Organisation intergouvernementale pour les transports internationaux ferroviaires
Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr
Intergovernmental Organisation for International Carriage by Rail

Working Group TECH

TECH-26043-CTE-WGT59-5.4
Distrib.: Public

11.08.2026
Original : EN

59TH SESSION

Use of electronic signatures or seals on certificates issued under the APTU or ATMF UR

I. INTRODUCTION

1. The aim of this document is to gather information about existing practices and to initiate discussion concerning the use of electronic signatures or seals on certificates issued under the APTU or ATMF UR and the development of guidelines.

2. The discussion is relevant in light of the increasing use of electronic signatures and the absence of rules governing them in OTIF's legal framework for interoperability.

3. The trigger for these considerations was Türkiye's request to the OTIF Secretariat to clarify whether the use of its national QR code-based digital verification system, integrated into the e-government platform (e-Devlet), would meet the "signature" requirements in the application and certification forms contained in the entity in charge of maintenance (ECM) certification templates of the ECM Regulation (Annex A to the ATMF UR).

4. The accepted technologies and legal status of electronic signatures or seals may differ among Contracting States. In the absence of harmonised international rules at OTIF level, different national and regional laws on electronic signatures may prevent certificates issued under the APTU and ATMF UR from being recognised and mutually accepted. It is therefore appropriate to examine this issue and to assess whether OTIF needs to take any action in this regard, for instance in the form of guidance or rules.

5. At its 58th session (Berne, 10–11 June 2026), WG Tech reviewed the initial version of this document, which had the reference TECH-26029. It concluded as follows:

   – WG Tech invited the Secretariat to collect further information on national digital signature and trust service schemes, including their interaction with secure registers such as ERADIS;

   – WG Tech invited CSs to share their experience with electronic signatures and encouraged Türkiye, Georgia and any other interested CSs to pursue bilateral discussions with ERA and the EC on the compatibility of their systems with the EU's trust service framework, and to keep the Secretariat informed;

   – WG Tech noted that the increasing use of electronic signatures and seals raises questions about the mutual recognition of certificates under the ATMF UR and highlighted the importance of a technology-neutral approach based on functional requirements;

   – WG Tech requested the Secretariat to develop proposals for a future session for functional, technology neutral guidance on electronic signatures and seals under the APTU and ATMF UR, taking into account the need for mutual recognition without causing further burdens for EU actors.

6. Substantive differences between this document and its previous version are indicated as "tracked changes".

II. TERMINOLOGY USED IN THIS PAPER

7. An electronic record is a broad term used to indicate data or information in electronic form that is created, modified and stored digitally, often with a unique token linked to it. An airline ticket is an example of an electronic record, where the actual substantive information is only stored online and, a unique code is linked to the ticket and enables it to be retrieved.

8. An electronic document is a file that presents information as a human-readable document, e.g. in .pdf format. Electronic documents may incorporate electronic records or derive from them, but are the human-readable representation, not the underlying data.

5.9. For the purpose of this paper, the terms "electronic signature" and "electronic seal" are used. Both terms mean data in an electronic form that is attached to or logically associated with an electronic document or record to permit verification of ~~the document's~~ its origin, authenticity and integrity. The differences between these terms are as follows:

- An electronic signature is used to identify the natural person signing and to express their consent to or approval of the content of the electronic document or record. It serves the same purpose as a wet-ink signature.
- An electronic seal is used to authenticate that an electronic document or record has been issued by a legal person (i.e. an entity rather than a natural person). It serves the same purpose as an official stamp or seal.

III. CURRENT SITUATION UNDER THE APTU AND ATMF UR

6.10. The following regulations and associated procedures require signatures to validate certain documents:

- The provisions on the uniform format of certificates. Technical certificates issued in paper form must be signed by the competent authority to validate them. [link]
- The ECM Regulation requires the signatures of the applicant and the certification body on applications for ECM certificates and for maintenance functions certificates, as well as the certification body's signature on the ECM certificates issued or the maintenance functions certificates issued. [link]
- Annex 4 to the Specification for vehicle registers (standard form for registration of vehicles) requires the signature of the entity applying for registration and, where applicable, the signature of the authorised representatives in the event of a change of keeper or ECM. [link]
- UTP Marking requires the keeper's (applicant's) signature when submitting a request concerning a Vehicle Keeper Marking (VKM) code (application for a new VKM, change to the code or its revocation) and the competent national authority's signature confirming that the applicable regulations have been complied with. [link]
- UTP GEN-D, concerning assessment procedures, requires the assessing entity's signature on the certificate of verification in accordance with the applicable UTP(s). [link]
- UTP GEN-G, concerning the Common Safety Method (CSM) on risk evaluation and assessment, requires the CSM assessment body's signature on the assessment report on the suitability of a system to fulfil its safety requirements. [link]

7.11. There are currently no provisions in the APTU and ATMF UR regulating the use of electronic signatures for certificates issued under these appendices. However, Article 6a § 1 of the ATMF UR, "Recognition of procedural documentation", establishes a relevant principle:

> "Assessments, declarations and other documentation made according to these Uniform Rules **shall be recognised at face value** by the authorities and competent bodies, the rail transport undertakings, the keepers and the infrastructure managers in all the Contracting States."

This provision presumes a level of trust between the Contracting States and their authorities, and entities acting in the scope of COTIF on their territories.

~~8.~~12. Although there are no rules in the APTU and ATMF UR governing electronic signatures, there are provisions concerning the use of electronic records, or registers, and data authenticity and integrity. These may contain elements that are relevant to electronic signatures as well. This particularly concerns the UTP TAF, which is currently subject to a revision process, the specifications for vehicle registers, and the uniform format of certificates, which is subject to a proposal for revision by the 18th session of the Committee of Technical Experts (CTE) on 9 June 2026.

IV. RELEVANT DISCUSSIONS AND PRACTICES AT OTIF LEVEL

A. Ad hoc Committee on Legal Affairs and International Cooperation

~~9.~~13. In the context of ongoing discussions on the digitalisation of transport documents under the CIM UR, issues related to electronic signatures have been considered as part of the broader examination of electronic consignment notes. The subject is currently being considered by the ad hoc Committee on Legal Affairs and International Cooperation (ad hoc Committee)[1].

14. There are differences between the signatories of CIM consignment notes and those of certificates issued under the APTU and ATMF UR. The signatures serve different purposes, involve different entities and may therefore require different conditions for their acceptance. Without entering into details about the CIM UR, it is worth noting that certificates issued under the APTU and ATMF UR are signed by bodies accredited, designated or recognised by the Contracting State to perform specific tasks. Furthermore, these certificates are generally published in dedicated registers to which access is restricted, adding a layer of trust in the authenticity of the certificates they include. In short, the CTE cannot simply rely on the outcome of the discussions at ~~JUR~~ the ad hoc Committee, as this outcome is primarily designed to apply to the CIM UR, but should consider the subject specifically for the purpose of technical interoperability. Nonetheless, the ad hoc Committee and the CTE will need to remain aware of each other's work in this area and cooperate closely to ensure that coherent and suitable processes are developed across the Organisation and the appendices. As discussions develop in each organ, it will be advisable to review progress periodically and to explore opportunities for a joint examination of this topic across both organs.

15. The ad hoc Committee has been considering digitalisation and potential modifications to the CIM UR since 2023. At its 7th session (April 2025), it adopted seven principles to be taken into account when proposing modifications to the CIM UR to provide fully for the use of digital transport documents:

1. minimal intervention [to the CIM UR];
2. non-discrimination of paper-based and paperless transport (new provisions must not only provide for electronic transport documents to be used, but also continue to respect and allow the use of paper documents);
3. technological neutrality (provisions cannot favour one technology solution over another);
4. functional equivalence (there needs to be a degree of functional equivalence between all functions of electronic and paper documents, whether it be the authenticity, integrity and reliability of data or any of the content of those documents);
5. compatibility with international electronic commerce law and transport law, in particular with the European Union legislation covering those matters;
6. take into account current practices and solutions in the railway sector;

1

7. give due respect to the autonomy of the parties involved in the carriage of goods.

~~10.~~16. At its 8th and 9th sessions (December 2025 and June 2026), the ad hoc Committee considered draft functional requirements for electronic consignment notes to be included in the CIM UR. Document LAW-26028-JUR9/4 of 12 May 2026 (restricted distribution) contains the latest provisions reviewed by the ad hoc Committee, which are set out in an annex to this document.

17. The Secretariat suggests that the WG Tech should not discuss these draft CIM UR provisions at this stage. Nevertheless, it seems appropriate for WG Tech to take note of these developments and align with the results where relevant.

B. Existing practice; an example related to ECM certificates

~~11.~~18. ECM certificates confirm that the ECM meets the requirements applicable to it in accordance with the ECM Regulation. They are issued by certification bodies accredited or recognised for this purpose. The mutual acceptance of ECM certificates is essential to enable vehicles to operate in international traffic.

~~12.~~19. The ECM Regulation does not explicitly set out detailed rules on the use of signatures and stamps on ECM certificates. However, the certificate templates set out in the annexes to the ECM Regulation contain dedicated fields for a certification body's signature and stamp, thus implicitly requiring them.

~~13.~~20. In practice, ECM certification bodies carry out their activities under the legal frameworks for accreditation, designation or recognition established by the Contracting States. In applying these legal frameworks, ECM certification bodies are presumed to comply with standards EN 17020 and EN 17065. Although these standards are not explicitly referred to in OTIF's legal framework, they reflect best practice for issuing certificates and emphasise responsibility and traceability. In line with these standards, certificates are issued under the responsibility of a specific authorised individual (natural person) designated by the certification body, whose identity is indicated by name and a signature. The use of a stamp alone, without indicating who is responsible, is not sufficient.

~~14.~~21. The joint OTIF/ERA ECM register has been operational since 1 April 2014. Since then, ECM certification bodies have entered issued, amended, renewed or revoked ECM certificates directly into the publicly accessible (read-~~-~~only) ERADIS database. In this context, there is no formal requirement for the type of signature used on ECM certificates.

~~15.~~22. A limited review of more than 40 randomly chosen ECM certificates in the ERADIS database from several EU and non-EU Contracting States was conducted to assess how they were signed. All the certificates reviewed were published in ".pdf" format. The review identified differences in signing practices: most certificates included both a signature and a stamp, while others included either a signature or a stamp. Judging by their appearance, some certificates seemed to feature a pre-scanned signature copied into the digital file, while other certificates appeared to have been signed by hand (wet-ink) and subsequently scanned. In a limited number of cases, qualified electronic signatures were used, either included in the certificate, placed on a second page, or attached as an additional page. These findings indicate that ECM certification bodies do not apply a uniform approach when signing the ECM certificates they issue. Despite these differences, all the ECM certificates reviewed were considered valid, as their acceptance was based on their inclusion in the ERADIS database.

V. ~~DIFFERENT FORMS AND STANDARDS OF~~ ELECTRONIC SIGNATURES AND SEALS UNDER EU LAW

~~16.~~23. The required level of security underpinning these functions depends on the purpose and legal nature of the document and the environment in which it is stored and used. Different signature technologies can meet these functions with different levels of security and reliability. For example, Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS)[2], distinguishes the following three main categories:

– Simple or basic electronic signature or seal. This includes scanned handwritten signatures or stamps, typed names or signature images in ".pdf" format. They are easy to use but offer limited security. They may be appropriate where the risks are low or where the document's origin can be verified by other reliable means.

– Advanced electronic signature or seal. This signature or seal is linked to the signatory (a natural person in the case of a signature), enables identification and is created under the signatory's control and detects any later modification of the document. It offers greater reliability and ~~is more trustworthy~~security.

– Qualified electronic signature or seal. This signature or seal ~~in the legal system that regulates it,~~ is issued through a certified trust service provider. It is the most secure~~trustworthy~~ category and is equivalent to a handwritten signature under EU law. However, outside ~~such a legal system~~the EU, its legal value and technical compatibility may differ, so it cannot be automatically recognised.

24. Document LAW-26027-JUR 9/4 of 12 May 2026 (restricted distribution) noted that:

– "A 'qualified electronic seal' is not just an 'advanced electronic seal', but an 'advanced electronic seal, which is created by a 'qualified electronic seal creation device', and that is based on a qualified certificate for electronic seal". The requirements of a "qualified electronic seal creation device" and a "qualified certificate for electronic seal" are outlined in Annexes II and III of the eIDAS Regulation respectively. Both concepts require the services of a "qualified trust service provider". The eIDAS Regulation contains significant detail on the concept of a "qualified trust service provider".

~~17.~~25. At WG Tech 58, the European Commission emphasised that the EU had no intention of exporting eIDAS requirements into COTIF or imposing them on non-EU CSs. However, OTIF's functional requirements for electronic signatures and seals should not add obligations beyond those already applicable in the EU, in order to avoid further burdens being placed on EU actors. It supported drafting OTIF rules at the level of functional requirements and ensuring compatibility with the EU framework.

VI. CONSIDERATIONS FOR POSSIBLE GUIDANCE OR RULES

26. Depending on the feedback from Contracting States and their current practices, minimum functional requirements for electronic signatures could be defined to ensure interoperability, preferably without prescribing specific technologies or national systems. The requirements should align with the "acceptance at face value" requirement set out in Article 6a of the ATMF UR. A distinction could be drawn between certificates that are stored in a secure register versus certificates that are freely transferrable in electronic format.

---

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (ELI: http://data.europa.eu/eli/reg/2014/910/oj).

~~18.~~27. OTIF guidance or rules could address the following questions:

- Whether and how identification of the natural person responsible for signing the certificate on behalf of the issuing body should be mandatory, as required by EN 17020 and EN 17065. Should an electronic signature (by a natural person) be required or could an electronic seal (by a legal entity, i.e. an organisation), together with the name of the responsible person, be sufficient?
- Which requirements should apply to the technology or method for electronic signatures or seals? In particular, should there be OTIF provisions which enable an assessment of whether specific technologies or methods developed for domestic use by a Contracting State are acceptable?
- Whether the "acceptance at face value" requirement set out in Article 6a of the ATMF UR could be invoked to promote mutual acceptance of different national solutions for digital signatures and seals, provided they meet certain basic requirements?
- Which functions of an electronic signature or seal could be achieved by a secure register (such as ERADIS) if the certificates can only be accessed through that register?

VII. DEVELOPMENT OF FUNCTIONAL REQUIREMENTS

28. One of the challenges for requirements equivalent to those for qualified electronic signatures or seals under eIDAS is the establishment and international recognition of qualified trust providers. Document LAW-26027-JUR 9/4 of 12 May 2026 (restricted distribution) noted on this topic that:
    - "The requirement to use the services of a 'qualified trust provider' when addressing the concept of 'qualified electronic seals' is to ensure that there are trusted and reliable methods of assuring the control and signing of electronic consignment notes. In the proposed modifications to the CIM UR, the concept of requiring reliable or trusted ways of signing and indeed issuing and operating electronic consignment notes is instead tackled by a series of flexible provisions contained in Article 6 § 12, setting out what may be a reliable 'method' relating to electronic consignment notes. This allows flexibility and the use of methods that meet these criteria without providing a series of rules in a prescriptive way. It also means that rules and practices across different Member States can be consistent with each other and the stated requirements, yet without having to be identical to each other."

29. The draft CIM UR requirements contained in the annex to this paper set out several key functional parameters. Below is a description of these parameters, which could also become a basis for functional requirements for digital records, signatures and seals under the APTU and ATMF UR.

30. These parameters should be considered the maximum requirements, functionally aligned with those for the qualified electronic signature or seal under the EU's eIDAS. For the purpose of the APTU and ATMF UR, the requirements could be adjusted to particular functional needs.

A. Identification and intention

31. A reliable method should be used to identify the signatory and to indicate that person's intention in respect of the information contained in the electronic record.

B. Control

32. A reliable method should be used to establish exclusive control of the electronic record by a person and to identify that person as the person in control from its issuance until it ceases to have any effect or validity

33. If permitted or required for the functions of the electronic record, control may or must be transferrable to another person.

C. Reference

34. A reliable method should be used to ensure that the electronic record can be referred to from its issuance until it ceases to have any effect or validity.

D. Integrity

35. A reliable method should be used to retain the integrity of the electronic record to which the signature or seal pertains.

36. The criterion for assessing integrity should be whether information contained in the electronic record, including any authorised change that is made from its issuance until it ceases to have any effect or validity, has remained complete and unaltered, apart from any change that is made in the normal course of communication, storage and display.

E. Reliability

37. The methods to control the electronic record, refer to it, maintain its integrity and identify the signatory should be appropriate to fulfil the function for which the method is being used.

38. The method used should provide appropriate reliability and can either be proven in fact to have fulfilled the function by itself, together with further evidence, or be assessed in the light of all relevant circumstances, which may include:

- any operational rules relevant to the assessment of reliability;
- the assurance of data integrity;
- the ability to prevent unauthorised access to and use of the system used to implement the method;
- the security of hardware and software;
- the regularity and extent of audit by an independent body;
- the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;
- any applicable industry standard.

39. Generally, it should be possible for the Committee of Technical Experts or a person authorised by it to designate providers or services or methods that are presumed sufficiently reliable for digital signatures or seals for a defined purpose. It should be able to publish and maintain a list of the service providers or providers of reliable methods.

~~VII.~~VIII. NEXT STEPS

~~19.~~40. If supported by WG Tech and the ad hoc Committee, the Secretariat could set up an informal meeting to which technical and legal experts could be invited to discuss requirements for electronic records, signatures and seals.

~~WG Tech could invite Contracting States to:~~

- ~~Consider the questions under point 18;~~
- ~~Share information on whether and how electronic signatures are used in practice for certificates issued under the APTU and ATMF UR. This could include an invitation to Türkiye to provide information about their QR code-based system.~~
- ~~Share information on their recognition of electronically signed or sealed foreign documents.~~

Annex

Draft texts for CIM concerning the digital consignment note

Article 6
Contract of carriage

[…]

§ 9 Where a consignment note is issued as an electronic record, a reliable method shall be used to:

- identify the electronic record as the consignment note;
- render that electronic record capable of being subject to control and subsequent reference from its issuance until it ceases to have any effect or validity;
- retain the integrity of that electronic record; and
- identify the signatory to indicate that person's intention in respect of the information contained in the electronic record.

§ 10 The criterion for assessing integrity shall be whether information contained in the electronic record, including any authorised change that is made from its issuance until it ceases to have any effect or validity, has remained complete and unaltered, apart from any change that is made in the normal course of communication, storage and display.

§ 11 a) An electronic record is subject to control if a reliable method is used:

1. to establish exclusive control of that electronic record by a person; and
2. to identify that person as the person in control.

b) A requirement to transfer control of a consignment note is met with respect to an electronic record through the transfer of control over the electronic record.

§ 12 The method referred to in Article 6 § 9, Article 6 § 11 and Article 6 § 14 shall be:

- as reliable as appropriate to fulfil the function for which the method is being used. Whether the method used provides appropriate reliability shall be assessed, in the light of all relevant circumstances, which may include:
  1. any operational rules relevant to the assessment of reliability;
  2. the assurance of data integrity;
  3. the ability to prevent unauthorised access to and use of the system used to implement the method;
  4. the security of hardware and software;
  5. the regularity and extent of audit by an independent body;
  6. the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;

7. any applicable industry standard; or proven in fact to have fulfilled the function by itself or together with further evidence.

§ 13 a) [Insert identified competent person] may designate services for the management of consignment notes issued as electronic records that are presumed reliable for the purposes of these Uniform Rules.

b) [Insert identified competent person] shall, when making a designation under Article 6 § 13 a):

1. take into account all relevant circumstances, including the factors listed in Article 6 § 12, in designating a manage-ment service or a method as reliable; and

2. publish and maintain a list of designated management services or reliable methods, including details of the management service provider or provider of reliable methods.

c) Any designation pursuant to Article 6 § 13 a) shall be consistent with recognised international standards and procedures relevant for performing the designation process.

§ 14 a) At the request of the consignor or the carrier and with the agreement of the other, the medium of the consignment note may be changed from paper to electronic record or from electronic record to paper provided that a reliable method for the change of medium is used.

b) At the time of the change of medium, the consignor and the carrier shall each ensure that the consignment note, in its previous medium, becomes inoperative and ceases to have any effect or validity.

c) A change of medium does not affect the rights and obligations of the parties.