fundamental values that will guide decision-making activities on the technical aspects of the eTIR international system (e.g. development, hosting, management, maintenance, etc.). The approach to define these three principles is based on the method for expressing architecture principles as detailed in the TOGAF Standard.[8]

2. Principle 1: Information security

(a) Statement

25. Information stored in the eTIR international system is considered confidential and shall be accessible at all times by authorized stakeholders only, by means of eTIR messages that shall be authenticated and secured.

(b) Rationale

26. Articles 7 and 8 of Annex 11 of the TIR Convention set up requirements for authentication and integrity of data.

27. Articles 11 and 12 of Annex 11 of the TIR Convention set up requirements regarding the availability and integrity of data.

(c) Implications

28. The confidentiality, integrity, availability and non-repudiation of information exchanged (data in transit) between the eTIR international system and eTIR stakeholders, and recorded on the eTIR international system (data at rest) should be ensured.

[7] See www.etir.org/documentation

[8] See the TOGAF ® Standard v9.2 : pubs.opengroup.org/architecture/togaf9-doc/arch/chap20.html

29. Information exchanged and recorded in the eTIR international system is classified as confidential information as per the dispositions of the Secretary-General's bulletin titled "Information sensitivity, classification and handling"[9] and the relevant policies and measures apply.

3. Principle 2: High reliability and quality

(a) Statement

30. The eTIR international system shall be developed and maintained following high standards in terms of reliability and quality, and these standards shall be continuously reviewed and improved.

(b) Rationale

31. A high reliability minimizes the costs to develop, operate and maintain the eTIR international system.

32. A high reliability minimizes the resources required by eTIR stakeholders to develop, operate and maintain the interconnection between their information systems and the eTIR international system.

(c) Implications

33. Proven best practices from the information technology industry should be adopted for the development, operation and maintenance of the eTIR international system.

34. Emerging trends from the information technology industry should be regularly assessed to find ways to continuously improve the development, operation and maintenance of the eTIR international system.

4. Principle 3: Ease of connectivity for the eTIR stakeholders

(a) Statement

35. The eTIR international system shall be designed and documented to facilitate the interconnection of eTIR stakeholders, including the upgrade to new versions.

(b) Rationale

36. Ease of connectivity minimizes the resources required by eTIR stakeholders to develop, operate and maintain the interconnection between their information systems and the eTIR international system.

37. Ease of connectivity minimizes the costs on the eTIR service desk to assist contracting parties in interconnecting their national customs systems to the eTIR international system.

(c) Implications

38. The eTIR international system, its interfaces and documentation should use, to the extent possible, worldwide renowned standards.

39. The necessary documentation should be produced, in addition to the eTIR specifications, to guide and accompany the eTIR stakeholders in their interconnection projects.

40. Thanks to the experience acquired and the feedback received while assisting eTIR stakeholders with their interconnection projects, additional enhancements should be included to continuously improve the documentation and assistance provided by the eTIR service desk.

[9] See undocs.org/st/sgb/2007/6

B. Overall architecture of the eTIR system

1. Introduction

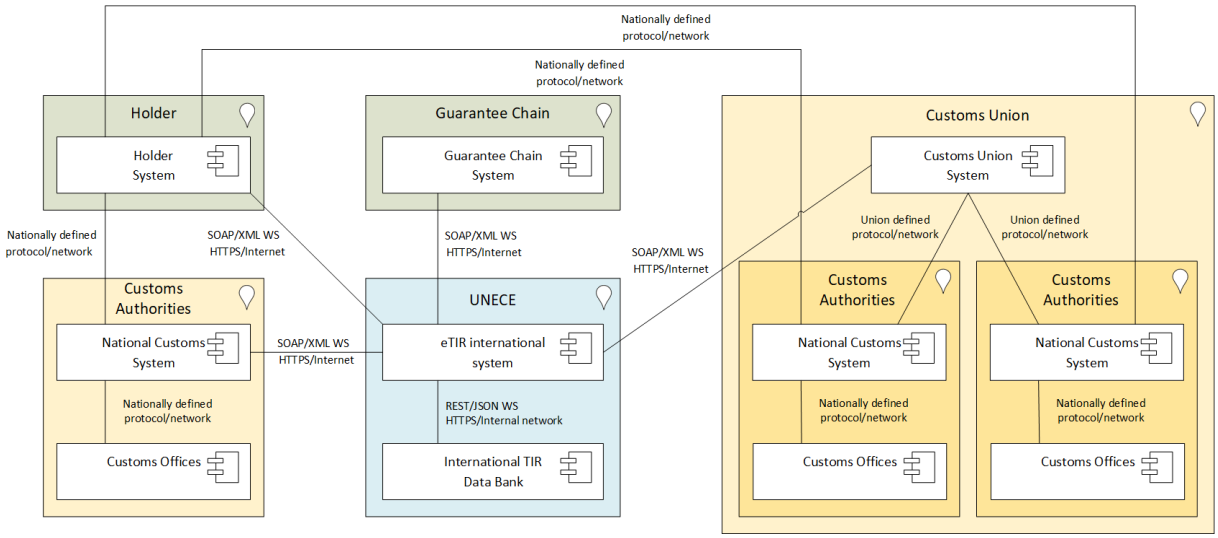
41. This section presents the overall technical architecture of the eTIR system and, in particular, the interactions between the information systems of the different actors of the eTIR procedure. It also provides a more detailed view of each actor's information systems, including the interfaces and the messages exchanged.

42. The diagrams in this section follow the ArchiMate[10] notations that are described in annex IV.A of the present document.

2. Overview

43. The eTIR system is composed of the interconnection of the information systems of the various actors involved in the eTIR procedure: customs authorities, holders, guarantee chains and ECE. The overall technical architecture presented in the figure below shows the interconnection between the information systems of all actors, including the case of customs unions. The latter could take advantage of information systems and interconnections already set up in the framework of the customs union.[11]

Figure I
Overall technical architecture of the eTIR system



44. The following sections provide more details of the information systems of each actor, in particular its interfaces and the messages exchanged. In order to avoid repetitions, the interfaces between two information systems are only detailed in the section devoted to the actor that initiates most of the transactions.

3. Customs authorities

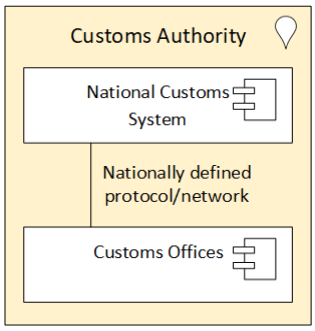
45. Customs authorities use information systems to manage customs procedures, such as import, export and transit. The design and architecture of these information systems is the sole decision of each and every customs authority and can therefore greatly vary from one contracting party to another. It is assumed that all customs offices are connected with the central information system of the customs authorities, hereafter called: the national customs system.

46. In order to properly implement the provisions of Annex 11 of the TIR Convention and adapt their information systems to the eTIR procedure, customs authorities must connect their national customs system to the eTIR international system. In the context of the eTIR procedure, the main actors on the side of customs authorities are customs officers (located in

[10] ArchiMate® 3.0.1 Specification. See: pubs.opengroup.org/architecture/archimate3-doc/
[11] As proposed in Explanatory Note to article 3, paragraph 2 of Annex 11 of the TIR Convention

customs offices) who process TIR transports. While it is necessary that all customs offices approved to carry out TIR transports under the eTIR procedure are connected to the national customs system, the way in which these connections are established is defined by each customs authority. Similarly, the user interfaces used by customs officers to handle the eTIR procedure are designed and implemented by each customs authority.

Figure II
Interactions between the national customs system and the customs offices



47. The customs officers, via their national customs system, exchange information with the eTIR international system using the following messages which allow to:

- accept the guarantee assigned to a TIR transport using the request message "I1 – Accept Guarantee" and its response "I2 – Acceptance Results";
- query all information related to an existing guarantee using the request message "I5 – Query Guarantee" and its response "I6 – Query Results";
- record the declaration data of a TIR transport using the request message "I7 – Record Declaration Data" and its response "I8 – Record Declaration Data Results";
- start a TIR operation for the TIR transport using the request message "I9 – Start TIR Operation" and its response "I10 – Start Results";
- terminate the TIR operation for the TIR transport using the request message "I11 – Terminate TIR Operation" and its response "I12 – Termination Results";
- discharge the TIR operation for the TIR transport using the request message "I13 – Discharge TIR operation" and its response "I14 – Discharge Results";
- refuse to start a TIR operation for the TIR transport using the request message "I17 – Refuse to Start TIR Operation" and its response "I18 – Refusal to Start Results".

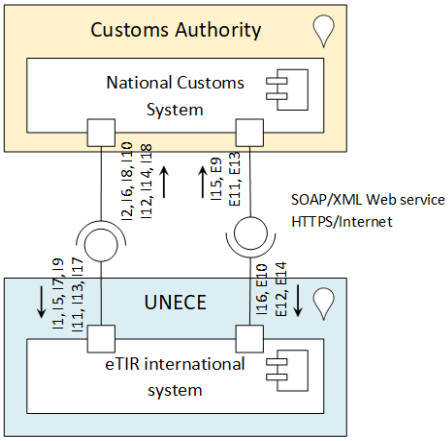
48. In addition, the eTIR international system can notify the national customs system, on specific events related to a TIR transport, using the request message "I15 – Notify Customs" and its response "I16 – Notification Confirmation".

49. Finally, the eTIR international system can forward information from the holder related to the advance TIR data and the advance amendment data[12] to the relevant customs authorities using the following messages which allow to:

- receive the advance TIR data sent by the holder via the eTIR international system using the request message "E9 – Advance TIR Data" and its response "E10 – Advance TIR Data Results";
- receive the advance amendment data sent by the holder via the eTIR international system using the request message "E11 – Advance Amendment Data" and its response "E12 – Advance Amendment Data Results";
- receive the cancellation of a previously sent advance TIR data or advance amendment data using the request message "E13 – Cancel Advance Data" and its response "E14 – Cancel Advance Data Results".

[12] As per paragraphs 2 and 3 of article 6 of Annex 11 of the TIR Convention.

Figure III
Interactions between the national customs system and the eTIR international system



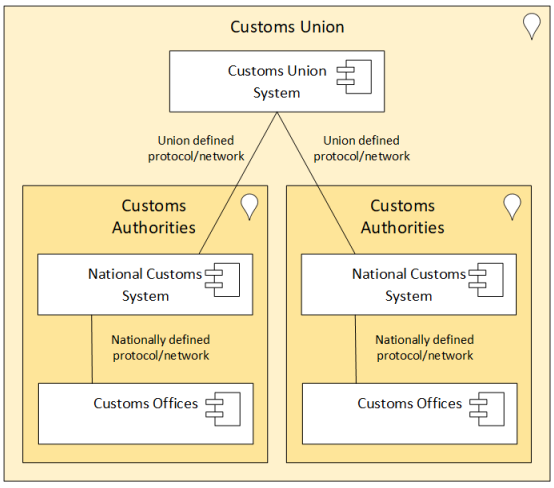
50. These messages (I1, I2, I5, I6, I7, I8, I9, I10, I11, I12, I13, I14, I15, I16, I17, I18, E9, E10, E11, E12, E13 and E14) are transmitted via HTTPS over the Internet using SOAP web services and the data transferred is formatted in XML.

4. Customs unions

51. Customs unions may have put in place an overarching customs union system to facilitate the exchanges of information between the national customs systems of their member states. The design and architecture of these overarching customs union systems is the sole decision of the customs unions so they can vary from one customs union to another.

52. In order to properly implement the provisions of Annex 11 of the TIR Convention and to adapt their information systems to the eTIR procedure, member states of a customs union may wish to interconnect their national customs systems to the eTIR international system via the customs union system. In such case, the customs union system would then dispatch the messages to the appropriate recipients and, possibly, also act as a converter if the messages exchanged between the customs union system and the national customs system do not follow the eTIR specifications.

Figure IV
Interactions between the customs union system and the national customs systems



53. For the rest of this document, we will consider that the interface between the eTIR international system and a customs union system is the same as between the eTIR international system and a national customs system, unless otherwise specified.

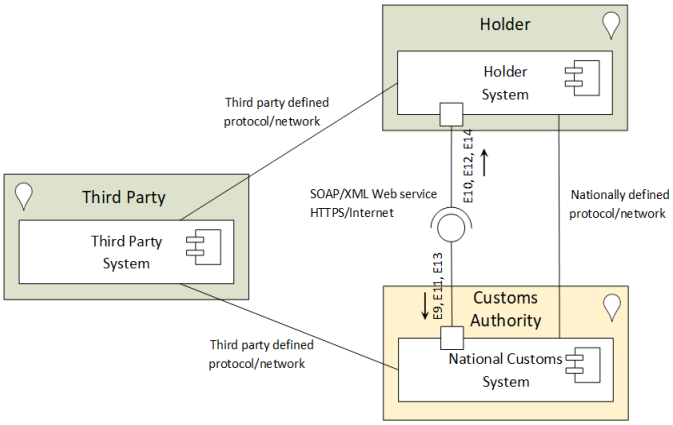
5. Holders

54. Holders have the responsibility to submit to the customs office of departure the advance TIR data of the TIR transport they wish to initiate. The holder can always cancel

previously sent advance TIR data and they can resubmit new advance TIR data. Once the declaration has been accepted by the customs office of departure, the holder can send an "advance amendment data" to the next customs office of entry or departure to request the declaration to be amended. The holder can then cancel a previously sent advance amendment data, as long as it has not yet been accepted by customs.

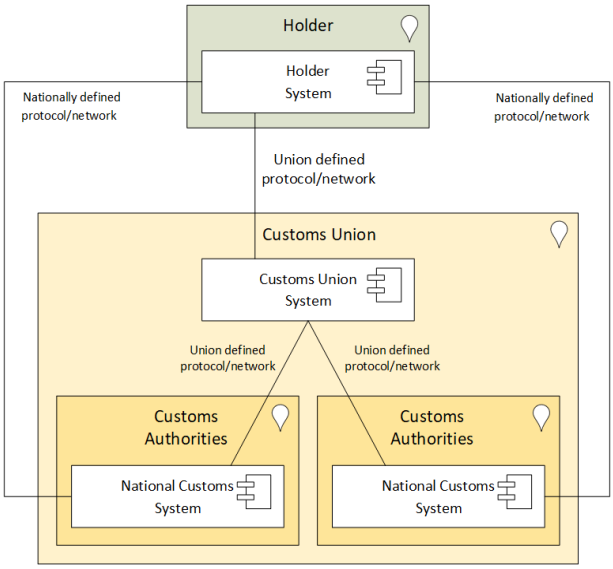
55. Submitting this information to the customs authorities can be done using several electronic means: from a web portal managed by the customs authorities, using web services following the eTIR specifications, from a web portal managed by a third party, etc. Each and every customs authority shall publish a complete list of the ways of submitting this information.[13] All these electronic means shall submit the information needed in the respective eTIR messages: E9, E11 and E13.

Figure V
Possible interactions between the holder system and the national customs system



56. In the case of customs unions, the same approaches exist for holders to submit pre-declaration information to the relevant customs authorities of the member states that compose this customs union. In addition to the means already detailed in the previous paragraph, an additional portal provided at the customs union level might also be available.

Figure VI
Interactions between the holder system and the systems of a customs union

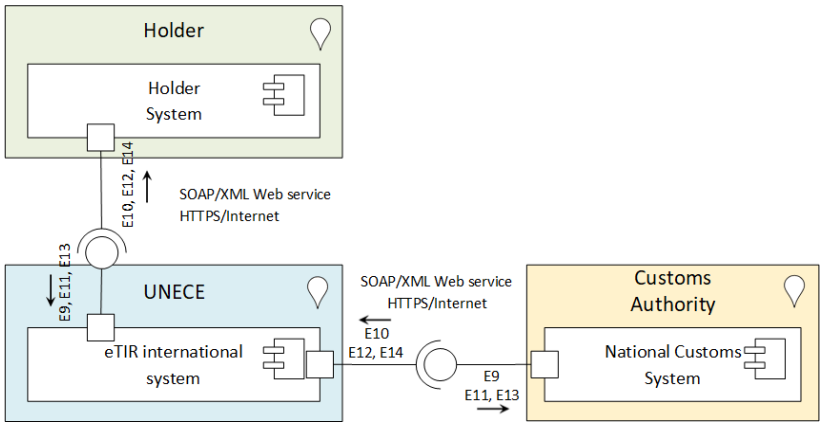


57. Finally, holders always have the possibility to submit pre-declaration information to the appropriate customs offices via the eTIR international system[14] using the following messages which allow to:

[13] As per paragraph 4 of Article 6 of Annex 11 of the TIR Convention.
[14] As per paragraphs 2 and 3 of Article 6 of Annex 11 of the TIR Convention.

- send the advance TIR data to the customs office of departure via the eTIR international system using the request message “E9 – Advance TIR Data” and its response “E10 – Advance TIR Data Results”;
- send the advance amendment data to the appropriate customs office via the eTIR international system using the request message “E11 – Advance Amendment Data” and its response “E12 – Advance Amendment Data Results”;
- send the cancellation of a previously sent advance TIR data or advance amendment data to the appropriate customs office via the eTIR international system using the request message “E13 – Cancel Advance Data” and its response “E14 – Cancel Advance Data Results”.

Figure VII
Interactions between the holder system and the national customs system via the eTIR international system



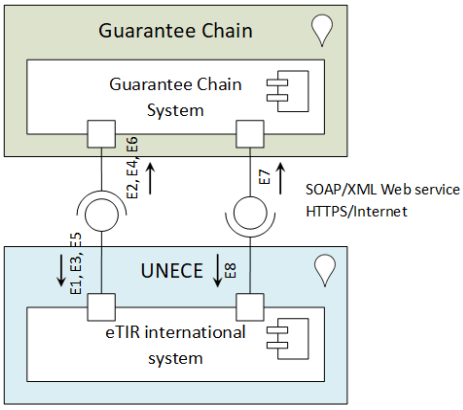
58. These messages (E9, E10, E11, E12, E13 and E14) are transmitted via HTTPS over the internet using SOAP web services and the data transferred is formatted in XML.

6. Guarantee chains

59. Guarantee chains manage the information systems used for the management of electronic guarantees (or eGuarantees) and the exchange of the required data with the eTIR international system using the following messages:

- register a new guarantee using the request message “E1 – Register Guarantee” and its response “E2 – Registration Results”;
- cancel an existing guarantee using the request message “E3 – Cancel Guarantee” and its response “E4 – Cancellation Results”;
- query all information related to an existing guarantee using the request message “E5 – Query Guarantee” and its response “E6 – Query Results”;
- be notified by the eTIR international system on specific events related to an existing guarantee using the request message “E7 – Notify Guarantee Chain” and its response “E8 – Notification Confirmation”.

Figure VIII
Interactions between the guarantee chain system and the eTIR international system



60. These messages (E1, E2, E3, E4, E5, E6, E7 and E8) are transmitted via HTTPS over the internet using SOAP web services and the data transferred is formatted in XML.

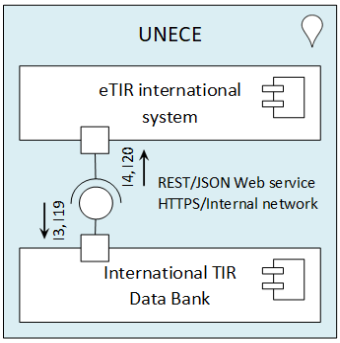
7. United Nations Economic Commission for Europe

61. ECE manages two information systems: the eTIR international system and the International TIR Data Bank (ITDB). The eTIR international system is the cornerstone of the eTIR system and its main role is to receive, validate, record and send data exchanged between the various actors during TIR transports following the eTIR procedure. The ITDB is an information system developed under the purview of TIRExB and its main roles, in the context of the eTIR system, are to manage the list of approved TIR Carnet holders and the list of approved customs offices for accomplishing TIR operations.

62. In the context of processing information received in eTIR messages, the eTIR international system queries the ITDB (when applicable) to:

- verify the authorization of the holder using the request message "I3 – Get Holder Information" and its response "I4 – Holder Information";
- verify the existence of the customs offices using the request message "I19 – Check Customs Offices" and its response "I20 – Customs Offices Validation".

Figure IX
Interactions between the eTIR international system and the ITDB



63. These messages (I3, I4, I19 and I20) are transmitted via HTTPS over the secured network of the data centre hosting both information systems, using RESTful web services and the data transferred is formatted in JSON.

C. Detailed architecture of the eTIR international system

1. Introduction

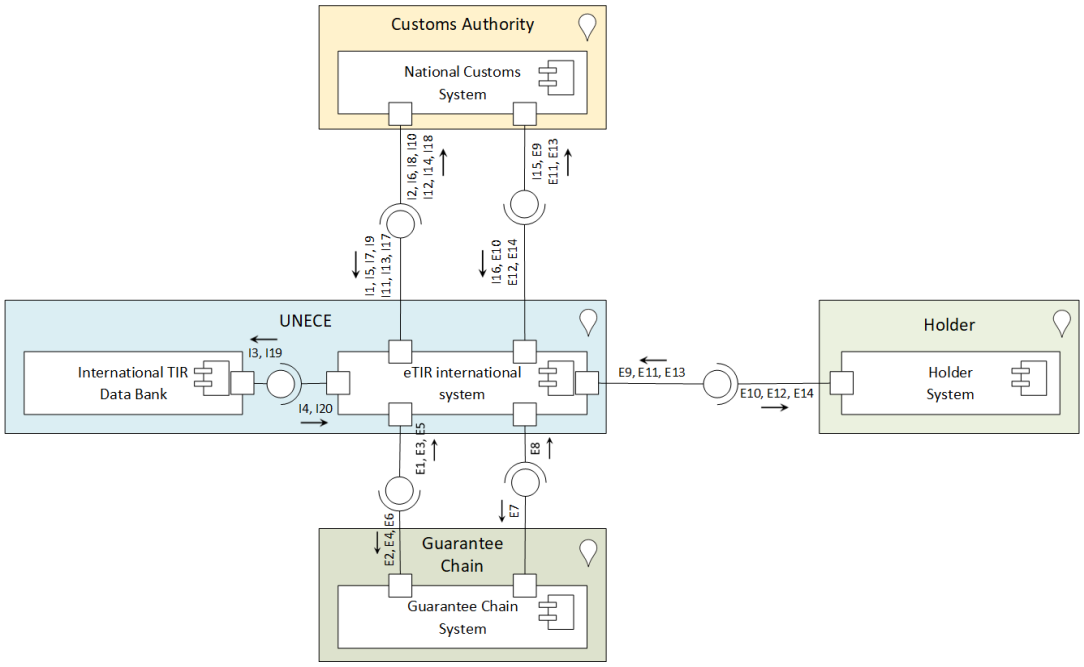
64. This section describes the software and hardware aspects of the architecture of the eTIR international system. In order to remain technology agnostic, this section does not provide information on products, frameworks or libraries used to implement the functions

needed by the components. Indeed, as technology quickly evolves, ECE will continuously monitor the available options and perform changes as it sees fit so that the components of the eTIR international system can continue to perform their functions and properly scale over time to match the capacity and performance requirements (see the next section on technical requirements).

2. Interfaces with eTIR stakeholders

65. The interfaces between the eTIR international system and other eTIR stakeholders are already detailed in the previous section. The following figure summarizes them all, by mentioning the message codes and the flow of information.

Figure X
Interfaces of the eTIR international system



3. Storage locations

66. Messages are processed by the eTIR international system and parts of them are recorded in three different storage locations:

- All incoming and outgoing messages are entirely recorded in the **eTIR logs** to save the data needed to ensure non-repudiation and to provide the information that may be requested by contracting parties;
- Data extracted from the messages is recorded in the **eTIR database** to be used by the query mechanism and for statistical purposes;
- If “attached documents” and “certificates of approval” are embedded into messages (which can be the case in E6, E9, I6, I7 and I15), they are extracted and saved as files in the **eTIR documents**, a separate centralized and secured file system.

4. Software architecture

67. The eTIR international system relies on the following software components:

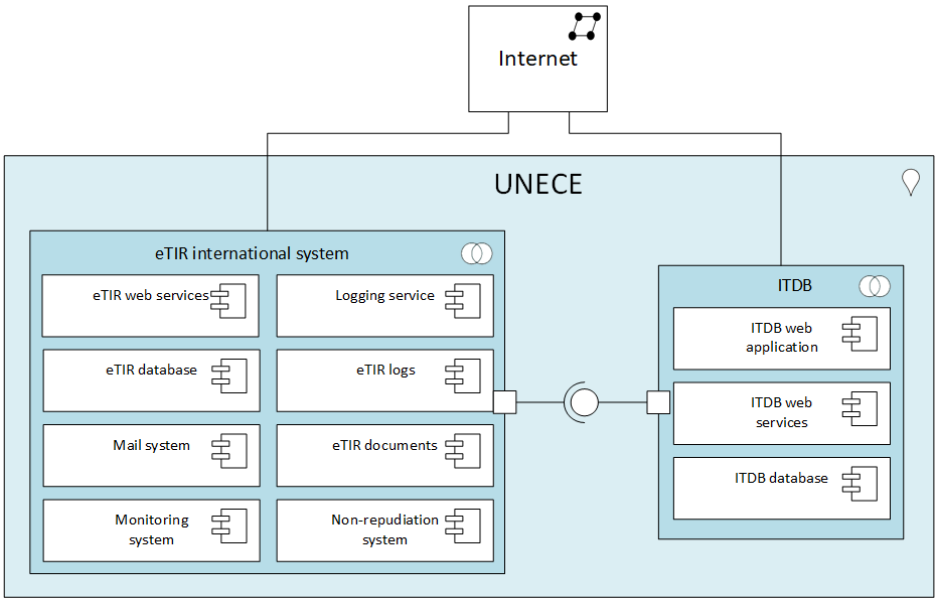
- The **eTIR web services** are the core of the eTIR international system where messages are received, validated, processed, recorded and sent;
- The **logging service** is used to record all messages sent and received by the eTIR international system, as well as all information logged by its other software components, frameworks and libraries.

68. The eTIR international system also relies on the following systems:

- The **mail system** is used to send email messages to eTIR stakeholders on specific occasions, principally during fallback procedures;
- The **monitoring system** is used to observe the resources and performance of the virtual servers, as well as the availability and performance of the services of the eTIR international system;
- The **non-repudiation system** will extract data stored in the eTIR logs, index them and feature a user interface only accessible by IT administrators from ECE. This user interface will allow querying the logs to find a particular message (using the unique "Message Identifier"), a pair of request/response messages, and to provide all information needed by contracting parties for verification purposes.[15]

69. The following diagram presents the software architecture of the eTIR international system. The interfaces exposed and consumed by the eTIR international system are not represented, as they are already listed and described in the sections above.

Figure XI
Software architecture of the eTIR international system



70. The technical requirements of the software components of the eTIR international system are listed in the following section. The software components of the ITDB are listed for informational purposes as they are managed by ECE, under the purview of the TIRExB.

5. Systems architecture

71. The United Nations entity that hosts the eTIR international system (hereafter the hosting entity) has its own private data centre which is located in a United Nations compound and thus benefits from the privileges and immunities enshrined in the United Nations Charter[16] and further detailed in the Convention on the privileges and immunities of the United Nations.[17]

72. The hosting entity uses a virtual server farm to provide virtual servers that form the various systems components of the eTIR international system and at the moment, each node corresponds to a virtual server. In a near future, ECE will consider using containers and container orchestration techniques to further ensure the scalability requirements of the eTIR international system while keeping the hosting costs to an acceptable level.

73. The eTIR international system is designed and implemented in a way that limits single points of failure (SPOF) to meet its availability objectives (as detailed in the next section).

[15] As per paragraph 3 of article 12 of Annex 11 of the TIR Convention.
[16] See www.un.org/en/charter-united-nations/
[17] See treaties.un.org/doc/Treaties/1946/12/19461214%2010-17%20PM/Ch_III_1p.pdf

This architecture also allows to intervene in systems components without having to stop the eTIR international system. This is particularly important to perform regular maintenance activities like replacing defective hardware parts, updating software components and applying security patches.

74. The eTIR international system relies on the following systems components (their technical requirements are listed in the next section):

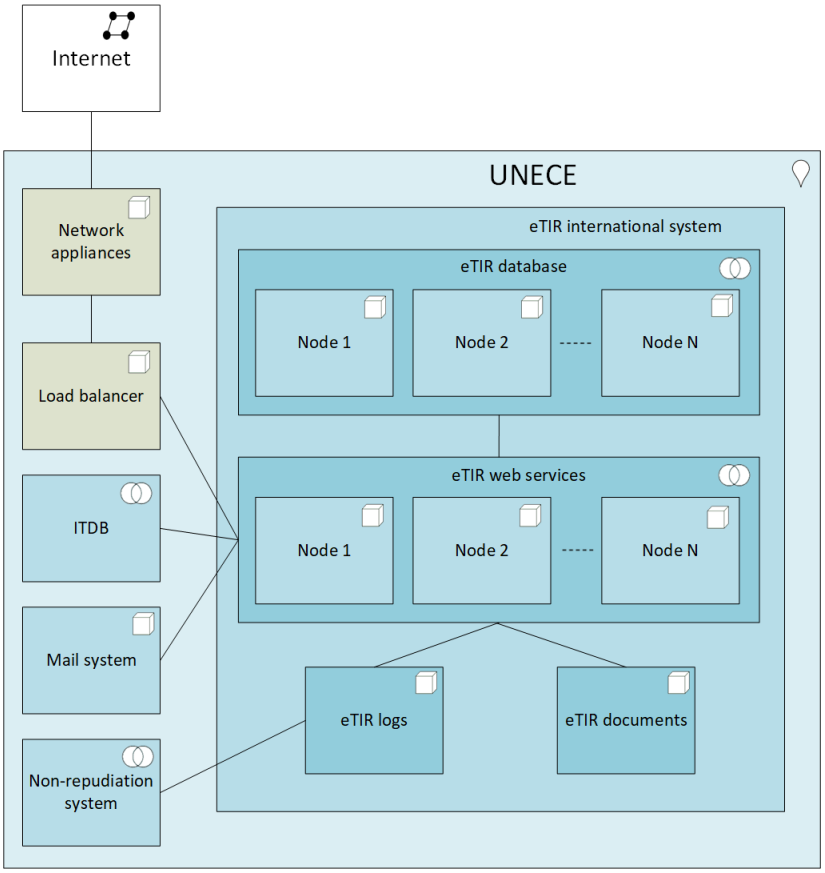
- The **eTIR web services** are the core of the eTIR international system where messages are received, validated, processed, recorded and sent. It consists of several front-end web server nodes to which messages are distributed by the load balancer;
- The **eTIR database** is the core storage location and consists of a clustered database management system (DBMS) using several virtual server nodes and high-performance disk storage;
- The **eTIR logs** is the storage location to which logs are transferred on a daily basis and consists of a virtual server with enough disk space to store all logging information;
- The **eTIR documents** is the storage location to which attached documents are saved and consists of a virtual server with enough disk space to store all documents.

75. The eTIR international system also relies on the following external systems components:

- The **ITDB** which has its own systems architecture to meet its availability objectives. In case of unavailability of the ITDB, the eTIR international system follows a failover procedure which is described later in the document;
- The **mail system** is provided by the hosting entity and consists of a virtual server only used for sending email messages. The eTIR international system principally uses this external system in case of fallback procedures;
- The **non-repudiation system** is an external administration system which is not directly needed for the proper functioning of the eTIR international system and thus consists of a unique virtual server.

76. The following diagram presents the systems architecture of the eTIR international system.

Figure XII
Systems architecture of the eTIR international system



77. With the following sample scenario, we wish to illustrate the usual exchange of information between systems components. An incoming message sent from an eTIR stakeholder over the internet first gets to the network appliances (BGP router and firewall) of the hosting entity. The message is then transferred to the load balancer system which forwards it to the appropriate node of the eTIR web services (front end web server) which validates and processes the message. This web server then stores relevant data in the eTIR database, in the eTIR logs and, if applicable, in the eTIR documents. Finally, the same web server prepares the response message and sends it back to the eTIR stakeholder who initially sent the request message. For the sake of clarity, additional systems related to network routing and security are not shown in this diagram (routers, switches, firewalls, IDS, IPS, etc.).

D. Technical requirements

1. Introduction

78. This section describes the technical requirements – or non-functional requirements – which must be met by the eTIR international system. Technical requirements specify criteria that can be used to judge how well a system performs its operations and fulfils its mission. These criteria are as important as functional requirements and will drive the architecture and design principles of the system.

79. Each following sub-section describes the requirements of a particular non-functional criterion. These requirements can be qualitative (e.g. the source code must be versioned on Git) and/or quantitative (e.g. the eTIR international system must be available 24 hours per day and 365 days per year). All requirements are given a unique identifier for ease of reference.

80. Quantitative requirements need metrics to be collected to be able to assess whether these requirements are met. Provided these metrics can be revealed without posing a security issue, they may be communicated on a periodic basis to TIB for its information.

81. Given the fact that the eTIR system is based on an exchange of messages using web services and that no user interface is expected to be developed for the eTIR international system (except for internal purposes related to its administration), the following criteria are therefore not applicable and will not be described: accessibility, compatibility and usability.

82. Several quantitative targets will be periodically assessed by ECE and reported to TIB, along with proposals to correct potential deficiencies and further increase the targets. TIB shall then decide whether to apply these proposals or recommend their application to AC.2.

83. Finally, when products, software, frameworks and libraries used to fulfil the requirements, are mentioned, ECE reserves the right to modify its selection later on, as long as there are no costs implications, in order to accrue additional benefits for the eTIR system. The information about these new selections would be communicated to TIB and the next version of the eTIR specifications would be updated accordingly.

2. Availability

84. The availability of the eTIR international system represents the state when it is fully accessible and operable by its authorized users (ECE and all eTIR stakeholders connected to it).

85. The availability of the eTIR international system will be critically important for the proper functioning of the whole eTIR system from the beginning and even more when the number of TIR transports carried under the eTIR procedure will increase. The following tables describe both the qualitative and quantitative aspects of the availability requirements. Several of them will be part of the service level agreement (SLA) to be signed with the United Nations hosting provider (hereafter the hosting entity) which will be selected to host the eTIR international system.

Table 4
Qualitative availability requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
AV.1	Normal maintenance operations for the software and systems components of the eTIR international system are performed transparently as the service remains available.	Design the eTIR international system in a way that avoids single points of failure (SPOF), using several front-end web servers to share the workload, database clustering, duplication of application components, and by possibly using high-availability proxies and orchestration of containers

Table 5
Quantitative availability requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
AV.2	General availability of the eTIR international system	Host the eTIR international system in a UN organization that proposes this level of availability and include it in the SLA.	24 hours per day, each day of the year.
AV.3	Percentage of uptime of the eTIR international system	Normal maintenance operations for the software and systems components of the eTIR international system are performed transparently as the service remains available. Issues with the system are quickly identified and dealt with using SOPs and escalation mechanism.	Greater than 99% (i.e. a maximum of 3d 15h 39m 29s of downtime per year).
AV.4	Maximum consecutive eTIR international system downtime in case of a major issue	Monitoring of services, software components and virtual servers is configured and agreed with the hosting provider. Procedures are prepared and agreed in the SLA.	4 hours during weekdays and 24 hours during weekends, per occurrence.

86. Once the eTIR international system starts to be used in production, following the study on measures collected and on the feedback from eTIR stakeholders, ECE or TIB may wish to propose to improve the target values of requirements AV.3 and AV.4 to increase the availability of the service. In this case, ECE would submit to TIB a proposal to improve the above-mentioned target values, along with possible budget implications.

3. Backup

87. A backup is a copy of eTIR related data made and stored elsewhere, in a secured location, so that it can be used to restore them after a data loss event.

88. Each storage location (i.e. eTIR database, eTIR logs and eTIR documents) will be backed up to ensure the requirements are met. The ones indicated in the following table will be part of the SLA to be signed with the hosting entity.

Table 6
Backup requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
BK.1	Frequency of backup of eTIR data	Information stored in the eTIR database, the eTIR logs and the eTIR documents is backed up twice per day and this backed up data is stored in a secured location.	12 hours
BK.2	Maximum time to restore backed up data following a data loss event	Restore procedures are prepared and agreed in the SLA with the hosting provider. Tests are regularly carried out.	6 hours

89. Once the eTIR international system starts to be used in production, ECE or TIB may wish to propose to improve the target values of requirements BK.1 and BK.2. In this case, ECE would submit to TIB a proposal to improve the above-mentioned target values, along with possible budget implications.

4. Capacity and scalability

90. There are basically two aspects to take into consideration regarding capacity management: the throughput of the system (i.e. its ability to process incoming messages and send responses) and the storage of the various pieces of information received. The scalability of the eTIR international system is its capability to handle a growing amount of workload by adding resources to the system.

91. The figures in the following table are based on an analysis performed to determine the needs in terms of capacity and scalability for the eTIR international system and available in annex V.C. As mentioned in its conclusions, the estimates and forecast in terms of throughput and volume of data are only as good as the various assumptions they are based on. Since the eTIR international system is not yet in operation, this analysis lacks actual data. For this reason, the eTIR international system should be designed while considering the capacity and scalability requirements for the first two years only, as there is a high probability that real data will correct several assumptions, which would change the calculation result and forecast for the next years.

Table 7
Capacity and scalability requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
CP.1	Maximum number of messages to be processed	A queuing component stores incoming messages. Several front-end web servers then pop messages from the queue to be processed under timeout thresholds.	2021: 12 messages per minute 2022: 78 messages per minute 2023: 270 messages per minute 2024: 570 messages per minute 2025: 1200 messages per minute

Identifier	*Description*	*How to achieve the target*	*Target value*
CP.2	Maximum storage dedicated to the eTIR logs	eTIR logs are directly saved on the front-end web servers. On a daily basis, they are moved to a central, secured location which will have enough storage space to aggregate them all.	2021: 371 GB per year 2022: 1.2 TB per year 2023: 4.9 TB per year 2024: 17.1 TB per year 2025: 36.1 TB per year
CP.3	Maximum storage dedicated to the eTIR database	Depending on the actual data received and on regular performance measurements, only the most recent data (last six months for instance) may be kept in the clustered database (while older data is regularly offloaded to a secondary database) to ensure the size of the main database does not negatively impact its performance.	2021: 1.4 GB per year 2022: 4.3 GB per year 2023: 17.9 GB per year 2024: 62.6 GB per year 2025: 133.3 GB per year
CP.4	Maximum storage dedicated to the eTIR documents	eTIR Documents are not stored in the database but on a central, secured, file system which will have enough disk space to gather them all.	2021: 100 GB per year 2022: 315 GB per year 2023: 1.3 TB per year 2024: 4.6 TB per year 2025: 9.8 TB per year

92. As mentioned in the conclusions of the analysis presented in annex V.C, ECE shall perform the same analysis six months after the eTIR international system is deployed in production in order to submit to TIB a revision of the above mentioned target values, along with a possible budget proposal.

5. Configuration management

93. Configuration management is the process that tracks all of the individual configuration items of the eTIR international system. A configuration item is an IT asset or a combination of IT assets that may depend on and/or have relationships with other IT processes (e.g. source code, configuration files, procedures, internal documentation, etc.).

94. An appropriate number of measures and procedures related to configuration management is the only effective and sustainable way to develop and maintain a major information system like the eTIR international system and ECE will ensure that the following technical requirements are properly addressed.

Table 8
Configuration management requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
CM.1	The source code of all modules of the eTIR international system should be versioned using a version control system (VCS) to allow for an effective management of this asset.	The source code of all modules of the eTIR international system is versioned using Git and hosted within UN premises.
CM.2	All changes related to the eTIR database should be versioned using a VCS to allow for an effective management of this asset.	All changes related to the eTIR database are versioned using Liquibase and Git and hosted within UN premises.
CM.3	All assets related to the documentation of the eTIR system should be versioned using a VCS to allow for an effective management of this asset.	All assets related to the documentation of the eTIR system are versioned using various VCS depending on their nature and hosted within UN premises.
CM.4	All assets related to the internal documentation of the eTIR system should be versioned and accessible to ECE using a collaboration software to allow for an effective sharing of knowledge and improved productivity.	All assets related to the internal documentation of the eTIR system are versioned and accessible to ECE on a knowledge management system (KMS) that acts as a secured and versioned

Identifier	*Description and objective*	*How to fulfil the requirement*
		collaboration platform hosted within UN premises.
CM.5	All bug reports, feature requests and other issues are logged, managed and eventually addressed using an issue tracking system to ensure that the issues raised by all eTIR stakeholders are properly evaluated and treated with the appropriate level of priority.	All bug reports, feature requests and other issues are logged, managed and eventually addressed using an issue tracking system hosted within UN premises.

6. Data Retention

95. Data Retention defines the policies related to persistent data and records management for meeting legal and business data archival requirements, such as the ones listed in Annex 11. The following table lists the requirements in terms of data retention for the eTIR international system.

Table 9
Data Retention requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
RE.1	Availability of the information stored in the eTIR international system	Information stored in the eTIR database, the eTIR logs and the eTIR documents are backed up on a daily basis and additional copies are made and kept on tapes stored in a separate, secured location, resistant to most disasters.	10 years[18]
RE.2	Retrieval of information requested by contracting parties for verification purposes[19]	Retrieval procedures are prepared and agreed in the SLA with the hosting provider.	Maximum of three days to retrieve the information

7. Disaster recovery

96. Disaster recovery involves a set of policies, tools and procedures to enable the recovery or continuation of the eTIR international system following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions and can therefore be considered as a subset of business continuity planning.

97. Usually, disaster recovery assumes that the primary site is not recoverable (at least for some time) and represents the set of processes needed to restore the services to a secondary site. In the scope of version 4.3 of the eTIR specifications, it is assumed that only a secondary site of type "warm site" is available for disaster recovery purposes, principally for costs reasons.

98. A "warm site" contains the equipment and data circuits necessary to rapidly establish operations. This equipment is usually preconfigured and ready to install appropriate applications to support an organization's operations. However, is this secondary site is to be used because the primary site is no longer available because of a disaster, all software components still have to be installed and configured on the servers of the "warm dite". Furthermore, live data from the primary site is not replicated on this type of secondary site in real time but data transactions are only copied on a regular basis.

99. The impact of a disaster is high because it brings the eTIR international system down for an unusual long period of time (typically more than one day). However, the probability of such a disaster occurring is extremely low. The resulting risk is minor in the context of version 4.3 of the eTIR specifications as the number of TIR transports using the eTIR

[18] As per paragraph 1 of article 12 of Annex 11 of the TIR Convention
[19] As per paragraph 3 of article 12 of Annex 11 of the TIR Convention

procedure will be low at first and only progressively increase as additional contracting parties interconnect their national customs systems to the eTIR international system. Furthermore, the fallback procedures described in the eTIR functional specifications act as mitigating measures for this risk.

100. The following table lists the disaster recovery requirements for the eTIR international system.

Table 10
Disaster recovery requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
DR.1	The recovery time objective (RTO)[20] of the eTIR international system, after a disaster.	Prepare a disaster recovery plan with all procedures detailing how to recover the eTIR international system and execute regular tests of this plan.	48 hours
DR.2	The recovery point objective (RPO)[21] of the eTIR international system.	Regularly and securely send copies of eTIR related data to the warm site. Perform recovery tests.	4 hours

101. Once the eTIR international system starts to be used in production, ECE or TIB may wish to propose to improve the target values of requirements DR.1 and DR.2. In this case, ECE would submit to TIB a proposal to improve the above-mentioned target values, along with possible budget implications.

8. Fault tolerance

102. Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. Modern information systems architectures and infrastructure take into account usual technical failures of components like hard disk drives, network connections, power failures and can provide a level of fault tolerance which is transparent to the end users.

103. The requirements listed in the following table provide a first level of technical fallback which does not need to be activated by the eTIR stakeholders. These requirements are mostly fulfilled by the underlying infrastructure and will be part of the SLA to be signed with the hosting entity.

Table 11
Fault tolerance requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
FT.1	Handle gracefully the failure of a physical server, which can be due to a piece of equipment (CPU, memory, motherboard, HDD, network card, etc.) to avoid the eTIR international system becoming unavailable.	An infrastructure based on a virtual server farm relying on several physical servers which manage hot swapping of virtual machines to mitigate such a failure. Architecture based on computer cluster to avoid any SPOF.
FT.2	Handle gracefully the failure of a piece of equipment used by the storage locations (HDD, SSD) to avoid the eTIR international system becoming unavailable.	An infrastructure based on a SAN using a redundant architecture for the disk drives (RAID). Architecture based on computer cluster to avoid any SPOF.
FT.3	Handle gracefully the loss of internet connectivity to avoid the eTIR international system becoming unavailable.	Double internet connection with two different providers.

[20] The RTO is the amount of time in which it should be feasibly to recover the IT service in the event of a disaster.

[21] The RPO is the maximum targeted period in which data (transactions) might be lost from an IT service due in the event of a disruption.

Identifier	*Description and objective*	*How to fulfil the requirement*
FT.4	Handle gracefully power failures to avoid the eTIR international system becoming unavailable.	Racks of uninterruptible power supplies (UPS) and emergency fuel generators to power the data centre with enough fuel in reserve to wait for the power to come back to be refilled with more fuel.

9. Internationalization and localization

104. Internationalization and localization are means of adapting computer software to different languages, regional peculiarities and technical requirements of a target locale. Internationalization is the process of designing a software application so that it can be adapted to various languages and regions without engineering changes. Localization is the process of adapting internationalized software for a specific region or language by translating text and adding locale-specific components.

105. Since the eTIR international system does not have a user interface, the requirements in terms of internationalization are limited to the eTIR messages and how data is stored in the various storage locations. Several approaches have been taken to limit the needs in terms of localization:

- Most of the attributes in the eTIR messages are using code lists. These code lists detail all the possible codes that an attribute can take, which facilitates the transfer of information from one system to another, since all systems are aligned on the same set of code lists. Furthermore, this method avoids having to translate values which therefore do not need to be localized;
- Numbers are expressed using fixed patterns which are clearly defined in the XML Schema Definitions of the eTIR messages. This approach clears any potential ambiguity related to decimal and thousands separators;
- Dates are also expressed using specific patterns either for a date only or for a date and time, including a Coordinated Universal Time (UTC) offset;
- Text fields are kept to a minimum and are used most of the time to represent words that are usually not translated like: identifiers, proper nouns and addresses. A few text fields are used to hold sentences in a given language and the sub attribute “Language, coded” can be used to define the language of the values stored in these text fields.

106. The following table lists the requirements in terms of internationalization and localization

Table 12
Internationalization and localization requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
IL.1	The eTIR messages should be able to handle text values in French, English and Russian.	The character set of the eTIR messages exchanged in SOAP/XML is UTF-8, the content type is “application/soap+xml”.
IL.2	The eTIR database should be able to store text values (from the eTIR messages) in French, English and Russian.	The character set of the eTIR database is UTF-8.
IL.3	The eTIR logs should be able to store the entire eTIR messages as they are received.	The character set of the files stored in the eTIR logs is UTF-8.
IL.4	The eTIR documents should be able to store the attached documents in various languages in addition to French, English and Russian.	The character set of the files stored in the eTIR documents is UTF-8.
IL.5	The language of the text values held in the eTIR messages should be identifiable.	The text values are characterized with the “Language, coded” sub attribute which uses a code list to specify the language name.

10. Interoperability

107. Interoperability is a characteristic of a system, whose interfaces are comprehensively detailed, to work with other systems, at present or in the future, in either implementation or access, with full compatibility.

108. The eTIR system is based on machine to machine communication triggered by specific events. Therefore, the interfaces between the various eTIR stakeholders must be clearly defined to ease the interconnection between the systems. Also, in order to further facilitate this interconnection, the interfaces should be based on worldwide renowned standards.

Table 13
Interoperability requirements

Identifier	*Description and objectives*	*How to fulfil the requirement*
IT.1	The eTIR data model should be aligned with a worldwide renowned data model to facilitate the connection between the eTIR international system and the information systems of the other eTIR stakeholders.	The eTIR Data Model is fully aligned with the World Customs Organization (WCO). Data maintenance requests (DMR) are submitted by ECE to continuously adapt the WCO data model to the needs of the eTIR procedure.
IT.2	The format and technical specifications of the eTIR messages are following strict guidelines to ensure the electronic exchange of messages is interoperable between information systems.	The eTIR message specifications are following the WCO XML guidelines. Automated compliance tests are also performed to validate this aspect.
IT.3	Information exchanged in the eTIR messages is standardized as much as possible to facilitate their processing by all eTIR stakeholders.	The attributes of the eTIR messages rely as much as possible on code lists from renowned standards (UN/EDIFACT and ISO).
IT.4	eTIR stakeholders should have sufficient time to migrate to the next version of the eTIR specifications while continuing to use the current version of the eTIR specifications.	The eTIR international system will be able to receive, process and send eTIR messages using two versions of the eTIR specifications: the current one and the next one proposed for implementation to all eTIR stakeholders during a specific migration time window which details are described in the release management processes.

11. Maintainability

109. Maintainability is the ease with which a product can be maintained in order to (inter alia): correct defects[22], meet new requirements, make future maintenance easier and cope with a changing environment.

110. A usual pitfall in software engineering and software management is to underestimate the need to continuously invest a reasonable amount of money to maintain and upgrade an information system, in order to prevent having to pay a very high amount of money to refactor it completely because it has not been properly maintained over the years.

111. The IT industry also recognizes that a large portion of the total cost of ownership (TCO) of an information system is spent during the maintenance phase of its lifecycle: usually between 50% to 80%. This highlights the importance of taking the appropriate preventive measures to keep the costs of maintenance of an information system to a reasonable level while ensuring that all exigencies on maintainability are met.

112. In particular, measures should be taken to avoid building a technical debt. Technical debt is a concept in software development that reflects the implied cost of additional rework caused by choosing a poor decision that might yield benefits in the short-term but will increase the costs of maintenance in the long term. Indeed, as with monetary debt, if technical

[22] See the definition of « defect » in the technical glossary

debt is not repaid, it can accumulate 'interest', making it harder to implement changes in the future.

113. The following table lists the requirements in terms of maintainability.

Table 14
Maintainability requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
MT.1	Technical debt should not accumulate on the programming languages, frameworks and libraries used to build the eTIR international system.	The latest stable versions of the underlying programming languages, frameworks and libraries used to build the eTIR international system are regularly reviewed and updates or upgrades are regularly planned. Recurrent reviews of the emerging trends are also performed, and appropriate actions are taken to migrate to better options before a component becomes deprecated.
MT.2	Technical debt should not accumulate on the source code of the eTIR international system.	A static code analysis tool is used to measure the maintainability index of the source code and regular attention is given to reduce the number of issues flagged by this tool. Regular code refactoring activities are also performed to reduce the *software entropy*[23] of the source code.
MT.3	Knowledge is retained to properly maintain and improve the eTIR international system	The internal documentation of the eTIR international system is managed on a KMS that acts as a secured and versioned collaboration platform between the members of ECE. One of the roles of the IT coordinator is to ensure that the appropriate level of documentation (including SOPs) is prepared and remains updated on the KMS in order to mitigate the risks of turnover and key person.[24]

12. Performance

114. Performance is the numerical indication, measuring the maximum or optimal possibilities of a hardware, software, system or technical process to perform a given task. In the case of the eTIR international system, the requirements are focused on the response time and the throughput characteristics.

115. Requirements on the throughput of the eTIR international system are already detailed in the section devoted to capacity, respectively with CP.1 and CP.2. Requirements on the response times are detailed in the following quantitative table, while additional requirements related to performance are listed in the qualitative table below.

Table 15
Quantitative performance requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
PE.1	Average response time involving short messages (up to 10KB) measured by the sender from sending the request message to receiving the response message.	The eTIR international system is properly designed and free of any logical or technical bottlenecks that could be a performance issue. The management of the eTIR database, writing information to the eTIR logs and connecting to the ITDB are all optimized operations.	1 second
PE.2	Maximum response time involving short messages (up to 10KB) measured by the sender from sending the request message to	Enough nodes are provisioned for the eTIR web services software components to be able to cope with all requests. Enough nodes are provisioned for the eTIR database to be able to cope with all requests.	10 seconds

[23] See a definition in the Technical Glossary.

[24] Key person risk: risk carried by an organization that depends to a great extent on one individual for its success.

	receiving the response message.		
PE.3	Maximum response time measured by the sender from sending the request message to receiving the response message.	The maximum size of the eTIR messages is set to 20 MB. The connection of the eTIR international system to the Internet has a high bandwidth (over 100 megabits per second).	The timeout is set to 60 seconds

Table 16
Qualitative performance requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
PE.4	Performance metrics of the eTIR international system should be monitored to identify any potential problem.	Metrics related to performance are logged at different key points during the reception of a request message, its processing, recording and sending of the response message. These metrics are monitored to raise an issue for ECE to investigate when their values increase above specific thresholds.
PE.5	Performance metrics of the eTIR international system remain stable or get better over time.	A load testing tool is used to perform automated load tests when new developments are introduced in the eTIR international system to ensure no sensible regression – in terms of performance – is introduced.

13. Reliability

116. Reliability is the ability of an information system to cope with errors during execution and cope with erroneous input. It also encompasses the set of practices followed to ensure that the objectives in terms of quality are met. Maximizing the reliability of the eTIR international system is the essence of the second guiding principle that is followed by ECE.

117. In order to ensure this objective and a high overall quality for the eTIR international system, the following proactive practices are put in place:

- Guidelines are established within ECE on the following aspects of the eTIR international system: development, deployment, operation and maintenance. These guidelines form a common set of rules and practices that ensure predictable, high-quality results;
- Strict versioning procedures exist to ensure that all changes brought to the source code of the eTIR international system and the structure and contents of the eTIR database can be traced back to a requirement entered in the issue tracking system;
- Code reviews are performed to decrease the probability of adding unwanted side-effects (defects) to the source code and to ensure that the coding guidelines are followed;
- All changes to the source code (either to introduce a feature or correct a defect) are accompanied by the appropriate automated tests to ensure that no regression is introduced in the source code;
- The source code is regularly checked by a static code analysis tool to determine several indicators related to maintainability, reliability, security, code coverage and code duplication. The issues raised by this tool are addressed by ECE to meet quality objectives (quality gates) previously set;
- A continuous integration pipeline is in place to automatically perform several operations during the development of the eTIR international system to ensure a high level of reliability and quality.

118. In addition to proactive practices, the following reactive practice is also put in place to be able to identify issues and solve them as soon as possible:

- The monitoring system continuously watches several indicators and metrics associated with the software and systems components of the eTIR international system

to detect any issue and raise the appropriate alerts for a quick resolution of the issue (depending on its severity).

119. The following tables list the requirements in terms of reliability.

Table 17
Quantitative reliability requirements

Identifier	*Description*	*How to achieve the target*	*Target value*
RL.1	Number of remaining issues with the highest severities found by the static analysis tool	Check the source code using the static analysis tool on a regular basis and correct any issue with the highest severities as a high priority.	0 (all issues of this kind should be corrected)
RL.2	Number of remaining issues with a normal severity found by the static analysis tool	Include checking the source code using the static analysis tool in the continuous integration pipeline to provide a quick feedback and improve the ways of working.	Less than 150
RL.3	Percentage of functional source code covered by automated tests (code coverage)	Code reviews and development guidelines ensure that any change to the source code is accompanied by the appropriate number of automated tests.	More than 60%
RL.4	Percentage of duplicated source code (code duplication)	Regular reviews of the code to ensure no code duplication is introduced.	Less than 3%

120. ECE will regularly review and restrict the targets set for the quantitative reliability requirements listed in the above table to continuously increase the overall quality of the source code of the eTIR international system.

Table 18
Qualitative reliability requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
RL.5	All changes to the source code are made in a way that decreases the probability to introduce issues.	Specific guidelines and best practices are followed by ECE while developing the eTIR international system. Automated tests allow to immediately flag any regression introduced. Commits which do not pass specific quality gates are rejected.
RL.6	All changes to the source code are linked to a requirement to ensure proper traceability.	The VCS used for the source code and the issue tracking system are connected. It is possible to find the issue related to a specific commit in the VCS and all commits need to reference an issue.
RL.7	Eliminate as many redundant, manual and error-prone tasks from the development procedures.	Put in place a continuous integration pipeline that relieves IT experts from mundane tasks and allow to give them a quick feedback on the quality of the change they bring to the source code.

14. Reusability

121. Reusability is the use of existing assets in some form within the software product development process. These assets are products and by-products of the software development life cycle and include code, software components, test suites, designs and documentation.

122. The main objective of reusability is to stop “reinventing the wheel”. In modern software engineering and with the use of object-oriented programming languages, it is easy to reuse existing software components. In addition, this approach is pertinent not only for software components but also for methods and frameworks as a lot of experience and good practices have been used to formulate these standard approaches. Here are the ones used in the development of the eTIR system:

- Project management: The UN secretariat has selected the PRojects IN Controlled Environments - PRINCE2® project methodology and ECE has tailored this method to apply it to the management of its projects;
- Enterprise architecture: ECE is using several aspects of The Open Group Architecture Framework - TOGAF® for its needs in terms of architecture;
- Software development: ECE is following an Agile methodology to develop and maintain the eTIR international system and apply several DevOps practices;
- Service management: ECE is using several aspects of the Information Technology Infrastructure Library - ITIL® for its procedures related to the eTIR service desk and its relationship with the UN entity hosting the eTIR international system;
- Security awareness: ECE is using several aspects of the Open Web Application Security Project - OWASP® to learn about the latest security threats and best practices.

123. Most of the times, selecting an element to be reused should be preferred rather than develop it oneself. Indeed, if the scope of functionality matches the requirements, it is usually quicker and less costly to select an existing element to be reused. In terms of software component or product, this can either be a piece of Open Source Software (OSS) or some proprietary software. In the decision-making process, the following aspects should be considered: TCO (including training and support), maturity and sustainability of the solution, advantages and disadvantages.

124. The following table lists the requirement in terms of reusability.

Table 19
Reusability requirement

Identifier	*Description and objective*	*How to fulfil the requirement*
RU.1	Reuse existing methods, frameworks, software and systems components to save time and achieve higher quality outputs	In case of a new requirement or during the regular assessment performed on currently reused elements, ECE looks for available options and applies its decision-making approach to select the best option.

15. Security

125. All security related aspects and technical requirements of the eTIR international system are described in the dedicated part “Security of the eTIR system” later in the document.

E. Development processes

1. Introduction

126. This section describes the processes followed by the Information Technology (IT) experts of ECE (hereafter “the IT experts”) to develop the eTIR international system so that contracting parties to the TIR Convention and the other eTIR stakeholders have a clear understanding of these aspects. Being transparent about these processes also provides an opportunity to all eTIR stakeholders to suggest proposals for improvement with the ultimate objective to have a more effective and efficient eTIR system in the long term.

2. General guidelines

127. The IT experts have taken the time to prepare, discuss and adopt their own internal guidelines related to all aspects of the development and maintenance of the eTIR international system. Proven best practices from the IT industry and experience acquired by the IT experts drive the formulation of these guidelines. Nevertheless, they are not set in stone and the IT experts will continuously strive to identify opportunities to improve them. This is especially important in an area of expertise such as Information and Communication Technology, that is evolving so quickly.

128. While preparing and improving guidelines, as well as in all decision-making processes, the IT experts are inspired and steered by the three guiding principles detailed at the beginning of this document.

129. When taking a technical decision on any aspect related to the eTIR international system, the IT experts follow the usual best practices in decision-making process. The time needed to explore and study emerging trends, approaches and possible products is invested. Possible options are then formulated, their respective advantages and disadvantages are listed and then a decision can be taken to select the best option. Decisions are documented, along with the rationale that led to this choice, to keep proper institutional memory.

130. Finally, the IT experts also recognize and take into account the Pareto principle[25] in their decision-making process to find the optimum in achieving most of the benefits in the least amount of time possible. This principle is usually confirmed when it is applied in software engineering and it becomes even more pertinent in times of difficult economic situations to ensure funds are wisely spent.

3. Development methodology

131. The development of a major information system such as the eTIR international system requires following an IT project methodology to be successful. In the short – although intense – history of IT, several paradigms and models have been proposed and extensively tested (e.g. Waterfall, V model, Prototyping, Incremental, Agile, etc.). In 2001, emerging from several new agile methodologies (e.g. eXtreme Programming and Scrum), a major breakthrough was achieved with the establishment of the Agile Manifesto[26] and its twelve principles. Since then, many IT projects were conducted using agile methodologies which offer the best chances of success for such complex endeavours.

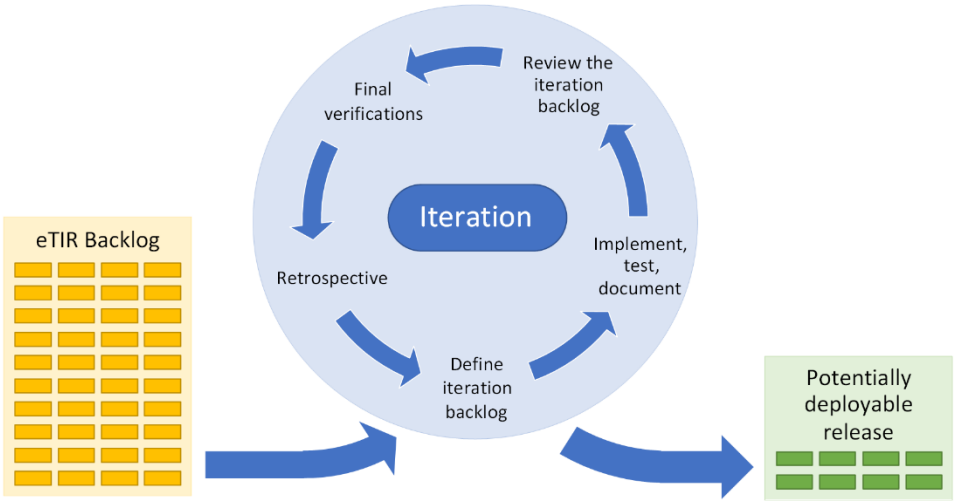
132. ECE has chosen to follow an agile methodology close to Scrum and Kanban to develop the eTIR international system. This approach focuses on the following objectives: developing valuable and working software, being able to quickly respond to change, instil a high level of quality and above all, satisfying the beneficiaries.

133. All the work that needed to be done is broken down into tasks (hereafter referred to as “issues”) and maintained in a list, called the eTIR backlog. Development is performed by iterations of several weeks. At the beginning of each iteration, the IT experts select from the eTIR backlog a set of issues to define the iteration backlog. During the iteration, the implementation, testing and documentation activities are performed on these selected issues which are then reviewed towards the end of the iteration to define the final scope of the iteration (as several unfinished issues can be removed from the iteration). After a last stage where final verifications are performed on the quality of the iteration, the output of the iteration constitutes a potentially deployable release.

[25] See en.wikipedia.org/wiki/Pareto_principle

[26] See agilemanifesto.org

Figure XIII
Development by iteration



134. Keeping in mind that the eTIR international system should be developed once and then properly operated and maintained indefinitely, ECE has also chosen to adopt several practices from the DevOps movement which aim at preventing issues that may arise while moving from the development phase to the operational phase of the project. These practices are the following (which are further described below): invest in automated testing, rely on continuous integration, analyse telemetry and perform blameless post-mortems.

4. Development guidelines

135. Standard coding guidelines and abundant IT literature[27] on the subject constitute the cornerstone of the development guidelines. The underlying technology stack of the eTIR international system is Java and the IT experts use a modern and renowned integrated development environment (IDE) to program effectively with this language and related ecosystem. This IDE also allows integrating some of the development guidelines (access to the version control system (VCS), static code analysis tool, code formatting rules).

136. The IT experts use Git as the VCS of the eTIR international system and follow the usual best practices related to this product. Modifications brought to the source code are regularly committed and pushed to the central repository to be shared between all developers and prevent any loss of work in case of a workstation malfunction. Large developments are usually performed on separate branches. Finally, pushing code changes to the central repository requires prerequisites steps (detailed in the next sections) to ensure that each contribution has a high quality.

5. Logging guidelines

137. The logging service of the eTIR international system is very important as it produces the data needed for the non-repudiation system and for producing the metrics required to monitor the global health of the system. As explained in DevOps practices, these metrics (or telemetry) are the only way for the IT experts to monitor the eTIR international system in operation, and to be alerted of any issue arising and, thus, being able to efficiently resolve the issue even before being contacted by end-users.

138. The logging service generates several files, each having its own function. Each entry to a logging file is accompanied with the date and time information when it occurred and a potential severity:

- **eTIR messages**: all contents of the incoming and outgoing messages are saved into a file to store the entire communication threads between the eTIR international system and the information systems connected to it. This data is then used by the non-

[27] In particular from authors Kent Beck, Martin Fowler and Robert C. Martin.

repudiation system and can be retrieved upon request by the contracting parties to the TIR Convention;

- **Database**: all queries to the eTIR database are saved in a file along with the time needed to perform these queries. This allows to continuously measure the performance of these queries and give indicators to the IT experts to identify and remove potential bottlenecks as well as better plan for future scalability requirements;
- **ITDB**: all calls made to the interface with the International TIR Data Bank (ITDB) are saved in a file along with the time needed to perform these queries. This allows to continuously measure the performance of these calls and give indicators to the IT experts to further optimize this interface;
- **Application**: all events occurring in the eTIR web services module are saved in a file to store the whole history of events which is used by the monitoring system to alert on any serious issue occurring in real time with the eTIR international system. This data is also used when investigating a past issue to identify its root cause.

6. Testing guidelines

139. Tests are a vital part of software engineering. IT history consistently shows that without proper attention dedicated to this aspect, software projects have a substantially higher probability to fail. Tests can either be manually or automatically executed. In the case of manual execution, the tester follows a series of steps to interact with the information system to be tested and compares the actual results he or she gets with the expected results. If they match, the test is successful and if not, it is a failure. Manual tests are the most obvious action a software engineer can immediately apply on a newly developed piece of software to verify if it works as expected. However, the biggest impediment of manual tests is that they rely on a person to execute them, which is not cost-effective and error prone. Moreover, they only verify the state of the system at the moment they are executed and their result (success/failure) is therefore no longer relevant when the conditions change (the source code is updated, the environment settings are updated, etc.).

140. Nowadays, in modern software engineering practices, it is acknowledged that manual tests are no longer sufficient to ensure high reliability and quality for the information system being developed. As explained in the related DevOps practices, tests now need to be automated to be executed on specific frequent events (when the conditions change, as mentioned above) to ensure that no regressions are introduced. Indeed, when implementing new features or correcting defects in the source code, software engineers always risk bringing in unwanted side-effects (like defects). In order to solve this inherent problem of software engineering, automated tests have to be implemented to verify any change being brought to the source code. It is important to keep in mind that this investment in time in implementing automated tests always pays off. Indeed, when automated tests are absent, the number of defects is much higher, and the time needed to investigate and correct them is substantially higher than the time needed to implement automated tests. In addition, regular issues experienced with systems because of defects can frustrate their users and cause severe reputational damage to the entity in charge of the system.

141. There are several types of automated tests that have their own characteristics that complement one another:

- **Unit tests**: tests written to check that a piece of software (known as the "unit") meets its design and behaves as intended. In object-oriented programming languages like Java, the unit is often an entire interface, such as a class, but could also be an individual method. The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. A unit test provides a strict, written contract that the piece of code must satisfy. Unit tests are usually quick to implement and then to execute;
- **Integration tests**: tests written to check that software modules are combined and tested as a group. Integration testing is conducted to evaluate the compliance of a system with specified functional requirements. It occurs after unit testing and before validation testing. Integration testing takes as its input modules that have been unit

tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for validation testing;

- **Performance tests**: tests written to check that a software system meets its performance requirements. This family of tests also includes tests written to simulate a given load (high number of queries) applied to the software. This type of tests is important to verify that the performance of the software does not degrade over time, in particular when new features are added;
- **Validation tests**: tests written to check that a software system meets its specifications and that it fulfils its intended purpose. Usually these tests are the most complex and costly to implement and maintain, as they involve simulating actions performed by end users on the user interface (UI) of the system. In the specific context of the eTIR international system, there is no UI, as data is exchanged automatically with the information systems of the other eTIR stakeholders using the eTIR messages. This approach allows for a very easy and efficient way to perform validation tests, as each test request message sends back a response message that can be validated to ensure the system behaves as expected;
- **Conformance tests**: similar to the validation tests, this type also includes, in the context of the eTIR system, the necessary tests to ensure that a representative set of simulated TIR transports is properly managed by sending and receiving a specific sequence of eTIR messages that are checked to validate entire scenarios. These tests can also focus on testing the information system of one particular eTIR stakeholder, or they can also include several of them to better replicate real TIR transports following the eTIR procedure.

142. When writing automated tests, software engineers also need to ensure that most (if not all) relevant lines of the source code are covered and validated. In particular, software engineers need to ensure that all paths in the source code are covered with tests (this practice and related metrics are called “branch coverage”). In addition to an appropriate “code coverage”, software engineers also need to make sure that the assertions validating the source code are pertinent and comprehensive, otherwise the tests are not achieving their objective.

143. As described above, achieving a good code coverage is the only sustainable way to develop and maintain an information system and the IT experts have integrated this objective and related practices in the development processes. When a new feature is implemented, the appropriate number of unit and validation tests should be written to meet the code coverage objective. When a defect is corrected, one or more tests should be written to prevent the same issue from occurring again.

7. Static code analysis

144. Static code analysis consists in automatically examining the quality of the source code of a piece of software without actually executing this software. This examination is performed by a tool which is loaded with programming rules and best practices, most of them being defined over the years by the worldwide community of IT experts. Static code analysis is a very efficient way to perform a first check on the quality of the source code and an excellent complement to targeted manual code reviews performed by the IT experts on the source code.

145. While acknowledging the usefulness of this type of automated tool, the IT experts also recognize the need to jointly review the pertinence of several rules, given the specific context of the eTIR international system. As a result, the IT experts configure rules and their severity to best match this context.

146. Static code analysis is regularly performed on the entire source code of the eTIR international system and, in addition, the IT experts also benefit from the integration of this capability in the IDE they use for programming, which gives them an immediate feedback on the quality of the code they produce.

147. The objective is to progressively increase the quality of the source code and maintain it at a very high level throughout its lifecycle. This increases the reliability and

maintainability of the source code and, eventually, saves time to the IT experts, which increases their productivity. This objective is performed in two phases: progressively increasing the quality of the source code and maintaining it at a high level.

148. During the first phase, the IT experts set low quality gates[28] in the static code analysis tool and correct as many issues as needed to meet these targets. Once these low targets are met, they are gradually increased, and the IT experts continue working on solving issues to meet the new targets. Once the quality gates reach a level deemed sufficient by the IT experts[29] (also by taking into account the Pareto principle), the second phase can start.

149. During the second phase, the objective is to continue developing and maintaining the eTIR international system while continuing to meet all quality gates. Additional measures can be put in place to send a notification to the IT experts if one of these quality gates is breached following the update of the source code, so that the IT experts can immediately look into this issue to solve it.

8. Continuous integration (CI) pipeline

150. In software engineering, continuous integration (CI) is the practice of merging all developers' working copies to a shared mainline several times a day. This practice is not new (it dates from the 1990) and was continuously refined and expanded to finally get to the current DevOps practices, known as continuous integration and continuous deployment (CD) or CI/CD. The IT experts have chosen to focus on CI to start with, and once the appropriate maturity level is reached, they may consider also adopting the CD practice, which requires solid foundations.

151. Nowadays, the definition of CI reflects to the automation of all steps related to the integration and verification of changes in the source code of a software. CI allows software developers to get quick feedback on the quality of the code they commit to the VCS by executing all automated tests against a newly built and deployed version of the software, which contains the latest modifications brought to the VCS. CI relieves software developers from mundane, error-prone tasks related to building, testing and deploying a new version of the software, so that they can concentrate on where they have the best added value: to deliver features to the clients.

152. The IT experts have put in place a CI pipeline which consists of a specialized tool in which several actions are defined and configured to execute as successive automated steps. These steps are executed every time one of the IT expert commits a code change to the VCS. These steps are the following:

(a) **Build**: the CI pipeline detects that a commit was added to the VCS and will retrieve the latest version of the source code and build the new software components affected by the code change;

(b) **First testing phase**: automated unit and integration tests are then executed against the newly built software components to verify no regression was introduced with the code change;

(c) **Deployment on the SIT**[30] **environment**: the newly built software components are deployed on the SIT environment as a fully functional instance of the eTIR international system;

(d) **Second testing phase**: automated validation tests are then executed against the new instance of the eTIR international system to continue verifying, at the highest level, that no regression was introduced with the code change.

153. If an error happens during one of the steps (for instance if even only one test fails), the CI pipeline stops and a notification of failure is sent to the IT experts on their collaboration platform. The time of execution for all steps should not take more than 30 minutes to ensure

[28] A quality gate is a quantitative target set a on a particular criterion (e.g. «Less than 10 critical issues», «More than 40% of the source code covered with tests»)

[29] As detailed in the reliability requirements of the eTIR international system

[30] System Integration Testing (SIT), see next section for more information.

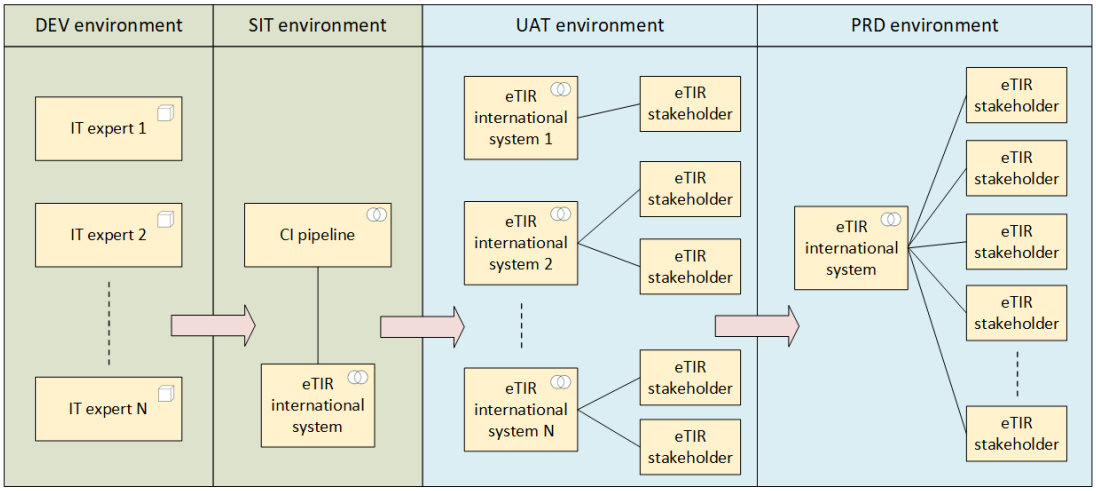
quick feedback to the IT expert who commits a change to the VCS. This CI pipeline combines several best practices described above and is an excellent way to ensure high reliability of the eTIR internationals system and increase the productivity of the IT experts.

9. Environments

154. Following modern best practices from the IT industry, the IT experts have set up and configured four different environments to develop and maintain the eTIR international system in the best conditions. One of the challenges in managing several environments is to limit the number of variances between each of them to avoid defects linked to a specific environment. Specific development procedures are set up and followed by all IT experts to limit the probability of occurrence of this type of defect.

155. The figure below shows the different environments, which are then described in the following paragraphs.

Figure XIV
Environments of the eTIR international system



156. **Development (DEV) environment**: each IT expert has his/her own workstation on which s/he can develop and test a local copy of the eTIR international system without interfering with the work of others. Once a code change has been prepared and tested, the IT expert commits it to the VCS so that it can be automatically deployed and tested on the SIT environment by the CI pipeline.

157. **System Integration Testing (SIT) environment**: this internal environment is used by the CI pipeline as a temporary location where newly instances of the eTIR international system are built, deployed and automatically tested. Once a set of code changes are validated on this environment, the IT experts may decide to build and deploy the latest version of the eTIR international system to the UAT environment.

158. **User Acceptance Testing (UAT) environment**: this environment is accessible by eTIR stakeholders to perform tests in the context of their interconnection projects. Several instances of the eTIR international system are available and each eTIR stakeholder gets access to one or more of these instances. Conformance tests of the eTIR international system and of the information systems of the eTIR stakeholders are also performed in the UAT environment. Once a version of the eTIR international system has been extensively tested in the UAT environment, it can be moved to the PRD environment.

159. **Production (PRD) environment**: this environment holds a unique instance of the eTIR international system which is only accessible to the eTIR stakeholders that have completed their interconnection project. This “live” environment is the only one used for performing TIR transports following the eTIR procedure.

10. Database guidelines

160. The eTIR database uses a database management system (DBMS) to record the information received in the eTIR messages. This component is the core of the eTIR

international system and its development and maintenance should be treated with the utmost care.

161. The structure of the eTIR database was inherited from the eTIR pilot projects and the IT experts have identified several opportunities for improvement and optimization which are planned to be progressively implemented. The IT experts use a specialized tool, Liquibase, to track, version and apply database schema (structure) changes. Furthermore, this library also allows managing changes applied to the master and reference data stored in the database.

162. In the context of the eTIR system, "master and reference data" refers to data about the parties, the roles, and data used to classify or categorize the data processed and stored from the eTIR messages (e.g. eTIR stakeholders identities, country codes, guarantee types, goods classification, etc.). This data changes on rare occasions and needs to be meticulously managed.

163. Using this tool also allows to easily check which changes have been applied to the various copies of the eTIR database, present in all environments listed in the previous section. This is important to ensure that a recent change implemented to the schema or the master and reference data is consistently applied on all environments following the relevant release management procedures.

11. Issue management

164. One of the cornerstones of the adopted agile methodology is a defined and effective issue management. In this context, an issue can represent a feature request, a change request or a defect report. All changes to the eTIR data model, to the source code or to the documentation of the eTIR international system first need to be logged into the issue tracking system of ECE. This is essential to ensure proper traceability of all changes and allows verifying that only authorized changes are applied.

165. When logging an issue into the issue tracking system, an IT expert ensures that all necessary details are documented so that any other IT expert should be able to understand what needs to be done. This is also a prerequisite to ensure retaining institutional memory without being affected by potential turnover in ECE.

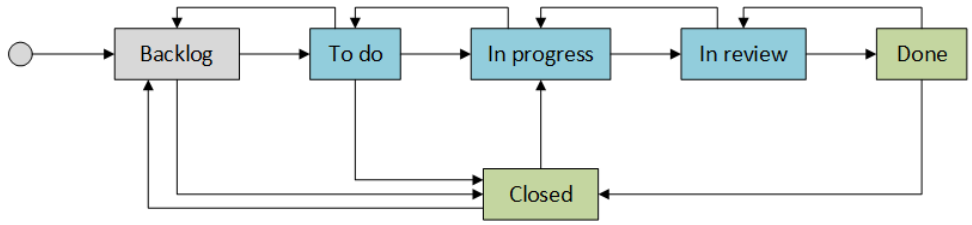
166. The IT experts have agreed on a series of activities that should be performed during the various stages of the lifecycle of any issue before it can be considered as completed. The stages are named with the different statuses of issues. This is the "definition of done" and it is defined as follows:

- **Definition of done (DOD)**: is when all conditions, or acceptance criteria,[31] that an issue must satisfy, are met. The objective is to ensure a proper level of quality and reliability of the system, at all times. The investment in time spent on all of these activities always pays off in terms of preventing defects from being deployed to the PRD environment. Having less defects prevents from spending time and stress in troubleshooting and avoids impacting the reputation of ECE.

167. A newly created issue gets assigned the "backlog" status, symbolizing its belonging to the eTIR backlog, and a priority is also assigned to it. Issues are the atomic work packages that are assigned to the IT experts by the IT coordinator when they have been selected in the iteration backlog. The following figure shows the issue lifecycle with the various statuses that an issue can take, and the following list describes them.

[31] The conditions and acceptance criteria are defined later on in the section.

Figure XV
Issue lifecycle



- **Backlog**: the issue has been identified and logged into the issue tracking system but is not yet selected for processing;
- **To do**: the issue has been selected to be worked during an iteration and is assigned to an IT expert who needs to complete the steps related to the "To do" stage of the DOD (see below);
- **In progress**: the issue is being processed by the IT expert who needs to complete all steps related to the "In Progress" stage of the DOD;
- **In review**: the issue is being reviewed by another IT expert to check several aspects related to quality assurance by following all steps related to the "In Review" stage of the DOD;
- **Done**: the issue is done (implemented and reviewed) and it will be finally validated by the IT experts during regular meetings where all deployed issues on the PRD environment are finally closed;
- **Closed**: the issue is either deployed (coming from "Done") or closed as it will not be corrected or it is considered as a duplicate of another issue (coming from "Backlog" or "To do").

168. The DOD describes the following key objectives and acceptance criteria for the abovementioned stages:

- **To do**: the issue is sufficiently detailed and has enough background information so that it can be understood by any other IT expert, and a first estimation of the time needed is made;
- **In progress**: the change needed is entirely performed across all appropriate IT assets (eTIR data model, source code, documentation). All exigencies in terms of quality and reliability are met (including the verifications performed by the CI pipeline and the static analysis tool) and all applicable guidelines are followed;
- **In review**: the outputs of the tasks performed during the “In progress” stage are checked by another IT expert. In particular, the test coverage for the source code updated is verified.

12. Documentation guidelines

169. ECE maintains three types of documentation related to the eTIR international system. The first type corresponds to the eTIR specifications, for which amendment procedures are described in Article 5 of Annex 11 of the TIR Convention.

170. The second type corresponds to the internal documentation that is necessary for ECE to properly develop, operate and maintain the eTIR international system. This documentation is prepared and updated by the IT experts of ECE and is managed on a secured KMS that offers versioning capabilities to properly store institutional memory. The internal documentation contains confidential information about, inter alia:

- Development: guidelines, technical documentation, training, stakeholder’s documentation, related standard operating procedures (SOPs), etc.
- Management: team administration, meeting notes, related SOPs, etc.

- Operations: connection with contracting parties, environments, eTIR service desk, related SOPs, etc.

171. The third type corresponds to the documentation that is produced by ECE for the eTIR stakeholders to interconnect their information systems with the eTIR international system. These documents are shared with the eTIR stakeholders on the web site[32] dedicated to eTIR. These documents are produced in addition to the eTIR specifications to facilitate the interconnection projects and benefit from the feedback received during these projects. They are a way for ECE to continuously clarify various aspects of the eTIR system in a more frequent and flexible way. All these documents are always fully aligned with Annex 11 and with the version of the eTIR specifications on which they are based.

13. Version management

172. ECE manages the source code of the eTIR international system and the changes applied to the schema and "master and reference data" of the eTIR database with a VCS. ECE has selected Git as its VCS and uses an internal and secured platform as the central Git repository.

173. The IT experts follow the usual best practices from the IT industry related to Git, and especially the ones from DevOps. In particular, IT experts should frequently commit and push their code to the central Git repository, after having performed all tests locally to ensure that this would not create a failure during the execution of the CI pipeline. Each commit should feature changes related to only one issue and the comment of the commit should clearly mention the issue to which it is related and describe the substance of the changes.

174. Branches are created and used in several cases. Firstly, they can be created by an IT expert who needs to work on a complex feature that cannot immediately be committed on the master branch. Once the feature is completed and tested, the branch is merged back into the master branch. Secondly, a branch is created every time a version of the eTIR international system is released on the PRD environment, following the release management guidelines. Tags are also created when a new version of the eTIR international system is deployed on the UAT environment or on the PRD environment.

175. Regarding the version number of the eTIR international system, ECE has selected an approach which uses the following three numbers:

- **Major version number**: it is incremented when a breaking change happens on the API which allows eTIR stakeholders to connect to the eTIR international system. It may also be incremented when a substantial change is brought to the eTIR international system without changing the API.
- **Minor version number**: it is incremented in any other case than the ones that affect the major of the hotfix version numbers. When the major version number is incremented, the minor version number is reset to 0.
- **Hotfix version number**: it is only used when one or more hotfixes need to be deployed on a version which is already deployed on the PRD environment, without willing to create a new version of the eTIR international system.

176. The major and minor version numbers, as well as the hotfix version number, if it exists, are always updated simultaneously on all software components of the eTIR international system and represent its version number under the form XX.YY.ZZ with XX being the major, YY the minor version numbers and ZZ the hotfix version number (ignored if equal to 0). Here are two examples of the version number for the eTIR international system:

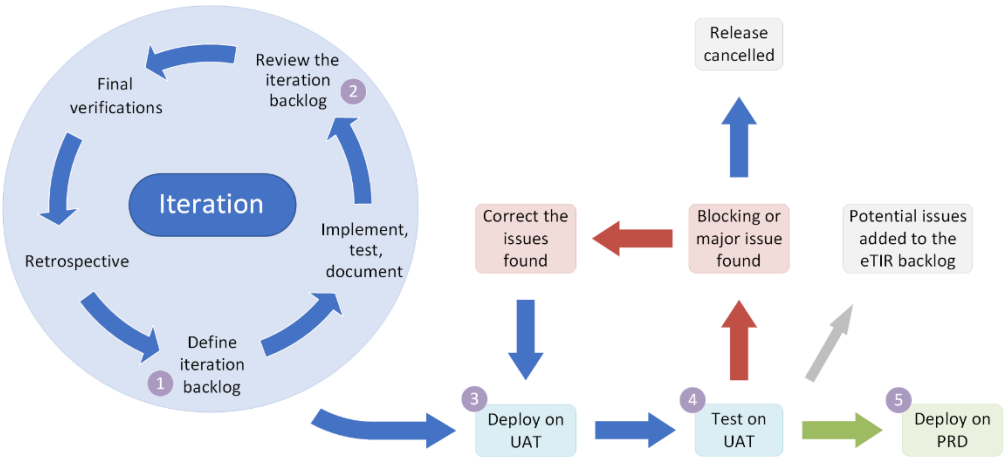
- **eTIR international system 4.15**, where 4 is the major version number and 15 is the minor version number (frequent case).
- **eTIR international system 4.15.1**, where 4 is the major version number, 15 is the minor version number and 1 is the hotfix version number (rare case).

[32] See etir.org/documentation.

14. Release management

177. Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases. In the context of the eTIR international system, it refers to the process described in the following figure and stages.

Figure XVI
Release management process



(a) **Define the iteration backlog**: the IT experts select from the eTIR backlog which issues should be worked on during the iteration and determine the version number of the new release. Each release has its own, unique version number which is mandatory if the release is to be deployed on the UAT or PRD environments.

(b) **Review the iteration backlog**: the IT experts review which issues are considered as "done" and modify either the iteration length or the list of issues assigned to this version. In the end, all issues are completed, tested and documented and the quality gates are passing on the SIT environment. The release notes, which explain the changes brought by this new version, are prepared.

(c) **Deploy on UAT**: the eTIR stakeholders working on the instances of the eTIR international system are informed about the new deployment to come. Then the new version is deployed on all instances of the eTIR international system and the related eTIR databases are reset. The release notes are communicated to the eTIR stakeholders.

(d) **Test on UAT**: the newly deployed release will then be tested by the eTIR stakeholders during a given period of time agreed by all parties. The IT experts determine if a new execution of the conformance tests is needed or not. Any issue found will be raised to the eTIR service desk to be logged and categorized. If one or more blocking or major issues are found, then either they are corrected, or the current release is cancelled and a new one will be prepared which will include as a priority the issue(s) to be corrected. If these issues are corrected, the updated release needs to be deployed on the UAT environment and tested again by all eTIR stakeholders for a given period of time before being validated. Minor issues can be added to the eTIR backlog to be fixed in a subsequent release.

(e) **Deploy on PRD**: if no major issue was reported after a given period of test on UAT, the release can be scheduled to be deployed on the production environment after a proper communication to the eTIR stakeholders. Once the deployment is performed on this final environment, the eTIR service desk actively monitors the telemetry to verify everything is working correctly.

178. Then, if an issue is identified on the production environment, three cases can happen:

(a) **The issue is blocking**: the IT experts roll back the PRD environment to the previous release and inform all eTIR stakeholders accordingly.

(b) **The issue is major**: the IT experts quickly prepare a hotfix, perform all tests needed on the SIT environment and deploy it on the PRD environment to correct the issue. All eTIR stakeholders are informed accordingly.

(c) **The issue is minor**: the issue is logged and added to the eTIR backlog to be fixed in a subsequent release.

F. Maintenance processes

1. Introduction

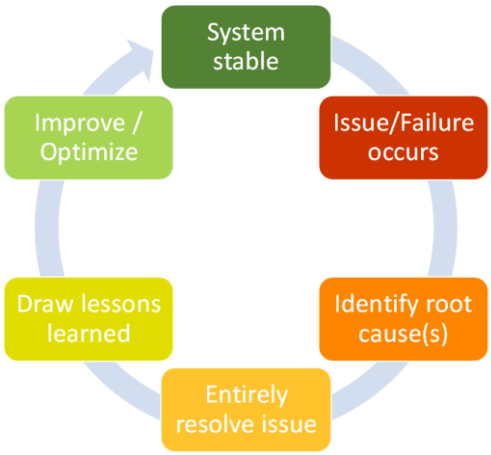
179. This section describes the processes followed by the IT experts of ECE to support and maintain the eTIR international system to ensure it functions correctly, to properly deal with issues and to anticipate and prevent possible problems in the future. This section also describes the procedure to be followed by the eTIR stakeholders when reporting an issue and informs of the internal activities performed to address it.

2. Continuous improvement

180. One of the underlying principle of the DevOps practices is about adopting a continuous improvement approach. It means that none of the outputs created (software, processes, documentation, etc.) are ever final as they can always be improved. Especially if an issue (a defect in the system, a flaw in a process, an omission or imprecision in the documentation) is raised, it should always be considered as an opportunity to improve. This principle is similar to the one used in the Deming cycle or PDCA[33].

181. With this approach, the IT experts recognize the importance of always seizing the opportunity to learn from issues to ensure that the same issues should not happen again in the future (or, at least, that the actions taken decrease the probability for a future occurrence). In particular, it is important to take the time to identify the root cause(s) of the issue to be able to entirely correct them and improve or optimize the processes, if possible. This approach is also applied in development processes but it is especially important in maintenance processes as their main objectives are to solve and prevent issues. The main processes mentioned above are shown in the following figure. They are also further explained in the next sections.

Figure XVII
Continuous improvement process

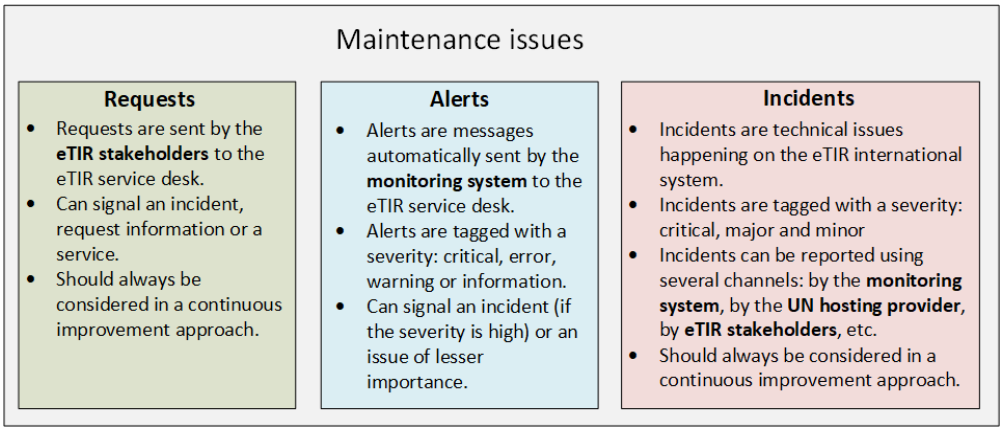


3. Issue management

182. In maintenance, there are three different types of issues that have their own characteristics and that are handled using specific procedures. The following figure describes these three types of issues.

[33] See en.wikipedia.org/wiki/PDCA

Figure XVIII
Types of maintenance issues



183. Requests are further described in the section related to the eTIR service desk. Alerts are further described in the section related to monitoring management. Incidents are further described in the section related to incident management.

4. eTIR service desk

184. The eTIR service desk is the single point of contact (SPOC) for eTIR stakeholders to raise any request related to the eTIR system. It is possible to do so by sending messages to its email address (etir@un.org) or through the "contact us" form of the eTIR web site.[34] The eTIR service desk is composed of the IT experts and subject matter experts of the TIR Convention of ECE.

185. Requests received by the eTIR service desk are dispatched by a (Tier-1) service desk agent to the appropriate (Tier-2) expert, depending on the nature of the request. Requests that signal an incident or a technical issue are dealt with as a priority.

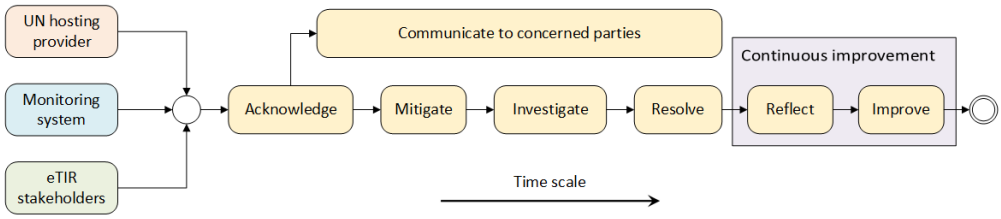
186. In the context of the interconnection projects, the eTIR service desk assists the eTIR stakeholders in connecting their information systems to the eTIR international system. These projects are closer to the development processes and, during the project initiation stage, the eTIR stakeholders define the best ways of communicating with the eTIR service desk to get information and raise any request. Given the limited resources of the eTIR service desk, the scope of its assistance is limited to providing information and guiding the experts of the eTIR stakeholders in their interconnection projects. For instance, the eTIR service desk cannot directly perform changes into the information systems of the eTIR stakeholders to connect them to the eTIR international system.

5. Incident management

187. Incidents are generally technical issues with significant consequences that need to be addressed by the eTIR service desk as a priority. Incidents have a severity associated to them which drive the type of answer that need to be given: critical, major and minor. The whole process to manage them is inspired from the Information Technology Infrastructure Library (ITIL) service management methodology and is described in the following diagram. Its stages are further described hereunder.

[34] See etir.org/contact-us

Figure XIX
Incident management process



(a) **Acknowledge**: after having been alerted, the IT experts confirm the incident (not a false positive) and ongoing (not already solved). They define its scope (the affected components), its severity and the list of concerned parties. From that point, all actions are logged to be further analysed during the "Reflect" stage;

(b) **Communicate to concerned parties**: transparent communication to the concerned parties about the incident is essential so that information can be given of the estimated time needed to resolve the issue, as this can drive decisions of the parties to apply specific measures (e.g. fallback procedures). The IT experts decide on the content and frequency of the communication until the incident is resolved (step (e));

(c) **Mitigate**: if possible, mitigation measures are applied in order to either decrease the severity of the issue, or to temporarily resolve it;

(d) **Investigate**: the IT experts take the time needed to comprehensively investigate the incident and determine its root cause(s);

(e) **Resolve**: after the investigation, the root cause(s) are addressed and corrected and the incident must be considered as resolved before moving to the next stage;

(f) **Reflect**: the IT experts gather all data and actions performed so far to resolve the incident and have a "blameless post-mortem" meeting. The goal is to take a deeper look at the incident and figure out what happened, why it happened, how the IT experts responded, and what can be done to prevent repeating this type of incident as well as improve future responses; while assuming the responsibility of the incident collectively. An "incident report" is prepared during this meeting and follow-up actions are defined and planned accordingly;

(g) **Improve**: the follow-up actions that have been defined in both previous stages are progressively selected from the eTIR backlog as per their priority, and performed to improve the software, processes, documentation and other assets so that the probability of having the same incident happening is decreased.

188. During the "Reflect" stage, the IT experts prepare an incident report which is then stored in the knowledge management system (KMS) for institutional memory. This report contains the following information about the incident (including date and time when applicable): severity, description, services affected, how it was notified and by who, response actions performed to mitigate and then solve it, communication sent and received, results of the investigation, list of root causes, lessons learned from the blameless port-mortem and list of follow up actions.

189. With this process, the IT experts wish to achieve the following benefits: the prevention of similar incidents (or at least decreasing their probability to happen), an improvement on the average time to resolve incidents, a further reduction of downtime of the eTIR international system and an overall improved experience for the eTIR stakeholders.

6. Incidents managed by the United Nations hosting provider

190. As displayed in figure X, incidents can be reported to the eTIR service desk by the United Nations hosting provider which hosts the eTIR international system. A service level agreement (SLA) is signed with this provider to ensure a 24/7 support of the eTIR international system. SOPs are prepared by the IT experts for the officers of the United Nations hosting provider so that they can respond to specific types of incidents.

191. When an incident occurs, the officers of the United Nations hosting provider are notified by alerts sent by the monitoring system and they respond using these SOPs. If the response resolves the incident, they notify the eTIR service desk, for further investigation, mentioning that the incident is closed. If the response does not resolve the incident, they escalate it by contacting the eTIR service desk as displayed in figure X, using various communication ways and procedures depending on the severity of the incident.

7. Backup and restore management

192. Backup and restore management represents the strategy and related procedures put in place to ensure that copies of eTIR related data are frequently made and can quickly be restored, in case of a data loss event. Indeed, data can be lost during several types of events, inter alia: the malfunction of a server, fire in the data centre or a cyberattack. The preparation of the SOPs are the joint responsibility of the United Nations hosting provider and ECE and they are mentioned in the SLA.

193. Data stored in all eTIR storage locations (the eTIR database, the eTIR logs and the eTIR documents) is backed up twice per day. This backed up data is securely stored in, at least, one other location than the primary site to avoid being destroyed if this site sustains a disaster. It is also not accessible from the same network to avoid being compromised by a cyberattack of type ransomware. Only the most recent and complete backups are kept and old backups are erased.

194. Finally, it should take no more than 6 hours to store the last backup in case of data loss event. Tests are regularly performed with the United Nations hosting provider to ensure that this requirement can be met.

8. Monitoring management

195. The act of monitoring an information system includes the collection of information produced by this system and the ability to produce alerts when certain events are met, so that (automated or manual) actions can be performed as answers to these events. Monitoring a system allows to proactively detect any issue that may turn into a failure and may eventually impact the availability of the system. The ability to quickly respond to these early warnings usually decreases the impact of failures and can also sometimes prevent them altogether.

196. A monitoring system is provided by the United Nations hosting provider and it is configured in collaboration with ECE to observe the resources and performance of the virtual servers, as well as the availability and performance of the various services of the eTIR international system. In particular, the list of indicators that are tracked by the monitoring system include the following metrics: CPU usage, RAM usage, percentage of disk used, processes, availability of the services, system's response time and resource usage of applications.

197. Alerts are configured to be triggered when specific thresholds are exceeded. Alerts have a severity associated to them which drives the type of answer that needs to be given: critical, error, warning and information. Several types of answers can be activated depending on their configuration: an automated process can be executed or a communication can be sent to one or more persons (by email, SMS or phone call) to notify them of the alert so they can take action as soon as possible. The first persons notified are usually the officers of the United Nations hosting provider so they can take immediate actions by applying the SOPs prepared for such occasions. Alerts can also be sent to the eTIR service desk, depending on the urgency and importance of the issue. A comprehensive list of indicators, thresholds, alerts and related answers are jointly documented by the United Nations hosting provider and ECE, and are mentioned in the SLA.

198. In addition to tracking metrics gathered from the virtual servers and processes, the monitoring system also exploits data contained in the eTIR logs. This information, also referred to as telemetry, logged by the eTIR international system, provides valuable data which can be used to detect any potential immediate issue with the system. It also informs about the performance of the system and gives an indication to the IT experts on related trends. It is important to track this data to ensure that target values set in the technical requirements of the eTIR international system are met.

199. Finally, it is important to take into consideration one drawback usually associated with the practice of monitoring. When initially configured, thresholds and alerts can lead to false positives or, on the contrary, they can "miss" issues that should have been detected. For this reason, the practice of continuous improvement is particularly relevant and the configuration of the monitoring system should regularly be reviewed to be optimized.

9. Patch management

200. A patch is a set of changes to a piece of software designed to update, correct, or improve it. This includes fixing security vulnerabilities and other defects. In this document, patch management refers to the strategy and related procedures put in place to ensure that all software components, including the operating systems of the underlying servers, are regularly patched to correct any recently found issues.

201. It is especially important to remove security vulnerabilities that are uncovered in existing versions of all software by the cybersecurity community. Regularly applying patches from authorized and verified sources is one of the most effective way to protect the eTIR international system from cyberattacks (see the part dedicated to the security of the eTIR system).

202. SOPs are prepared and applied on a regular basis (at least every three months) to patch the following software components, if a patch is available: underlying operating systems, frameworks and libraries (e.g. Java virtual machine) and database management systems. Regular schedules do not prevent applying important patches as needed, most of the time for security reasons. Software components are patched by the United Nations hosting provider and by ECE, depending on the responsibilities detailed in the SLA.

10. Upgrade management

203. An upgrade is generally the replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its functionalities. In this document, upgrade management refers to the strategy and related procedures put in place to ensure that technical debt is regularly addressed and will not grow over time (see the maintainability requirements of the eTIR international system). Upgrade management differs from patch management as upgrades are new versions of software which need to be carefully tested to detect and address potential issues before they can be applied.

204. Replacing the hardware and associated firmware is the responsibility of the United Nations hosting provider. Regarding software, the responsibilities are shared between the United Nations hosting provider, which needs to plan and perform the upgrades of all software components under its purview (e.g. virtual server farm system, operating systems of the virtual servers), and ECE which needs to plan and perform the upgrades of all software components of the eTIR international system.

205. At least once per trimester, the latest versions of the underlying programming language, frameworks and libraries used to build the eTIR international system are checked. The IT experts then regularly review and document the various advantages and disadvantages to migrate a software component to one of its new versions. The following criteria are taken into consideration to decide when to plan such a migration: end of support date of the currently used version, maturity of the new version as assessed by the IT community, potential benefits regarding security and additional features.

206. When the decision is taken to migrate a software component to a new version, an internal project is launched and its associated tasks are included into the eTIR backlog to be prioritized and considered in the usual development by iteration approach. The objectives of this type of project are the following: comprehensively test the new version of the software component to detect any issues that may arise in the context of the eTIR international system, correct any major issue found, possibly take advantage of the new features brought by the new version to improve the eTIR international system, further test and validate on the UAT environment before eventually deploying a new version of the eTIR international system on the PRD environment.

IV. Security of the eTIR system

207. This part describes all aspects of the eTIR system related to information security, in particular the objectives and requirements, and the corresponding measures and controls put in place to achieve them. Information security is one of the guiding principles selected for the development of the eTIR international system because of its importance in modern information systems and ECE wishes to properly address this endeavour. The goal is to define a comprehensive baseline embracing all relevant aspects on information security, which should be regularly reviewed and updated by TIB.

208. Information security covers not only software, but all domains that can influence the security of a system. As a result, this part will mention aspects related to the following domains: security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations and software development security.

209. As underlined in the previous part, describing the technical aspects of the eTIR international system, the level of details of the following sections depends on the aspects being described and not all information may be provided for security reasons.

A. Security objectives and principles

1. Information classification and security policies

210. The starting point of any discussion related to information security is to determine the sensitivity of the information managed in the information systems. In the United Nations, these aspects are governed by the Secretary-General's bulletin on "Information sensitivity, classification and handling".[35] Data exchanged by the stakeholders of the eTIR system, as well as data exchanged by the users of the International TIR Data Bank (ITDB) is classified as "confidential", as defined in section 2 of the bulletin.

211. This classification level is then used, and referred to, in other documents of the United Nations to specify the rules, guidelines and best practices to apply. In particular, the Office of Information and Communications Technology (OICT) issues policies, including several ones related to information security, that specify different security controls, depending on the classification level.[36] The eTIR technical specifications comply with these policies by specifying security measures and controls that are as stringent as the ones required in the policies when managing confidential information.

2. Security objectives

212. Information security is based on the following three main fundamental objectives[37]:

- **Integrity** states that information retains its veracity and is intentionally modified by authorized subjects only.
- **Availability** states that authorized subjects are granted timely and uninterrupted access to information.
- **Confidentiality** states that information is not disclosed to unauthorized subjects.

213. These three fundamental objectives, along with their associated requirements when developing information systems, determine the main information security aspects, as depicted in the following figure.

[35] See document ST/SGB/2007/6.
[36] See a list of the policies on iseek.un.org/nyc/department/policies
[37] Comprehensive definitions for these three terms are provided in the technical glossary.

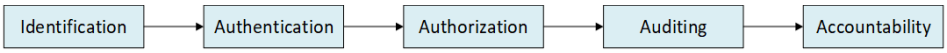
Figure XX
Fundamental objectives of information security

214. In the case of the eTIR system, the requirements of these three objectives are high. Indeed, as data is classified as confidential, its confidentiality should be ensured by adequate security controls. Because the eTIR system is to be used by multiple stakeholders, for the international transport of goods following the eTIR procedure, it should always be available to its users. Finally, the integrity of data transferred between the eTIR stakeholders should be preserved, so that all stakeholders can trust it and also in order to achieve non-repudiation.

3. How to achieve accountability and non-repudiation

215. In addition to integrity, availability and confidentiality, it is important to describe how a subject[38] authenticates itself in a system and how its actions can lead to accountability and non-repudiation. This materializes as a sequence of five processes which are listed in the following figure and described hereafter.

Figure XXI
From identification to accountability



(a) **Identification** is the process by which a subject claims an identity and accountability is initiated. A subject must provide an identity to a system to be authenticated. Providing an identity might, for example, entail entering a username or positioning a finger in the proximity of a scanning device. A core principle of authentication is that all subjects must have unique identities;

(b) **Authentication** is the process of verifying or testing that the claimed identity is valid. It requires subjects to provide additional information that corresponds to the identity they are claiming, like providing a password or a digital certificate. This process verifies the identity of a subject by comparing one or more factors against a database of valid identities, such as user accounts;

(c) **Authorization** is the process of granting access to a resource or object, based on the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. Only if the specific action is allowed, then the subject is authorized;

(d) **Auditing** is the programmatic means by which a subject's actions are tracked and recorded for the purpose of holding the subject accountable for their actions while authenticated in a system. It is also the process by which unauthorized or abnormal activities are detected by a system;

(d) **Accountability** is the process of holding subjects accountable for their actions. Effective accountability relies on the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the security services and mechanisms of auditing, authentication, and identification.

216. **Non-repudiation** is an important derived objective which ensures that a subject that triggers an activity or event cannot deny that he or she triggered it. It prevents a subject from

[38] A « subject » is to be understood here as an individual or an information system that tries to access another system.

claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event. This objective is important for the eTIR system, as information stored in the eTIR international system can be requested by contracting parties in case of claims.[39] By meeting both the objectives of accountability for the subjects and integrity of the data stored in the eTIR international system, the objective of non-repudiation is achieved.

4. Security principles

217. As for the guiding principles selected for the development of the eTIR international system, ECE also acknowledges and adopts the following principles which are recognized and widely used by the community of information security experts.

218. The first one is the principle of **due care** which, in the context of information security, refers to taking reasonable care to protect the assets of an organization on an ongoing basis. This requires a strong level of proactivity and the creation of a culture of security. Implementing the security concepts and procedures covered in this part, along with performing periodic security audits and reviews, demonstrates to the eTIR stakeholders that ECE exercises due diligence to maintain its due care effort.

219. The second one is the **principle of least privilege**, which requires that in a particular abstraction layer of a computing environment, every element (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.[40] This principle also applies for ECE staff members in charge of developing and operating the eTIR international system: permissions and accesses are selectively granted to them to perform their work and administrative controls are put in place to periodically review the list of permissions and to remove them if they are no longer needed. This comes in addition to outboarding procedures, which aim at removing all accesses from individuals (staff members, consultants, interns, etc.) that would no longer work for ECE. Finally, physical and technical access controls are also put in place to ensure that only authorized individuals have access to specific information and systems to perform their duties.

220. The third principle is **defence in depth**, which represents the concept in which multiple layers of security controls (defence) are placed throughout an information system. Its intent is to continue to provide adequate security in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security.[41] This principle is used on many occasions and, for example, in the eTIR international system by implementing several layers of validation for inputting data (received in the eTIR messages) to verify their quality and conformance with the eTIR specifications.

221. The fourth principle is the **separation of duties**, which represents the concept of having more than one person required to complete a task. In sensitive operations, the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.[42] For example, this principle is used in the development process of the eTIR international system, when another IT expert reviews the code of a first IT expert which has implemented and committed lines of code. It allows finding potential omissions and mistakes which can then be immediately corrected by the original submitter.

B. Security requirements

1. Previously mentioned technical requirements

222. As explained in the section above, information security covers a large spectrum of the non-functional (technical) requirements of an information system, as many of them play a role in one or more of the three main objectives: integrity, availability and confidentiality. In particular, the following requirements, already discussed in the previous part on the eTIR

[39] As per paragraph 3 of Article 12 of Annex 11 of the TIR Convention.
[40] See en.wikipedia.org/wiki/Principle_of_least_privilege.
[41] See en.wikipedia.org/wiki/Defense_in_depth_(computing).
[42] See en.wikipedia.org/wiki/Separation_of_duties.

international system, should be understood as playing a role in the information security component of the eTIR system:

- **Availability**, as one of the three main security objectives, is obviously one of the most important, and the IT experts should dedicate particular attention to this set of requirements: AV.1, AV.2, AV.3 and AV.4.
- **Backup**, with its two requirements (BK.1 and BK.2), is part of the availability objective, as the goal is to restore the access of information to authorized subjects in case of a data loss event.
- The first requirement of **capacity**, CP.1, is also part of the availability objective as the goal is to ensure that the eTIR international system can process, at all times, the messages sent by the eTIR stakeholders. The other requirements (CP.2, CP.3 and CP.4) also follow the same logic, to a lesser extent.
- All **configuration management** requirements (CM.1, CM.2, CM.3, CM.4 and CM.5) impact all three objectives (availability, integrity and confidentiality) as they characterize important aspects of the development and maintenance processes of the eTIR international system.
- **Data retention** requirements (RE.1 and RE.2) detail specific aspects of the availability objective by indicating how long data, exchanged in the eTIR system should be kept, and how to get access to it.
- **Disaster recovery** requirements (DR.1 and DR.2) are also obviously related to the availability objective as they tackle the specific case of restoring the eTIR international system in case of a disaster.
- **Fault tolerance** requirements (FT.1, FT.2, FT.3 and FT.4) which detail various technical fallback aspects of the eTIR international system, and which also impact the availability objective.
- The first two **maintainability requirements**, treating with technical debt (MT.1 and MT.2), are part of the preventive measures put in place to prevent future information security related problems with the eTIR international system.
- As for CP.1, the two **performance requirements** PE.2 and PE.3 are also part of the availability objective, as the goal is to ensure that the exchange of messages between the eTIR international system and another eTIR stakeholder can always be performed within a reasonable amount of time. Furthermore, the last two performance requirements (PE.4 and PE.5) are also part of preventive measures to anticipate a potential issue with the eTIR international system which could impact its availability.
- Most of the **reliability requirements** (RL.1, RL.2, RL.3, RL.5 and RL.7) are also mechanisms put in place to prevent, as much as possible, issues from occurring with the eTIR international system, which could impact its availability.

223. It is obvious that information security is a transversal, pervasive theme that cannot be treated in isolation and requires adopting a consistent approach to consider it in all stages of the software development lifecycle. The following non-functional (and not necessarily technical) requirements are specific to information security and are generally applicable to all components of the eTIR system: to the eTIR international system, to the information systems of all other eTIR stakeholders (including those put at the disposal of the holders to submit advance data) and to the network connections between all these systems. However, it is important to note that several of the following requirements may only apply to a subset of these components.

224. In the following sections, a “user account” is to be understood as an account uniquely identifying either an individual or an information system in another information system (which uses and manages these accounts).

2. Auditing

225. The following table contains the requirement related to the auditing process as mentioned in Figure XXI. While this requirement mainly applies to eTIR international

system, it is recommended for other information systems of the eTIR system to also conform to it.

Table 20
Auditing requirement

Identifier	*Description and objective*	*How to fulfil the requirement*
AU.1	All information sent to and received by the eTIR international system is linked to a user account and can be audited.	All messages transmitted sent to or received by the eTIR system are entirely logged, including the digital signature. These logs are then securely kept and maintained in the eTIR logs storage location and can be requested by customs authorities in case of claims.

3. Authentication

226. The following table lists the requirements related to the authentication process as mentioned in Figure XXI. Only the first one (AE.1) applies to the authentication of the eTIR stakeholders in the eTIR international system while the other requirements apply to the other information systems involved in the eTIR system.

Table 21
Authentication requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
AE.1	Select a strong authentication mechanism for the eTIR international system to prevent unauthorized access	The eTIR stakeholders who wish to access the web services of the eTIR international system should authenticate themselves using a digital certificate. The private key of this certificate should be securely stored by each and every eTIR stakeholder.
AE.2	Enable session lock after inactivity to protect the access to the user accounts.	For user accounts assigned to individuals only: when providing a user interface to access an information system (either on a web site or on a mobile application), a time limit of 15 minutes should be set to close the session if it becomes inactive.
AE.3	Manage passwords securely to prevent unauthorized access.	Password should be securely stored in databases using modern cryptographic hash functions. Passwords should comply with the best practices, including in terms of minimum length and complexity.
AE.4	Recommend multi-factor authentication for system access to protect user accounts.	When applicable, user accounts assigned to individuals should follow a multi-factor authentication using, for instance, a two factor approach with “something the user knows” (a password) and “something the user has” (a security card or a mobile phone).

4. Authorization

227. The following table lists the requirements related to the authorization process as mentioned in Figure XXI for the information systems involved in the eTIR system.

Table 22
Authorization requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
AO.1	Grant the minimum, sufficient access or privileges to prevent unauthorized access.	Any user account should be assigned the minimum access and permissions needed to get the information it is allowed to retrieve and to perform the operations it is allowed to accomplish.
AO.2	Employ role-based access controls (RBAC) to improve the	When applicable, user accounts should be granted access and permissions based on roles or groups. This is a sustainable way to manage access control lists as it is easy and less error prone to globally review and update the access and permissions to all

	maintenance of the user accounts.	members of a group than doing it for each and every user account.
AO.3	Revoke access upon termination of personnel appointments to prevent unauthorized access.	"Offboarding" procedures should be in place to remove access and permissions assigned to the user accounts of the individuals whose appointments are terminated. These user accounts should then be disabled.
AO.4	Review user accounts at least annually to prevent privilege creep.	A procedure should be in place to review, at least annually, all user accounts to verify and validate that the access and permissions assigned to them are accurate.

5. Awareness and training

228. It has been demonstrated several times already that humans are the weakest link in the information security chain. Therefore, it is vital to raise awareness and train in information security, its best practices and common threats, of the personnel that will be using information systems involved in the eTIR system. As humans are targeted by specific attacks like phishing, spear phishing and social engineering, it is important to emphasize these aspects. It is, therefore, recommended for all eTIR stakeholders to put in place similar processes.

229. The following table lists the requirements related to the processes put in place to raise the awareness and train all relevant personnel.

Table 23
Awareness and training requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
AW.1	Ensure all relevant personnel follow basic training courses on information security to raise their awareness.	Basic training courses on information security (including best practices and common threats) should be available to personnel using information systems involved in the eTIR system. Procedures should be in place to ensure that all personnel using information systems related to the eTIR system followed these training courses.
AW.2	Maintain records of participation in required training courses.	Records should be kept and managed to ensure that all personnel using information systems related to the eTIR system have followed basic training courses on information security. Ideally, following these training courses should be performed on a regular basis (for instance, every three years).

6. Confidentiality

230. Information exchanged with and stored in the eTIR system is confidential. As a result, controls should be put in place to ensure that data is protected against unauthorized access while it is exchanged with the eTIR international system (data in motion) and when it is stored inside it (data at rest). The following table lists the confidentiality requirements of the eTIR system.

Table 24
Confidentiality requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
CO.1	Information transferred between the information systems of the eTIR system remains confidential.	All messages exchanged between all information systems of the eTIR system are encrypted using protocols and encryption mechanisms that are considered secured by the international InfoSec community.[43] The eTIR technical specifications should specify them and this list should be revisited on a regular basis to remove the mechanisms that are no longer considered as secured and replace them with more secured ones

[43] The term «InfoSec» is a contraction of «Information Security». The internatioanl InfoSec community contains national agencies specialized in information security that issue regular publications on the subject, as well as IT experts and researchers specialized in this field.

CO.2	Access to the information stored in the eTIR international system is restricted.	Information recorded in the three storage locations of the eTIR international system (eTIR database, eTIR documents and eTIR logs) is restricted to authorized user accounts only. These storage locations are located in a secured environment protected by physical and software security controls.

7. Identification

231. The following table contains the requirement related to the identification process as mentioned in Figure XXI for the information systems involved in the eTIR system.

Table 25
Identification requirement

Identifier	*Description and objective*	*How to fulfil the requirement*
ID.1	Uniquely identify an individual or an information system with a user account to be able to hold it accountable for its actions.	Any user account should be assigned and linked to an individual and not to a group of users (in the case of persons) or to a unique information system (in the case of systems). The same information system should have different identities depending on the environment used (development, user acceptance testing and production).

8. Integrity

232. The integrity of the information exchanged and stored in the eTIR international system needs to be preserved. As a result, controls should be put in place to ensure that data is protected against any change, irrespectively of the nature of the change: error while transferring data, human error, misconfiguration or cyberattacks. The following table lists the integrity requirements of the eTIR international system.

Table 26
Integrity requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
IN.1	The integrity of the information transferred between the information systems of the eTIR international system remains intact.	All messages sent to or received by the eTIR international system are digitally signed by the sender. The recipient validates the electronic signature of the message upon reception and discards it if it is not valid.
IN.2	The integrity of the information stored in the eTIR system remains intact.	All messages sent to or received by the eTIR international system are entirely logged, including the digital signature. These logs are then securely kept and maintained in the eTIR logs storage location to which access is restricted.

9. Nodes security

233. As defined in the architecture part, a node represents any device, physical or virtual, which hosts or interacts with programs or information composing the eTIR international system. Nodes can be the virtual servers hosting the various software components of the eTIR international system or the devices part of the network infrastructure, like firewalls, routers, proxies, reverse proxies, or dedicates information security devices (IDS, IPS, etc.). The following table lists the security requirements of the nodes of the eTIR international system.

Table 27
Nodes security requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
NS.1	Securely configure virtual servers, containers or pods to	Ensure that all recommendations related to information security from the vendors of the operating system are applied. The credentials of the service accounts to these servers are securely

	prevent unauthorized access.	kept in a password management system and available only to authorized personnel. When applicable, activate the software firewall and implement default-deny, least-privilege policies.
NS.2	Securely configure network infrastructure devices to prevent unauthorized access.	Implement default-deny, least-privilege policies on network devices like firewalls. Ensure all recommendations from the vendors are applied. Maintain accurate documentation on network interconnections and devices configuration. These actions are performed by the hosting entity.
NS.3	Isolate trusted networks containing sensitive data from non-trusted networks to prevent unauthorized access.	Apply the best practices in terms of network infrastructure design by separating servers into different security zones, based on their role and on the sensitivity of the information stored on them. Implement IP whitelisting to deny access to the eTIR international system by default, except for the a given list of external servers (eTIR stakeholders). These actions are performed by the hosting entity.
NS.4	Monitor events on the nodes to detect potential security issues.	Enable logging for the nodes that support it and direct the metrics to the monitoring system. Restrict log access to authorized staff members only. Protect log data from unauthorized changes and operational problems. Set up automated alerts based on rules, including logging failures.

10. Non-repudiation

234. The following table lists the non-repudiation requirements of the eTIR international system.

Table 28
Non-repudiation requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
NR.1	eTIR stakeholders are accountable for the messages they send to the eTIR international system.	When they send messages to the eTIR international system, eTIR stakeholders should be uniquely identified and authenticated by signing the messages with their electronic signature. In addition, requirement AU.1 should be met.
NR.2	The integrity of the message sent by the eTIR stakeholders to the eTIR international system is ensured.	Requirements IN.1 and IN.2 should be met.
NR.3	The eTIR international system can continue to validate messages stored in the eTIR logs up to the duration mentioned in the data retention period.	As digital certificates should be periodically renewed, a key management system should be implemented to keep the old digital certificates of all eTIR stakeholders to be able to continue to authenticate and verify the integrity of messages exchanged in the past that are kept in the eTIR logs.

11. Physical security

235. This section groups the main requirements and related measures put in place to ensure that the premises, buildings and infrastructures of the United Nations organization hosting the eTIR international system are physically secured. The following table lists the physical security requirements of the buildings and infrastructures hosting the eTIR international system.

Table 29
Physical security requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
PS.1	The data centre hosting the eTIR international system should be immune to	The eTIR international system is hosted in a data centre located in one of the United Nations premises and operated by United Nations staff members only. It is, therefore,

	search, requisition or confiscation to protect the information stored in it.	protected by the dispositions of the Convention on the Privileges and Immunities of the United Nations.
PS.2	The data centre hosting the eTIR international system should be sufficiently protected to prevent intrusions and disasters.	United Nations premises are surrounded by a closed protective perimeter, guarded by security officers 24/7 and covered by a video surveillance system. Access to these premises is restricted to registered people wearing electronic badges. Access to the data centre is restricted to a handful of authorized IT staff members only. Appropriate fire detection and suppression systems are set up in the data centre.

12. Secure coding and application security

236. Secure coding is the practice of developing software in a way that guards against the accidental introduction of security vulnerabilities. Defects and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities. The following table lists the secure coding and application security requirements of the eTIR international system.

Table 30
Secure coding and application security requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
SC.1	Define security requirements in the early stages of the Software Development Life Cycle (SDLC)[44] to lower the costs and decrease the number of security issues.	Consider all aspects related to security for each and every feature when designing and adding it to the eTIR backlog. Always validate input data before processing it. Design and integrate validation tests focused on security (evil stories). Execute proper error handling to always leave the system in a stable state. Ensure all security related events are properly logged with the right severity. Regularly review the source code to remove unnecessary classes and functions; and to refactor portions of code.
SC.2	Separate the stages of the SDLC to prevent mixing different versions.	Use different environments with appropriate security controls and procedures for the stages of Development (DEV), Systems Integration and Testing (SIT), User Acceptance Testing (UAT) and Production (PRD).

13. Vulnerability management

237. Vulnerability management embeds the practices of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities. Vulnerability management is integral to computer security and network security, and includes vulnerability assessment. The following table lists the vulnerability management requirements of the eTIR international system.

Table 31
Vulnerability management requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
VU.1	Ensure the known vulnerabilities are patched to prevent potential security issues.	Update and patch nodes, including operating systems and middleware on a regular basis. Regularly upgrade to the latest stable versions of the third party dependencies of the software components. Regularly migrate to the latest versions of the components of the external systems (ITDB, mail system and non-repudiation system).
VU.2	Conduct vulnerability assessment and testing to prevent potential security issues.	Regularly scan nodes, systems and their components for known vulnerabilities. Conduct code security reviews (like penetration testing) to validate new versions of the eTIR international system.

[44] See en.wikipedia.org/wiki/Systems_development_life_cycle

VU.3	Ensure incidents are properly managed to prevent potential security issues.	Alerts raised from the monitoring system should be investigated based on their severity by following the appropriate procedures. The incident management process is followed for every incident which gives opportunities to learn, improve and perform follow up actions to help preventing further similar issues.

C. Security of the eTIR international system

1. Introduction

238. In addition to the previous parts of the eTIR technical specifications, this section complements various aspects of the security of the eTIR international system, so that contracting parties to the TIR Convention and the other eTIR stakeholders have a clear understanding on these features. This section elaborates on how ECE will meet several of the security requirements pertaining to the eTIR international system, as listed in the previous section. Being transparent about these aspects also provides an opportunity for all eTIR stakeholders to suggest proposals for improvement, with the ultimate objective to have a more secure eTIR system in the long term.

2. Information security awareness

239. It is important to understand that information security is like a chain, which is as strong as its weakest link. As individuals are part of this chain, no matter how many security devices or software barriers are also put in place in the chain, if the individuals do not have the knowledge and experience needed to understand the common threats and how to react, then the overall security of the system is at risk.

240. Information security awareness focuses on raising consciousness regarding potential risks of the rapidly evolving forms of cyberattacks which target human behaviour. As threats have matured and information has increased in value, attackers have also increased their capabilities and expanded to broader intentions, developed new attack methods and methodologies and are acting on more diverse motives. Attackers are more and more targeting (and successfully exploiting) individuals human behaviour to breach corporate networks and critical infrastructure systems. Targeted individuals who are unaware of the sensitivity of information and of the threats, may unknowingly circumvent traditional security controls and processes and enable a breach of the organization.

241. In order for efforts in this domain to be effective, it is not only important for the IT experts directly involved in the eTIR international system to be aware of information security, but also to all staff members of ECE. Indeed, as an example, any staff member opening a document infected by a malware (which would be attached to an email) could potentially open a back door for an attacker to breach the information security of the organization. For this reason, OICT has developed, in 2015, a set of three training courses on information security awareness (foundational, advanced and additional). It is mandatory for all staff members of the United Nations to complete the foundational training course, so that all personnel have the necessary knowledge and awareness of the good practices to adopt in case of a potential threat.

3. Legal aspects

242. The Convention on the Privileges and Immunities of the United Nations,[45] passed by the United Nations General Assembly on 13 February 1946 in New York, defines and specifies numerous provisions related to the status of the United Nations, its assets, and officials, in terms of the privileges and immunities that must be granted to them by its member states. In particular, as mentioned in Article 2, the premises of the United Nations are inviolable: its properties and assets, wherever located and by whomever held, are immune to search, requisition, confiscation, expropriation and any other form of interference.

[45] See treaties.un.org/doc/treaties/1946/12/19461214%2010-17%20pm/ch_iii_1p.pdf

243. In practice, this means that only security officers of the United Nations Department of Safety and Security (UNDSS) are in charge of the safety and security of the properties and assets located in the premises of the United Nations. Police and any other security forces of the hosting country cannot enter the United Nations premises unless having been allowed to do so by security officers of UNDSS. Therefore, as long as the eTIR international system is hosted in a data centre located in the premises of the United Nations, it is covered by the privileges and immunities described above.

4. Physical security

244. Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm (such as espionage, theft, or terrorist attacks). Physical security involves the use of multiple layers of interdependent systems that can include video surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, deterrent systems, fire protection, and other systems designed to protect persons and property. In the organizations of the United Nations, this aspect of security is ensured by UNDSS providing professional safety and security services to enable the United Nations to deliver its programmes globally. This section only touches upon the main aspects of physical security for obvious security reasons.

245. United Nations premises are surrounded by a closed protective perimeter (walls, fences, security bollards, etc.) which prevents any individual or vehicle to enter without having received an authorization. The premises are guarded by security officers 24 hours per day, all days of the year The premises are covered by a video surveillance system continuously monitored by the security guards and recorded for potential future investigations. Access to the premises is restricted to registered people wearing electronic badges issued by UNDSS. Access to the data centre is restricted to a handful of authorized IT staff members only and the location of the data centre inside the premises is not publicly known.

246. Also, regarding safety, fire detection and suppression systems are set up generally in the premises and in particular in the data centre, and security exercises are carried out several times per year.

5. United Nations hosting entity

247. When it comes to the United Nations hosting entity (hereafter the hosting entity), several aspects related to security have already been described in previous parts of the eTIR technical specifications:

- In the detailed architecture of the eTIR international system, the systems architecture describes how the usage of a virtual server farm infrastructure, as well as a load balancer can play a role to design a system free of any Single Point of Failure (SPOF);
- In the technical requirements, the important role that the hosting entity plays is detailed in the requirements related to availability, backup and, especially, fault tolerance, which describes several characteristics of its data centre;
- In the maintenance processes, the hosting entity also plays an important role in areas like incident management, backup and restore, monitoring, patch and upgrade management.

248. The hosting entity is also in charge of the general security of its data centre, its networks and infrastructure (as mentioned in the nodes security requirements above). Furthermore, in order to demonstrate its maturity and commitment in information security, the hosting entity should ideally hold a renowned certificate like ISO/IEC 27001:2013.

249. Finally, since regular changes have to be applied by the hosting entity of its networks, infrastructure and nodes (network, security or server appliances), a well-defined change management process should be in place to test, prioritize, authorize and deploy changes in a controlled and effective manner. The communication about these changes with the clients of the hosting entity should be appropriate, timely and possible unavoidable downtime periods should be discussed in advance to find alternative solutions or at least inform the eTIR

stakeholders concerned. Ideally, ECE should have a say when authorizing and planning changes that have an impact on the eTIR international system or on ITDB, possibly by having a seat in the Change Advisory Board (CAB) of the hosting entity.

6. Software security

250. One of the objectives of DevOps (also coined with the term DevSecOps), is about "leaning security left", meaning to think about information security very early in the development process, rather than addressing it at the end, when changes made to a piece of software are more expensive. ECE has adopted the following practices and design decisions to pursue this objective:

- **Security requirements as features**: security and compliance are not separate processes that happen at the end of the development of software but are "shifted left" in the development process and are integrated in the same eTIR backlog as any other features.
- **Validations mechanisms**: all input data contained in the eTIR messages is validated at several levels to ensure its correctness, alignment with the specifications and pertinence. These mechanisms include, inter alia: a specific validation layer per request message, a validation layer using the related XSD file and integrity constraints in the eTIR database. In addition, the automated validation tests include testing malformed input data, null or blank values, values too long and specific evil stories.[46]
- **Error handling**: errors occurring during the execution of the eTIR international system should be properly handled to always leave the system in a correct state. All errors should be logged for further study and should be tested, if possible, using automated tests to ensure that the error handling mechanism is behaving as expected.
- **Vulnerability check**: A static code analysis tool is used to regularly check the source code for bad practices that could create potential security vulnerabilities. Also, as numerous software libraries are used nowadays in any piece of software, a dependency checking tool is used to check the versions of the libraries against a database of known vulnerabilities to flag important upgrades to be performed in order to patch these vulnerabilities.
- **Protect the development toolset**: it is important to keep all the tools and internal knowledge used and produced by the IT experts secured. First and foremost, the Version Control System (VCS), keeping the source code of the eTIR international system and of all related utilities. Then, the internal documentation kept in the Knowledge Management System (KMS) and in the issue tracking system. Finally, the Continuous Integration (CI) pipeline and all related tools needed in the various development processes, including the documentation for the eTIR stakeholders (like the technical guides).
- **Telemetry**: it is the process of recording the behaviour of the eTIR international system. The IT experts should design and implement it to generate and log metrics that can then be analysed to – inter alia – prevent potential (security) incidents. Such metrics would include the following: eTIR message validation success/failures, use of invalid digital signatures, exceptions raised by the system, performance of the processing of the messages, etc. All these metrics generated and output in the eTIR logs are then exploited and can be displayed in graphics to study variations and potentially trigger alerts, based on specific patterns that may signal a potential cyberattack.
- **Continuous technology watch**: the IT experts should regularly engage in training activities to keep abreast of evolving technologies and techniques in securing software, including studying the latest products from entities like OWASP.[47]

[46] «Evil stories» follow a similar approach as «user stories» and describe scenarios that an attacker would follow to breach the security of the eTIR international system.

[47] The Open Web Application Security Project® (OWASP) is a non-profit foundation that works to improve the security of software. See owasp.org

7. Security assessments

251. An IT security assessment is an explicit study to locate IT security vulnerabilities and risks. It can be performed internally by ECE, by information security experts from the United Nations or by external specialized companies mandated by ECE. The goal of a security assessment is to ensure that necessary security controls are integrated into the design and implementation of the eTIR international system. A properly completed security assessment should provide documentation outlining any security gaps and suggestions on how to address them. The results of security assessments are confidential.

252. The IT experts should strive to engage in performing regular security assessments and should ideally automate some of these assessments to be executed frequently. For instance, the type of security assessment called "vulnerability assessment", whose purpose is to scan the source code and software components used to build and run the eTIR international system, should be automated using specific tools and executed regularly. This way, potential vulnerabilities can immediately be detected (and remediated) when patching and upgrading software components.

253. Whenever a new major version of the eTIR international system is developed, a more thorough security assessment should be performed, either by information security experts from the United Nations, or by an external specialized company, mandated by ECE. This security assessment would, most likely, take the shape of a "penetration testing" where the testers take the role of attackers and try to find and exploit security vulnerabilities in the eTIR international system. Depending on various factors, this exercise can be of type black, grey or white boxes. The colour indicates how much information a tester has at his or her disposal. A black-box tester has no prior knowledge about the system that will be targeted. With a grey-box assessment, the level of access and information is not complete, but only partly provided and available. Finally, a white-box assessment stands for a test in which the tester has full access to the source code, network diagrams and other relevant information.

D. Security of exchanges with the eTIR international system

1. Introduction

254. This section describes the security model and controls that should be followed by the different eTIR stakeholders while exchanging messages with the eTIR international system. The security model is designed to meet the requirements in terms of confidentiality, integrity and non-repudiation listed above. The technical details and versions of the algorithms and protocols mentioned should be regularly reviewed by TIB to ensure that the objectives and exigencies, in terms of security, are continuously covered.

2. Confidentiality

255. As the eTIR messages are exchanged between the eTIR stakeholders over the internet, these exchanges need to be encrypted to prevent any third party from being able to read the messages exchanged and, thus, get access to this confidential information. The HyperText Transfer Protocol Secure (HTTPS), used to access the eTIR international system endpoints, is an extension of the HyperText Transfer Protocol (HTTP) where communication is encrypted using Transport Layer Security (TLS), a cryptographic protocol designed to provide communications security over public networks like the internet. The bidirectional encryption of the exchanges using HTTPS/TLS between a client and server protects against eavesdropping and tampering of the communication. The version of TLS to be used should be either version 1.2 or 1.3.[48]

256. As the encryption of the exchanges between the eTIR stakeholders uses the HTTPS/TLS protocols to ensure the confidentiality of the communication, there is no need to either set up Virtual Private Networks (VPN) or to perform a double encryption at the eTIR messages level using the techniques available using SOAP.

[48] Versions 1.0 and 1.1 of the TLS have been deprecated in 2020 as they are no longer considered as secure

3. Integrity and non-repudiation

257. Messages exchanged with the eTIR international system must be authenticated and their integrity must be ensured to achieve non-repudiation. This is accomplished using the concept of electronic signatures. Definitions of electronic signatures vary depending on the applicable jurisdiction and a common denominator is therefore set in the context of the eTIR specifications. This common denominator states that electronic signatures should achieve the following requirements:

- The signatory can be uniquely identified and linked to the electronic signature;
- The signatory must have sole control of the private key that was used to create the electronic signature;
- The electronic signature must be capable of identifying if its accompanying data has been tampered with after the message was signed.

258. From a technical point of view, this is achieved using a digital certificate (also known as public key certificate) following the X.509 standard,[49] version 3. Each eTIR stakeholder wishing to interconnect his or her information systems with the eTIR international system should be issued a X.509 certificate from a trusted Certificate Authority (CA)[50]. The X.509 certificate, which uniquely identifies the eTIR stakeholder is used to sign the eTIR messages. This way of implementing electronic signature not only ensures the identity of the sender but also guarantees that the message content has not been tampered during the transmission, thus ensuring integrity.

259. In order for the X.509 certificates to ensure a high level of security, they should be created using the following parameters:

- The validity period should be, maximally, one year;
- The public key algorithm should be RSA with a key length of 4096 bits;
- The signature algorithm should be one of the following: SHA-256 with RSA, SHA-384 with RSA or SHA-512 with RSA (recommended).
- The “Country (C)”, “State Name (ST)” and “Locality Name (L)” parameters should reflect where the eTIR stakeholder is located. Only the “State Name (ST)” parameter is optional;
- The “Email (E)” parameter should provide the email address of the IT service desk of the eTIR stakeholder;
- The “Common Name (CN)” and the “Organization Name (O)” parameters should hold the same value which is the full name of the eTIR stakeholder as an entity/organization.

260. As the X.509 certificates have a limited validity period, they will be regularly replaced with new ones and the exchange of new certificates should be properly planned between ECE and the other eTIR stakeholders to prevent any interruption of service. Also, since data exchanged and stored with the eTIR international system should be kept for ten years,[51] ECE will keep all previous X.509 certificates of the eTIR stakeholders in a secure location to be able to verify the electronic signature of old eTIR messages, in case ECE is requested by the competent authorities of contracting parties to provide all data related to a TIR transport.

4. Whitelisting

261. As the eTIR stakeholders who wish to communicate with the eTIR international system need to complete an interconnection project, ECE keeps an accurate and up-to-date list of these companies/entities/organizations. This approach allows to put an extremely effective security measure in place: whitelisting. The eTIR international system is configured not to be accessible by anyone from the internet, except by a restricted list of IP addresses

[49] See itu.int/ITU-T/recommendations/rec.aspx?rec=X.509
[50] Also known as Trusted Third Parties
[51] As per Article 12 of Annex 11 of the TIR Convention

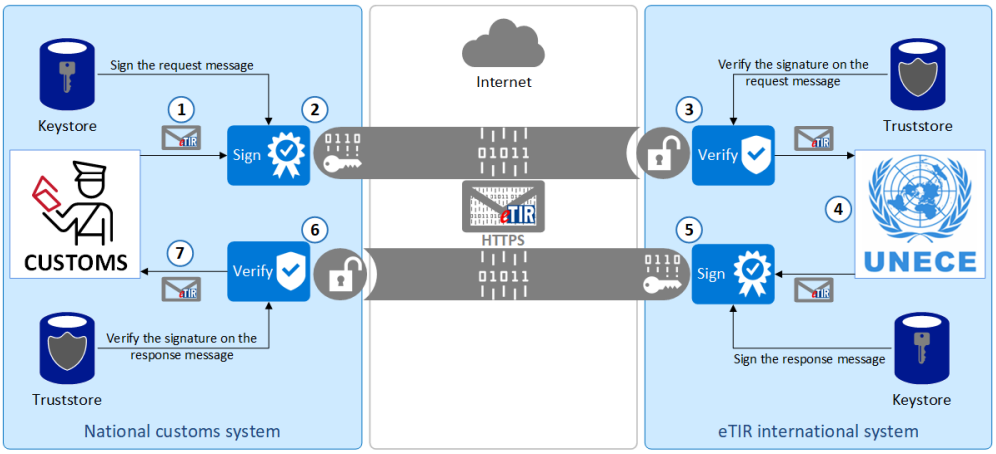
which correspond to the main servers of the eTIR stakeholders which have completed their interconnection projects. This approach drastically reduces the potentiality of cyberattacks to the eTIR international system, including "denial of service" and trying to "spoof"[52] an eTIR stakeholder.

262. During the course of the interconnection project, ECE requests the IP addresses of the servers of the eTIR stakeholder which will connect with the eTIR international system, both on the UAT and PRD environments, and liaises with the United Nations hosting entity to configure the network appliances accordingly.

5. eTIR security model

263. The eTIR security model combines all security aspects mentioned above to provide a highly secured approach. The following figure illustrates how this security model works with an eTIR message being sent from a national customs systems to the eTIR international system using web services. The same approach applies when communicating in the same way with guarantee chains and holders.

Figure XXII
eTIR security model



264. In the example above, as a preliminary step, the X.509 certificate of the national customs system is installed in the eTIR international system truststore and the eTIR international system X.509 certificate is installed in the national customs system truststore. This mandatory initial step allows the validation of the digital signatures that are transferred as security tokens in all eTIR messages exchanged in the context of the eTIR procedure. The procedure below describes the steps numbered in the figure above and explains how a request message is sent by the national customs system to the eTIR international system, and how the related response is sent back:

(1) The national customs system generates a request message to be sent to the eTIR international system web service;

(2) The request message is signed with the private key of the national customs system X.509 certificate. It is then encrypted using HTTPS/TLS and sent over the internet. The connection can be successfully established, as the national customs system is whitelisted by the network appliances of the eTIR international system;

(3) The eTIR international system receives the request message, decrypts it, verifies the signature of the message using the public key of the national customs system X.509 certificate to authenticate it and to confirm its integrity. The full message including its digital signature is then securely stored in the eTIR logs;

(4) The eTIR international system processes the request message and generates a response message in return;

[52] A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

(5) The response message is signed with the private key of the eTIR international system X.509 certificate and securely stored in the eTIR logs. It is then encrypted using HTTPS/TLS and sent over the internet;

(6) The national customs system receives the response message, decrypts it, and verifies the signature of the message using the public key of the eTIR international system X.509 certificate to authenticate it and to confirm its integrity;

(7) The national customs system finally processes the response message.

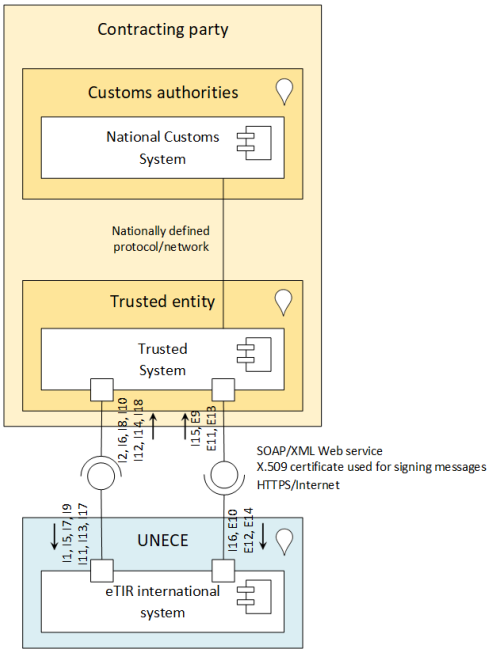
265. The completion of this whole process illustrates the implementation of the various security measures described in the sections above to achieve the requirements of confidentiality, integrity and non-repudiation.

6. Alternative security models

266. National legislations and regulations in contracting parties may prevent their customs authorities from interconnecting their national customs systems to the eTIR international system by following the specifications described above. In that case, an alternative security model should be designed and agreed between the IT experts of ECE and of the customs authorities. It should also be reviewed and approved by TIB. This alternative security model should meet the same security requirements in terms of confidentiality, integrity and non-repudiation, to be accepted.

267. A possible alternative security model is described below in case the customs authorities of a contracting party are required to use specific encryption algorithms or other technical aspects that would prevent them to initiate a direct connection with the eTIR international system. This security model is similar to the one described above, except that another entity under the contracting party government jurisdiction would play the role of a proxy between the eTIR international system and the national customs system. This entity should be trusted by the customs authorities and the technical details of the connection between this entity and the national customs system would be the sole decision of the contracting party and should be described in the eTIR technical specifications. The following figure shows the architecture of this alternative security model.

Figure XXIII
An alternative security model



268. This alternative security model still requires that the communication between the eTIR international system and the trusted system be done using HTTPS/TLS and signing the eTIR messages using X.509 certificates that would comply with the technical specifications described above. On the contracting party's end, the X.509 certificate signing messages sent by the customs authorities could belong to the customs authorities or to the trusted entity, at the decision of the customs authorities.

7. Common threats and mitigation measures

269. A table is provided in annex VI.D of the present document to summarize all security measures and controls that should be put in place for the eTIR international system, and to give an overview for the contracting parties to the TIR Convention on how these measures will mitigate the risks posed by common security threats.

E. Security of exchanges between other eTIR stakeholders

1. Introduction

270. The previous section describes the technical specifications of the exchanges between any eTIR stakeholders and the eTIR international system using web services. These eTIR stakeholders include customs authorities, guarantee chains and holders and all of them should have undergone an interconnection project. In addition to these types of exchanges, holders can also exchange information (advance TIR data and advance amendment data) directly with the customs authorities.[53] This section describes the technical specifications of this latter type of communication only.

2. Authentication of the holder

271. Each contracting party shall publish a list of all electronic means by which advance TIR data and advance amendment data can be submitted by the holder to the customs authorities.[54] The authentication mechanisms used by these electronic means should uniquely identify the holder and should feature security measures and controls which provide sufficient assurance that the authentication mechanism is secure, in accordance with national laws.[55] In

[53] As per paragraph 2 of Article 6 of Annex 11 of the TIR Convention
[54] As per paragraph 4 of Article 6 of Annex 11 of the TIR Convention
[55] As per paragraph 1 of Article 7 of Annex 11 of the TIR Convention

order to be specific and transparent about this important point, each contracting party shall publish the list of authentication mechanisms used by these electronic means.[56] Finally, it is also important to mention that the authentication of the holder performed in this context shall be recognized by the other contracting parties along the itinerary of the TIR transport following the eTIR procedure.[57]

272. The authentication of the holder exchanging data directly with the customs authorities is, therefore, a matter of national concern and is not governed by the eTIR specifications. In order to assist and facilitate the decision of contracting parties about this important topic, the next sections provide guidelines and best practices of authentication mechanisms that do not rely on electronic signatures.

3. Multi-Factor Authentication (MFA)

273. MFA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two (or more) pieces of evidence (or factors) to an authentication mechanism. These two (or more) pieces should belong to at least two different classes among the three that exist:

- **Knowledge**: something only the user knows, like a password or a personal identification number (PIN) code;
- **Possession**: something only the user has, like a smartphone with a configured software-based authenticator, a smartcard or a security card (as used in ITDB);
- **Inherence**: something only the user is, like fingerprints, voice prints, retina patterns, iris patterns or face shapes.

274. It is recommended to use MFA in the authentication mechanism as it provides a high level of assurance that the user is indeed who he or she claims to be.

4. Password strength

275. Most of the web sites and web applications rely on passwords (either solely or as part of an MFA) to authenticate their users. It is important to understand and comply with the minimum requirements in terms of password length and complexity as effective attacks can crack passwords that would not be compliant in seconds. All passwords should conform to the following specifications:

- At least 12 characters long; more than 14 characters is better;
- Different from the default (initial) password;
- Not be the same as the username;
- Composed of, at least, three of the following character classes:
    - upper case letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - lower case letters: abcdefghijklmnopqrstuvwxyz
    - numbers: 0123456789
    - punctuation marks: !@#$%^&*()+=\`{}[]:";'< >?,./)
- Not be based on words found in dictionaries of any language or based on simple patterns such as “aaabbb”, “qwerty”, “zyxwvuts”, “123321”, etc.

276. In addition, users should be encouraged not to base their password on any personal information that is easily available to potential adversaries, such as names of family members, pets, friends, co-workers, birthdays, addresses, phone numbers, etc. And, finally, passwords should be regularly changed, at least once per year.

[56] As per paragraph 3 of Article 7 of Annex 11 of the TIR Convention

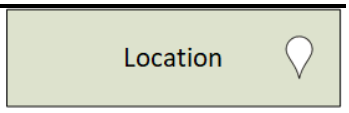
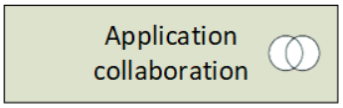
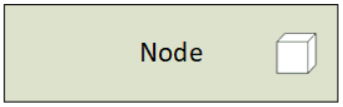
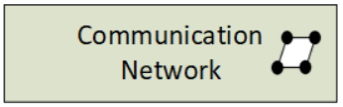
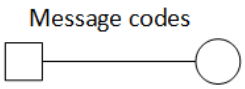
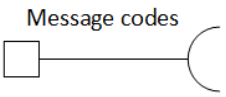
[57] As per Article 8 of Annex 11 of the TIR Convention

V. Annexes

A. Diagram notation

277. The ArchiMate (ArchiMate® 3.0.1 Specification. See: pubs.opengroup.org/architecture/archimate3-doc/) notation is used to represent the various architectural viewpoints in the diagrams of this document. Only the ArchiMate concepts used in the diagrams are described in the table below. Note that the colours used in the background of the shapes represent different actors or systems, not a particular ArchiMate concept.

Table 32
ArchiMate diagram notation

Concept	*Description*	*Symbol*
Location	A location is used to model the places where other concepts are located.	
Application Component	A modular, deployable, and replaceable part of a software system that encapsulates its behaviour and data and exposes these through a set of interfaces.	
Application collaboration	**An application collaboration represents an aggregate of two or more application components that work together to perform collective application behaviour.**	
Node	**A node represents a computational or physical resource that hosts, manipulates, or interacts with other computational or physical resources.**	
Communication Network	**A communication network represents a set of structures that connects computer systems or other electronic devices for transmission, routing, and reception of data.**	
Interface provided	Represents a point of access where application services are made available to another application component. The codes of the messages provided by this interface can be listed on top of the symbol.	
Interface required	Represents a need to connect to application services that are made available by another application component. The codes of the messages sent back through this interface can be listed on top of the symbol.	

B. Technical glossary

278. This annex provides in the following table the definition of all technical terms that are used in the eTIR technical specifications.

Table 33
Technical glossary

Term	*Definition*
Application programming interface	An application programming interface (API) is a software interface which is used for accessing an application or a service from a program.

Term	*Definition*
Asymmetric encryption	A cryptographic system that uses two keys: a public key known to everyone and a private (or secret) key only known to the owner of the key pair. For example, when Alice wants to send a secured message to Bob, she uses Bob's public key to encrypt the message. Bob then uses his private key to decrypt it. RSA is an example of asymmetric algorithm.
Authentication	The process of verifying or testing that the claimed identity is valid. Authentication requires subjects to provide additional information that corresponds to the identity they are claiming. The most common form of authentication is using a password (this includes the password variations of personal identification numbers - PINs - and passphrases). Authentication verifies the identity of the subject by comparing one or more factors against the database of valid identities (that is, user accounts).
Certification authority	A certification authority (CA), is a recognized entity that holds a trusted position because the certificate that it issues binds the identity of a person or business to the public and private key pair (asymmetric cryptography) that are used to secure most transactions transmitted over the internet. For example, when a business or person wants to use these technologies, they request to a CA to issue them a certificate. The CA collects information about the person or business that it will certify before issuing the certificate.
Confidentiality	Confidentiality is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources. The goal of confidentiality protection is to prevent or minimize unauthorized access to data. Confidentiality focuses on security measures ensuring that no one other than the intended recipient of a message receives it or is able to read it. Confidentiality protection provides a means for authorized users to access and interact with resources, but it actively prevents unauthorized users from doing so.
Defect	The IT literature usually makes a distinction between the terms "bug" and "defect". Indeed, a "bug" is the result of a coding error and a "defect" is a deviation from the requirements. In the context of this document, only the term "defect" is used and encompasses both meanings.
Digital certificate	In cryptography, a digital certificate (or, simply, certificate in this document), is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.
Digital signature	A digital code (chain of characters) that can be attached to an electronically transmitted message and that has two distinct goals: 1) Digitally signed messages assure the recipient that the message truly came from the claimed sender. They enforce non-repudiation (that is, they preclude the sender from later claiming that the message is a forgery) and 2) Digitally signed messages assure the recipient that the message was not altered while in transit between the sender and recipient (its integrity was preserved). This protects against both malicious modification (a third party altering the meaning of the message) and unintentional modification (because of faults in the communications process, such as electrical interference).
Environments	During its lifecycle, a piece of software is developed and maintained on several environments that serve different purposes. Some of them are used for development, some others for testing and, finally, another one, the production environment, is used to operate the system when it is "live" and is available as a service to its end users
Error	An error is a severe validation failure, which will cause the message to be rejected.
Front-end web servers	A web server that receives request messages from the web service endpoints of the eTIR international system (or sends request messages to web service endpoints of other eTIR stakeholders).
Git	Git is a version control system for tracking changes in any set of files, usually used for coordinating work among programmers collaboratively developing source code during software development. Its objectives include optimized performance, data integrity, and support for distributed, non-linear workflows.
Hash	A hash value (or simply hash), also called a message digest, is a value generated from a text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that any other text can produce the same hash value.
Integrity	Integrity is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data. It ensures that data remains correct, unaltered, and preserved. Properly implemented integrity protection provides a means for authorized changes while

Term	*Definition*
	protecting against intended and malicious unauthorized activities (such as viruses and intrusions) as well as mistakes made by authorized users (such as mistakes or oversights).
Java	Java is a class-based, object-oriented programming language that is designed to have as few implementation dependencies as possible. It is a general-purpose programming language intended to let application developers write once, run anywhere, meaning that compiled Java code can run on all platforms that support Java without the need for recompilation.
Keystore	A keystore is a database used to store the certificates of the information systems of the owner of the keystore, and may include the certificates of trusted parties (truststore), for use by a program. Through its keystore, an entity can authenticate itself to other parties and may authenticate other parties as well.
Load balancer	The load balancer is a software component that distributes a set of tasks over a set of resources (server nodes), with the aim of making their overall processing more efficient.
Non-repudiation	Non-repudiation ensures that the subject of an activity or who caused an event cannot deny that the event occurred. Non-repudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event. It is made possible through identification, authentication, authorization, accountability, and auditing. Non-repudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanisms.
OASIS	The Organization for the Advancement of Structured Information Standards (OASIS) is a non-profit, international consortium whose goal is to promote the adoption of product-independent standards.
Public key infrastructure	A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage asymmetric encryption.
Receiver	In the context of this document, the "receiver" is the information system of the eTIR stakeholder which receives an eTIR message sent by another stakeholder, and processes it.
RSA	The RSA algorithm was invented by Ronald L. Rivest, Adi Shamir, and Leonard Adleman in 1977. It is an asymmetric encryption algorithm using two different keys with a mathematic relationship to each other. The public key and private keys are carefully generated using the RSA algorithm; they can be used to encrypt information or sign it.
Sender	In the context of this document, the "sender" is the information system of the eTIR stakeholder which generates and sends an eTIR message to another eTIR stakeholder.
Single point of failure	A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.
SOAP	Simple Object Access Protocol (SOAP) is a messaging protocol specification for exchanging information in the implementation of web services. It is an XML-based protocol consisting of three parts: • an envelope, which defines the message structure (a header and a body) and how to process it; • a set of encoding rules for expressing instances of application-defined data types; • a convention for representing procedure calls and responses.
Software entropy	The second law of thermodynamics, in principle, states that a closed system's disorder cannot be reduced, it can only remain unchanged or increase. A measure of this disorder is entropy. According to studies, this law also seems plausible for software systems: as a system is modified, its disorder, or entropy, tends to increase. This is known as software entropy. The process of code refactoring can result in stepwise reductions in software entropy.
Token	A token (sometimes called a security token) is an object that controls access to a digital asset. Traditionally, this term has been used to describe a hardware authenticator, a small device used to create a one-time password that the owner types in a login screen along with an ID and a PIN. However, in the context of web services and with the emerging need for devices and processes to authenticate to each other over open networks, the term token has been expanded to include software mechanisms too. A token may be an X.509 certificate, that associates an identity to a public key for example.
Total cost of ownership	The total cost of ownership (TCO) represents the total amount of money that the owner of an information system had to spend during the life cycle of the latter. All costs (direct and indirect) are taken into account.
Truststore	A truststore is a keystore file that contains the certificates from other parties that you expect to communicate with, or from Certificate Authorities that you trust, to identify other parties.

Term	*Definition*
Virtual server farm	A virtual server farm is a networking environment that employs multiple application and infrastructure servers running on two or more physical servers using a server virtualization program. This architecture offers several benefits, including server consolidation, redundancy, failover, high availability and optimized resource utilization.
Web service	Virtual service/function exposed over a network (private or internet) allowing for system to system communication using messages following a strict format. Machine-to-machine is another term to define this type of communication.
Web Services Security	The Web Services Security (WS-Security) specification describes enhancements to SOAP 1.1 that increase the protection (integrity) and confidentiality of the messages. These enhancements include functionality to secure SOAP messages through XML digital signature, confidentiality through XML encryption, and credential propagation through security tokens (e.g. X.509 token).
Web Service Description Language	Web Service Description Language (WSDL) is an XML-based interface description language that is used for describing the functionality offered by a web service.
X.509 certificate	X.509 is a common format for digital certificates, that is widely used on internet with the TLS protocol. An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number and validity interval. It is defined in the request for comments (RFC) document 5280.[58]
X.509 token	The X.509 token represents the digital signature generated using the X.509 certificate of the sender, and which will be used to authenticate the entity sending the message. It is therefore part of the message itself, in the header section of the SOAP envelope.
XML	XML stands for eXtensible Markup Language which is a language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is used by SOAP to encode messages sent by web services.
XML signature	The XML signature specification is a joint effort between W3C and IETF. XML signatures provide integrity, message authentication and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.
XML Schema Definition	XML Schema Definition (XSD) is a W3C recommendation that describes how the elements in an XML document are structured and formatted.

C. Analysis to determine the needs in terms of capacity and scalability of the eTIR international system

1. Introduction

279. This annex analyses, based on existing data (February 2021) and on experience acquired during the development of the eTIR international system, the requirements in terms of throughput of messages and volume of data to be handled by the eTIR international system.

280. Since the eTIR international system is not yet in operation, this analysis cannot use real data and, therefore, takes a cautious approach by always considering worst case scenarios and providing estimates based on maxima rather than averages. When the eTIR international system starts to be used in production, ECE will revisit this analysis to provide better forecasts in terms of capacity requirements for the coming years and link them with the number of eGuarantees sold.

2. Analysis on the number of messages

281. Based on the most recent statistics on sales of TIR Carnets (and on the number of eGuarantees issued in the context of the eTIR pilot projects), the following table shows an aggregated view of the past statistics, combined with estimates of sales of TIR Carnets and eGuarantees for the next five years.

Table 34
Statistics and forecast of the sales of TIR Carnets and eGuarantees

[58] See tools.ietf.org/html/rfc5280

Year	*Number of TIR Carnet sold*	*Number of eGuarantees sold*	*Increase of the number of eGuarantees sold per year*
2001	2 707 950	*N/A*	*N/A*
2002	3 095 200	*N/A*	*N/A*
2003	3 298 000	*N/A*	*N/A*
2004	3 211 050	*N/A*	*N/A*
2005	3 240 650	*N/A*	*N/A*
2006	3 599 850	*N/A*	*N/A*
2007	3 076 250	*N/A*	*N/A*
2008	3 253 800	*N/A*	*N/A*
2009	2 230 400	*N/A*	*N/A*
2010	2 822 200	*N/A*	*N/A*
2011	3 074 500	*N/A*	*N/A*
2012	3 158 300	*N/A*	*N/A*
2013	2 920 150	*N/A*	*N/A*
2014	1 945 050	*N/A*	*N/A*
2015	1 500 450	(eTIR pilot) 5	*N/A*
2016	1 223 400	(eTIR pilot) 59	*N/A*
2017	1 154 650	(eTIR pilot) 82	*N/A*
2018	1 020 650	(eTIR pilot) 81	*N/A*
2019	858 100	(eTIR pilot) 78	*N/A*
2020	679 300	(eTIR pilot) 2	*N/A*
2021	(estimate) 600 000	(eTIR pilot) 63, (estimate) 5 000	*N/A*
2022	(estimate) 550 000	(estimate) 15 000	200%
2023	(estimate) 500 000	(estimate) 60 000	300%
2024	(estimate) 450 000	(estimate) 200 000	233%
2025	(estimate) 400 000	(estimate) 400 000	100%
2026	(estimate) 300 000	(estimate) 700 000	75%

282. In order to calculate the estimates on eGuarantees sold, the following factors were taken into consideration:

(a) The number of countries that have initiated interconnection projects between their national customs system and the eTIR international system during 2020;

(b) The number of countries that have already expressed an interest to perform this interconnection for which projects should most likely start during 2021;

(c) The numbers of TIR Carnets issued in recent years along the corridors involving those contracting parties that have launched interconnection projects or will soon do so;

(d) The efforts undertaken or interest expressed by Regional Economic Organizations in order to prepare proofs of concept to interconnect their customs union system with the eTIR international system and the possible dates for these interconnections;

(e) The results of the "study on the reasons for the decline in the number of TIR Carnets used" document (hereafter "the study") prepared by the TIR Executive Board (TIRExB) in 2020 and, especially, the trends related to the TIR Carnets sales;

(f) The efforts that ECE and the international organization will make in the coming years in order to attract more countries and markets (intermodal, postal) and expand the TIR Convention to new regions as described in the study;

(g) Neither any sensitivity analysis nor other scientific forecasting method was used, so far, to prepare such estimations.

283. The estimates on the increase in the sale of eGuarantees on a yearly basis show that, after the first years of adoption, the long term increase in percentage tends to become linear and could remain that way if the number of contracting parties to the TIR Convention connected to the eTIR international system continue to increase as well. We should, therefore, design the eTIR international system so that it can easily scale with a steady yearly increase of 100% of TIR transports following the eTIR procedure.

284. The number of messages sent and received per TIR transport depends on several criteria: the number of TIR operations, the number of pre-declaration messages (advance TIR data, advance amendment data and cancel advance data messages) sent by the holder, the number of uses of the query mechanism, the number of times that seals are changed, whether any incident or accident occurs during the TIR transport, etc. The following table shows several scenarios of TIR transports and details, for each of them, the maximum number of messages received and sent by the eTIR international system (if the holder sends the pre-declaration messages via the eTIR international system) as well as the number of request messages only.

Table 35
Messages received and sent by the eTIR international system by scenarios

Number of TIR Operations	*Messages received and sent for the TIR operations*	*Messages received and sent for the pre-declaration*	*Total number of messages per scenario*	*Number of request messages only, per scenario*
2	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 2, (E7/E8) x 9, (E5/E6) x 9, (I5/I6) x 2	E9/E10	64	21
3	E1/E2, I1/I2, I7/I8, (I15/I16) x 2, (I9/I10, I11/I12, I13/I14) x 3, (E7/E8) x 12, (E5/E6) x 12, (I5/I6) x 3	E9/E10	88	28
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E11/E12	110	36
4	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 5, (I9/I10, I11/I12, I13/I14) x 4, (E7/E8) x 14, (E5/E6) x 14, (I5/I6) x 4	E9/E10, E13/E14, E9/E10, E11/E12, E13/E14, E11/E12	118	40
5	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 7, (I9/I10, I11/I12, I13/I14) x 5, (E7/E8) x 17, (E5/E6) x 17, (I5/I6) x 5	E9/E10, E11/E12, E11/E12	136	44
6	E1/E2, I1/I2, (I7/I8) x 2, (I15/I16) x 9, (I9/I10, I11/I12, I13/I14) x 6, (E7/E8) x 20, (E5/E6) x 20, (I5/I6) x 6	E9/E10, E11/E12, E11/E12	160	51
7	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 15, (I9/I10, I11/I12, I13/I14) x 7, (E7/E8) x 24, (E5/E6) x 24, (I5/I6) x 7	E9/E10, E11/E12, E11/E12, E11/E12	198	61
8	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 18, (I9/I10, I11/I12, I13/I14) x 8, (E7/E8) x 27, (E5/E6) x 27, (I5/I6) x 8	E9/E10, E11/E12, E11/E12, E11/E12	224	68
9	E1/E2, I1/I2, (I7/I8) x 3, (I15/I16) x 21, (I9/I10, I11/I12, I13/I14) x 9, (E7/E8) x 30, (E5/E6) x 30, (I5/I6) x 9	E9/E10, E11/E12, E11/E12, E11/E12	250	75
10	E1/E2, I1/I2, (I7/I8) x 4, (I15/I16) x 30, (I9/I10, I11/I12, I13/I14) x 10, (E7/E8) x 34, (E5/E6) x 34, (I5/I6) x 10	E9/E10, E11/E12, E11/E12, E11/E12, E11/E12	292	85

285. In 2020, IRU reported the following sales[59]: 4,300 TIR Carnets of 4 vouchers (0.6%), 544,200 TIR Carnets of 6 vouchers (80%), 131,050 TIR Carnets of 14 vouchers (19.3%) and 0 TIR Carnets of 20 vouchers. Therefore, most of the TIR transports performed on that year had 3 TIR operations (6 vouchers). Given the previous table, and while taking a cautious approach with regard to the capacity of the eTIR international system, we will consider that the average total number of messages exchanged per TIR transport is 120 and that the average number of request messages is 40.

286. We will also assume that the average number of messages exchanged per TIR transport will also increase by 5% per year. This assumption is supported by the fact that more contracting parties will be connected to the eTIR international system over time, therefore increasing the possibilities for longer TIR transports following the eTIR procedure. Finally, new versions of the eTIR specifications could also contribute to this increase.

287. The following table gives estimates of the number of messages that the eTIR international system could send and receive, and should, therefore, be able to support, over the next years.

Table 36
Estimated number of messages to be supported by the eTIR international system

Year	*A. Estimated number of eGuarantees sold*	*B. Estimated average number of all messages per TIR transport*	*C. Estimated average number of all messages per year in millions (A x B)*	*D. Estimated average number of requests messages per TIR transport*	*E. Estimated average number of request messages per year in millions (A x D)*
2021	5 000	130	0.65	40	0.20
2022	15 000	137	2.06	42	0.63
2023	60 000	143	8.58	44	2.64
2024	200 000	150	30.00	46	9.20
2025	400 000	158	63.20	49	19.60
2026	700 000	166	116.20	51	35.70

288. We can then formulate, as a hypothesis, that the maximum number of messages would be between five and ten times the average number of messages. We can then produce the following two tables: one for the maximum number of messages received and sent by the eTIR international system and another for the maximum number of request messages received, both of them per minute.

Table 37
Estimated maximum number of messages received and sent

Year	*A. Estimated average number of all messages per year in millions*	*B. Estimated average number of all messages per minute (A / (365 x 24 x 60))*	*Estimated lower bound of maximum number of all messages per minute (B x 5)*	*Estimated upper bound of maximum number of all messages per minute (B x 10)*
2021	0.65	1.24	6.2	12.4
2022	2.06	3.92	20.0	39.2
2023	8.58	16.32	81.6	163.2
2024	30.00	57.23	286.2	572.3
2025	63.20	120.57	602.9	1 205.7
2026	116.20	221.69	1 108.5	2 216.9

Table 38
Estimated maximum number of request messages received

Year	*A. Estimated average number of request*	*B. Estimated average number of request*	*Estimated lower bound of maximum number of*	*Estimated upper bound of maximum number of*

[59] See Informal document WP.30/AC.2 (2021) No.5

	messages per year in millions	*messages per minute (A / (365 x 24 x 60))*	*request messages per minute (B x 5)*	*request messages per minute (B x 10)*
2021	0.20	0.38	1.9	3.8
2022	0.63	1.20	6.0	12.0
2023	2.64	5.02	25.1	50.2
2024	9.20	17.50	87.5	175.0
2025	19.60	37.29	186.5	372.9
2026	35.70	67.92	339.6	679.2

3. Analysis on the throughput of messages

289. The throughput of messages to be supported by the eTIR international system is defined as the number of request messages to be received and processed for a given unit of time. Based on the previous analysis, the average and the upper bound of the maximum number of request messages per minute, are selected.

Table 39
Estimated average and maximum requirements for the throughput of messages

Year	*Estimated average number of request messages per minute*	*Estimated maximum number of request messages per minute*
2021	0.38	3.8
2022	1.20	12.0
2023	5.02	50.2
2024	17.50	175.0
2025	37.29	372.9
2026	67.92	679.2

4. Analysis on the volume of data

290. In addition to the estimates on the throughput of messages that would need to be supported by the eTIR international system, it is also important to take into consideration the factor of the size of these messages and the total volume of data that would need to be exchanged, processed and recorded by the eTIR international system.

291. Based on the experience acquired during the development of the eTIR international system, the size of 70% of the messages is under 10 KB, the size of 25% of the messages is between 11KB and 50 KB and the size of the remaining 5% of the messages is between 51KB and 20 MB (the maximum size allowed). We assume that 5% of the messages would embed additional documents (which significantly increases the size of the message).

292. Therefore, we can assume that the average size of a message would be (90% x 5KB) + (9% x 25 KB) + (1% x 5 MB) = 57 KB. Building on previous results, we can deduce an estimate on the maximum total volume of data that would need to be handled by the eTIR international system and, in particular, to be stored in the eTIR logs.

Table 40
Estimated maximum volume of data to be stored in the eTIR logs

Year	*A. Estimated upper bound of maximum number of all messages per minute*	*B. Estimated maximum volume of data per minute in MB (A x 0.057)*	*C. Estimated maximum volume of data per year in TB (B x 60 x 24 x 365)*
2021	12.4	0.7	0.371
2022	39.2	2.2	1.174
2023	163.2	9.3	4.889
2024	572.3	32.6	17.146
2025	1 205.7	68.7	36.121

2026	2 216.9	126.4	66.417

293. Only a small subset of this volume is stored in the eTIR database. First, only the request messages are processed and recorded in this storage location. Then, the additional documents are not stored in the database, so we can remove the 1% largest messages, which gives the following new average size for a message: (91% x 5KB) + (9% x 25 KB) = 6.8 KB. Then, in each message, its header is not stored in the database and only the values of the body of the message are stored, which represent between 3% and 10% of the size of the message, therefore a maximum of 0.68 KB.

Table 41
Estimated maximum volume of data to be stored in the eTIR database

Year	*A. Estimated upper bound of maximum number of request messages per minute*	*B. Estimated maximum volume of data per minute in KB (A x 0.68)*	*C. Estimated maximum volume of data per year in GB (B x 60 x 24 x 365)*
2021	3.8	2.6	1.36
2022	12.0	8.2	4.29
2023	50.2	34.1	17.94
2024	175.0	119.0	62.55
2025	372.9	253.6	133.28
2026	679.2	461.9	242.75

294. Documents embedded in the messages are stored separately, in the eTIR documents system. As for the eTIR database, only the request messages are considered. Based on previous assumptions, we can, therefore, only keep the 1% largest messages holding embedded documents, which gives the following new average size for a message: 1% x 5 MB = 50 KB. Similarly, we can, therefore, infer an estimate on the maximum total volume of data that would need to be stored in the eTIR documents.

Table 42
Estimated maximum volume of data to be stored in the eTIR documents

Year	*A. Estimated upper bound of maximum number of request messages per minute*	*B. Estimated maximum volume of data per minute in MB (A x 0.05)*	*C. Estimated maximum volume of data per year in TB (B x 60 x 24 x 365)*
2021	3.8	0.2	0.100
2022	12.0	0.6	0.315
2023	50.2	2.5	1.319
2024	175.0	8.8	4.599
2025	372.9	18.6	9.800
2026	679.2	34.0	17.849

5. Conclusions

295. The estimations and forecasts in terms of throughput of messages and volume of data are only as good as the various assumptions are correct. Since the eTIR international system is not yet in operation, this analysis lacks actual data. For this reason, the eTIR international system should be designed while considering the capacity and scalability requirements for the first two years only, as there is a high probability that real data will adjust several assumptions, which will totally change the calculations and forecasts for the next years.

296. For this reason, it is strongly advised to perform this analysis again, six months after the eTIR international system is deployed in production in order to review the assumptions, redo the calculations and conclude with more reliable estimates and forecasts for the future needs in terms of capacity and scalability of the eTIR international system. Then, it will also be advised to review this analysis on a yearly basis to continuously refine it.

D. Error codes

297. This annex provides additional details on the error codes used in the context of the eTIR system.

298. The code list 99 defines all error codes that can be used in response messages to indicate problems that occurred while processing the corresponding request message. This code list is specific to the eTIR system and ECE has been continuously updating this list presented in the following table.

Table 43
Error code list (CL99)

Code	*Name*	*Description*
100	Invalid message	The message is invalid, and no additional details are available for this error
101	Missing parameter	A required parameter is missing in the message
102	Invalid domain value parameter	A parameter value is out of a defined list of acceptable values
103	Malformed date	A parameter holding a date cannot be properly converted
104	Not an integer	A numeric field is containing data that is not numeric
105	Parameter length exceeded	A String field contains too many characters
106	Invalid pattern	A String field does not match the pattern defined in the XML Schema Definition of the message
151	Condition C001 failure	The condition C001 is not fulfilled
152	Condition C002 failure	The condition C002 is not fulfilled
153	Condition C003 failure	The condition C003 is not satisfied
154	Condition C004 failure	The condition C004 is not fulfilled
155	Condition C005 failure	The condition C005 is not fulfilled
158	Condition C008 failure	The condition C008 is not fulfilled
168	Rule R008 failure	The rule R008 is not satisfied
200	Invalid state	The state of an internal object is invalid, and no additional details are available for this error
201	Guarantee not acceptable	The guarantee is not in a state that allows to accept it
203	Guarantee not cancellable	The guarantee is not in a state that allows to cancel it
204	Guarantee already registered	The guarantee has already been registered
205	Guarantee already cancelled	The guarantee is already cancelled or the request to cancel it has already been sent
210	Operation already started	The operation is already started
211	Operation already terminated	The operation has already been completed
212	Operation already discharged	The operation is already discharged
213	Operation not yet started	The operation is not yet started
214	Operation ID already registered	The “refusal to start” is an operation on its own and must have a unique operation ID
215	Operation sequence already registered	The “refusal to start” is an operation on its own and must have a unique operation sequence
216	Refusal to start not authorized	The "refusal to start" cannot be performed because of the current guarantee status or because it is the first operation for this transport
220	Declaration not yet received	The operation cannot be started because the declaration was not received
299	Duplicate message	The same message was already received from the same source
300	Invalid operation	An invalid operation was performed, and no additional details are available for this error
301	Guarantee not found	The guarantee was not found in the database
302	Guarantee chain not found	The guarantee chain was not found in the database
303	Guarantee type not found	The guarantee type was not found in the database
304	Customs office not found	This error code is not used in the eTIR specifications v4.3

Code	*Name*	*Description*
305	Country not found	The country was not found in the database
306	Control type not found	The control type was not found in the database
320	Holder/Guarantee mismatch	The holder id parameter and the guarantee reference parameter do not match what is recorded in the database
321	Holder not authorized	The holder is not authorized in the International TIR Data Bank (ITDB)
322	Holder not found	The holder is not found in ITDB
330	Guarantee chain not authorized	The guarantee chain is not authorized in the database
331	Guarantee chain/Guarantee mismatch	The guarantee chain code parameter and the guarantee reference parameter do not match what is recorded in the database
332	Guarantee type/Guarantee mismatch	The guarantee type parameter and the guarantee reference parameter do not match what is recorded in the database
400	eTIR problem	An internal error in the eTIR international system occurred and no additional details are available for this error

299. Not all error codes can be indicated in response messages and the following table displays which error codes can be referenced in response messages. This information is useful for the IT experts of the eTIR stakeholders to properly implement the follow-up actions when receiving specific error codes. This list is presented as it is at the time of the preparation of this document. Kindly check on the eTIR web site[60] to consult its latest version.

Table 44
List of possible error codes by response message

Error code	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
100	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
101	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
102	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
103	X			X	X	X	X				X				X		
104				X											X	X	X
105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
106	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
151				X											X		
152				X											X		
153				X											X		
154				X											X		
155				X											X		
158				X											X	X	
168				X													
200	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
201	X																
203												X					

[60] See www.etir.org/error-codes-list

Error code	*I2*	*I4*	*I6*	*I8*	*I10*	*I12*	*I14*	*I16*	*I18*	*I20*	*E2*	*E4*	*E6*	*E8*	*E10*	*E12*	*E14*
204											X						
205												X					
210					X												
211						X											
212							X										
213						X	X										
214					X	X	X		X								
215					X	X	X		X								
216									X								
220					X												
299					X	X	X										
300	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
301	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
302	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
303	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
304																	
305				X	X	X	X								X		
306					X	X	X										
320	X			X								X			X	X	X
321	X				X	X	X				X						
322	X	X	X		X	X	X				X		X				
330	X										X		X				
331	X											X					
332	X											X					
400	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

300. Finally, the following table gathers a set of recommended actions for consideration of the IT experts of the information system, when receiving a response message with one or more error codes.

Table 45
Recommended actions when receiving error codes

Code	*Name*	*Recommended actions*
100	Invalid message	Kindly check the message itself and its format as it is not recognized by the eTIR international system. **Kindly contact the eTIR service desk sending the content of the message communicated, the timestamps and the steps to reproduce this issue in order to address it.**

Code	*Name*	*Recommended actions*
101	Missing parameter	Kindly check the message parameters, in particular the parameters marked as mandatory in the message description section of this document, and make sure that all mandatory parameters are part of the message.
102	Invalid domain value parameter	Kindly check the coded parameter, its values and corresponding code lists. Make sure that each coded parameter is using one of the values of the corresponding code list.
103	Malformed date	Kindly check the date parameters and their format. Make sure that each date format has the format indicated, that the value follows the format/pattern and that the "formatCode" attribute is set to the correct value.
104	Not an integer	Kindly check the integer parameters. Make sure that each integer parameter has a value that can successfully be casted as an integer.
105	Parameter length exceeded	Kindly check the parameter value lengths. Make sure that each parameter length does not exceed the max length as defined in the documentation in the Format column.
106	Invalid pattern	Kindly check the pattern of the parameter value as it does not match the requirements set for this attribute in XML Schema Definition of the message.
151	Condition C001 failure	Kindly check the parameters constrained by the condition C001 and make sure their values respect the pseudo code of the condition.
152	Condition C002 failure	Kindly check the parameters constrained by the condition C002 and make sure their values respect the pseudo code of the condition.
153	Condition C003 failure	Kindly check the parameters constrained by the condition C003 and make sure their values respect the pseudo code of the condition.
154	Condition C004 failure	Kindly check the parameters constrained by the condition C004 and make sure their values respect the pseudo code of the condition.
155	Condition C005 failure	Kindly check the parameters constrained by the condition C005 and make sure their values respect the pseudo code of the condition.
158	Condition C008 failure	Kindly check the parameters constrained by the condition C008 and make sure their values respect the pseudo code of the condition.
168	Rule R008 failure	Kindly check the parameters constrained by rule R008 and make sure their values respect the conditions set by the rule.
200	Invalid state	Kindly check the state of the referred object (transport, guarantee, ...) and make sure it is consistent with the eTIR international system requested web service called.
201	Guarantee not acceptable	Kindly check the state of the guarantee you tried to accept, and make sure it is correct according to the workflow described in the guarantee state diagram.
203	Guarantee not cancellable	Kindly check the state of the guarantee you tried to cancel, and make sure it is correct according to the workflow described in the guarantee state diagram.
204	Guarantee already registered	Kindly check the state of the guarantee you tried to register as it seems to be already registered. You may use Query guarantee web service to check its existence in the eTIR international system.
205	Guarantee already cancelled	Kindly check the state of the guarantee you tried to register as it seems to be already cancelled. You may use Query guarantee web service to check its existence in the eTIR international system.
210	Operation already started	This message tries to start a TIR operation which has already been started. Make sure that this message is not a duplicate of a previously sent message and verify the values set in its parameters.
211	Operation already terminated	This message tries to terminate a TIR operation which has already been terminated. Make sure that this message is not a duplicate of a previously sent message and verify the values set in its parameters.
212	Operation already discharged	This message tries to discharge a TIR operation which has already been discharged. Make sure that this message is not a duplicate of a previously sent message and verify the values set in its parameters.
213	Operation not yet started	This message tries to perform an operation on a TIR operation which should be started and that is not yet started. Make sure that this message is sent in the right order and verify the values set in its parameters.
214	Operation ID already registered	Kindly check the message ID and that it is not conflicting with another operation ID.

Code	*Name*	*Recommended actions*
215	Operation sequence already registered	Kindly check the last operation's sequence number for this transport and increment it
216	Refusal to start not authorized	A refusal to start cannot take place if this the first operation registered or if the guarantee has not been accepted. Kindly check that your guarantee reference is also correct.
220	Declaration not yet received	This message tries to perform an operation whereas the Declaration has not yet been received. Make sure that this message is sent in the right order and verify the values set in its parameters.
299	Duplicate message	Kindly check the message already sent to this endpoint as this message has already been received by the eTIR international system.
300	Invalid operation	Kindly check the message content as it triggered a technical error in the eTIR international system but this one could not identify the source of the issue.
301	Guarantee not found	Kindly check the value of the guarantee reference ID in the message and make sure it matches the value received in previous messages.
302	Guarantee chain not found	Kindly check the value of the guarantee chain ID in the message and make sure it matches the value received in previous messages.
303	Guarantee type not found	Kindly check the value of the guarantee type in the message and make sure it belongs to the code list "Guarantee type code (eTIR)" (CL12), and that it matches the value received in previous messages.
304	Customs office not found	This error code is not used in the eTIR specifications v4.3.
305	Country not found	Kindly check the value of the country code in the message and make sure it matches the value received in previous messages and that it belongs to the code list "Country name code (ISO 3166-1-alpha-2)" (CL04).
306	Control type not found	Kindly check the value of the control type in the message and make sure it matches the value received in previous messages and that it belongs to the code list "Control type code (eTIR)" (CL25).
320	Holder/Guarantee mismatch	Kindly check the format and value of the TIR carnet holder in the message and make sure it matches the value received in previous messages. If it does, kindly check the existence of the holder and its status using either "I3 - Get holder information" message, ITDB dedicated web services or ITDB web application.
321	Holder not authorized	Kindly check the value of the TIR carnet holder in the message and make sure it matches the value received in previous messages. If it does, kindly check the status of the holder using either eTIR I3 message, ITDB web service or ITDB web application.
322	Holder not found	Kindly check the value of the TIR carnet holder in the message and make sure it matches the value received in previous messages. If it does, kindly double check the id of the holder using either eTIR I3 message, ITDB web service or ITDB web application.
330	Guarantee chain not authorized	Kindly check the value of the guarantee chain ID in the message and make sure it matches the value received in previous messages.
331	Guarantee chain/Guarantee mismatch	Kindly check the value of the guarantee chain ID in the message and make sure it matches the value received in previous messages.
332	Guarantee type/Guarantee mismatch	Kindly check the value of the guarantee type ID in the message and make sure it matches the value received in previous messages.
400	eTIR problem	**Kindly contact the eTIR service desk sending the content of the message communicated, the timestamps and the steps to reproduce this issue in order to address it.**

List of tables

Table 1 Applicable documents 5
Table 2 Definition of key terms 5
Table 3 Abbreviations 7
Table 4 Qualitative availability requirements 21
Table 5 Quantitative availability requirements 21
Table 6 Backup requirements 22
Table 7 Capacity and scalability requirements 22
Table 8 Configuration management requirements 23
Table 9 Data Retention requirements 24
Table 10 Disaster recovery requirements 25
Table 11 Fault tolerance requirements 25
Table 12 Internationalization and localization requirements 26
Table 13 Interoperability requirements 27
Table 14 Maintainability requirements 28
Table 15 Quantitative performance requirements 28
Table 16 Qualitative performance requirements 29
Table 17 Quantitative reliability requirements 30
Table 18 Qualitative reliability requirements 30
Table 19 Reusability requirement 31
Table 20 Auditing requirement 51
Table 21 Authentication requirements 51
Table 22 Authorization requirements 51
Table 23 Awareness and training requirements 52
Table 24 Confidentiality requirements 52
Table 25 Identification requirement 53
Table 26 Integrity requirements 53
Table 27 Nodes security requirements 53
Table 28 Non-repudiation requirements 54
Table 29 Physical security requirements 54
Table 30 Secure coding and application security requirements 55
Table 31 Vulnerability management requirements 55
Table 32 ArchiMate diagram notation 65
Table 33 Technical glossary 65
Table 34 Statistics and forecast of the sales of TIR Carnets and eGuarantees 68
Table 35 Messages received and sent by the eTIR international system by scenarios 70
Table 36 Estimated number of messages to be supported by the eTIR international system 71
Table 37 Estimated maximum number of messages received and sent 71
Table 38 Estimated maximum number of request messages received 71
Table 39 Estimated average and maximum requirements for the throughput of messages 72
Table 40 Estimated maximum volume of data to be stored in the eTIR logs 72
Table 41 Estimated maximum volume of data to be stored in the eTIR database 73
Table 42 Estimated maximum volume of data to be stored in the eTIR documents 73
Table 43 Error code list (CL99) 74
Table 44 List of possible error codes by response message 75
Table 45 Recommended actions when receiving error codes 76

List of Figures

Figure I Overall technical architecture of the eTIR system 11
Figure II Interactions between the national customs system and the customs offices 12
Figure III Interactions between the national customs system and the eTIR international system 13
Figure IV Interactions between the customs union system and the national customs systems 13
Figure V Possible interactions between the holder system and the national customs system 14
Figure VI Interactions between the holder system and the systems of a customs union 14
Figure VII Interactions between the holder system and the national customs system via the eTIR international system 15
Figure VIII Interactions between the guarantee chain system and the eTIR international system 16
Figure IX Interactions between the eTIR international system and the ITDB 16
Figure X Interfaces of the eTIR international system 17
Figure XI Software architecture of the eTIR international system 18
Figure XII Systems architecture of the eTIR international system 20
Figure XIII Development by iteration 33
Figure XIV Environments of the eTIR international system 37
Figure XV Issue lifecycle 39
Figure XVI Release management process 41
Figure XVII Continuous improvement process 42
Figure XVIII Types of maintenance issues 43
Figure XIX Incident management process 44
Figure XX Fundamental objectives of information security 48
Figure XXI From identification to accountability 48
Figure XXII eTIR security model 61
Figure XXIII An alternative security model 63