United Nations ECE/TRANS/WP.30/GE.1/2021/34

Economic and Social Council

Distr.: General
18 May 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

Security of the eTIR system*

Note by the secretariat

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 Terms of Reference (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 (20 May 2020) approved the establishment of WP.30/GE.1 until 2022, based on the ToR 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]

* This document was submitted late for processing since clearance in finalizing this document took longer than anticipated.

[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 UNECE www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09e.pdf and corrigendum www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09c1e.pdf

[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

2. The ToR 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 all aspects of the security of the eTIR system, which will be part of the eTIR technical specifications document.

II. Security of the eTIR system

4. 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.

5. 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.

6. 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

7. 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".[4] 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.

8. 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.[5] 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

9. Information security is based on the following three main fundamental objectives[6]:

[4] ST/SGB/2007/6

[5] See a list of the policies on iseek.un.org/nyc/department/policies

[6] Comprehensive definitions for these three terms are provided in the technical glossary.

- **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.

10. 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.

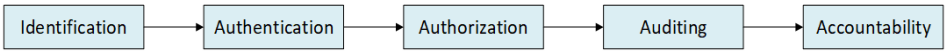
Figure I
Fundamental objectives of information security

11. 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

12. In addition to integrity, availability and confidentiality, it is important to describe how a subject[7] 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 II
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;

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

(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.

13. **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 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.[8] 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

14. 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.

15. 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.

16. 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.[9] 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.

17. 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.[10] 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.

18. 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

[8] As per paragraph 3 of Article 12 of Annex 11 of the TIR Convention

[9] See en.wikipedia.org/wiki/Principle_of_least_privilege

[10] See en.wikipedia.org/wiki/Defense_in_depth_(computing)

separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.[11] 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

19. 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 international system,[12] 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.

[11] See en.wikipedia.org/wiki/Separation_of_duties
[12] ECE/TRANS/WP.30/GE.1/2021/31

- Most of the **reliability requirements** (RL.1, RL.2, RL.3, RL5 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.

20. 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.

21. 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

22. The following table contains the requirement related to the auditing process as mentioned in Figure II. 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 1
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

23. The following table lists the requirements related to the authentication process as mentioned in Figure II. 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 2
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

24. The following table lists the requirements related to the authorization process as mentioned in Figure II (above) for the information systems involved in the eTIR system.

Table 3
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 maintenance of the user accounts.	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 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

25. 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.

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

Table 4
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

27. 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 5
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.[13] 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
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

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

Table 6
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

29. 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 7
Integrity requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
IN.1	The integrity of the information transferred between the information	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

[13] 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.

	systems of the eTIR international system remains intact.	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

30. 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 8
Nodes security requirements

Identifier	*Description and objective*	*How to fulfil the requirement*
NS.1	Securely configure virtual servers, containers or pods to prevent unauthorized access.	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 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

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

Table 9
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

32. 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 10
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 search, requisition or confiscation to protect the information stored in it.	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, 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

33. 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 11
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)[14] 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.

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

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

34. 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 12
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.
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

35. 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

36. 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.

37. 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.

38. 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

39. The Convention on the Privileges and Immunities of the United Nations,[15] 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.

40. 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

41. 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.

42. 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.

[15] See un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf

43. 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

44. 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,[16] 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,[17] 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,[18] the hosting entity also plays an important role in areas like incident management, backup and restore, monitoring, patch and upgrade management.

45. 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.

46. 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

47. 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

[16] ECE/TRANS/WP.30/GE.1/2021/30
[17] ECE/TRANS/WP.30/GE.1/2021/31
[18] ECE/TRANS/WP.30/GE.1/2021/33

testing malformed input data, null or blank values, values too long and specific evil stories.[19]

- **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.[20]

7. Security assessments

48. 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.

49. 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.

[19] «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.

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

50. 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.