



OTIF/RID/CE/GTP/2019/9

14. November 2019

Original: Englisch

RID: 11. Tagung der Ständigen Arbeitsgruppe des RID-Fachausschusses
(Wien, 25. bis 29. November 2019)

Thema: Leitfaden für die Anwendung des Unterabschnitts 5.4.0.2 RID/ADR/ADN

Mitteilung des Sekretariats

1. Bei der Gemeinsamen RID/ADR/ADN-Tagung (Genf, 17. bis 27. September 2019) wurde ein von der informellen Telematik-Arbeitsgruppe ausgearbeiteter Leitfaden für die Anwendung des Unterabschnitts 5.4.0.2 RID/ADR/ADN angenommen (siehe Bericht OTIF/RID/RC/2019-B Absätze 48 bis 51 und Anlage III).
2. Die Gemeinsame Tagung wies darauf hin, dass der Leitfaden auf freiwilliger Basis und für jeden Verkehrsträger getrennt angewendet werden kann. Bei einer Verwendung muss er jedoch in seiner Gesamtheit angewendet werden.
3. Die Gemeinsame Tagung bat die WP.15 und den RID-Fachausschuss die Veröffentlichung des Leitfadens auf den Websites der UNECE und der OTIF zu genehmigen.
4. Nachstehend ist der gesamte im Dokument OTIF/RID/RC/2019/44 enthaltene Leitfaden mit den von der Gemeinsamen Tagung vorgenommenen Korrekturen wiedergegeben.

Leitfaden für die Anwendung des Unterabschnitts 5.4.0.2 RID/ADR/ADN

Einleitung

1. Der Unterabschnitt 5.4.0.2 RID/ADR/ADN erlaubt die Verwendung des elektronischen Datenaustauschs zur Erfüllung der Dokumentationsvorschriften des Kapitels 5.4, sofern das Verfahren zur Erfassung, Speicherung und Verarbeitung der Daten den gesetzlichen Anforderungen hinsichtlich Beweiskraft und Verfügbarkeit während der Beförderung in einer Weise entspricht, die mindestens derjenigen der schriftlichen Dokumentation gleichwertig ist.
2. Das RID/ADR/ADN definiert jedoch nicht, was mit dieser Gleichwertigkeit gemeint ist. Um das Ziel zu erreichen, die Verfügbarkeit von Daten, die Sicherheit und die Beweiskraft zu gewährleisten, ist es notwendig, Webdienste, Schnittstellen und eine Kommunikationsarchitektur zur Unterstützung der Datenkommunikation zu implementieren.
3. Dieser Leitfaden basiert auf den von der Gemeinsamen Tagung genehmigten Ergebnissen der Telematik-Arbeitsgruppe, wurde aber noch nicht von allen RID-Vertragsstaaten und/oder ADR- und/oder ADN-Vertragsparteien umgesetzt. RID-Vertragsstaaten und/oder ADR und/oder ADN-Vertragsparteien, die bereit sind, diesen Leitfaden anzuwenden, können dies auf freiwilliger Basis tun. Sobald ein Vertragsstaat/eine Vertragspartei sich jedoch zur Anwendung verpflichtet hat, muss er/sie widerspruchsfrei handeln und den Leitfaden in seiner Gesamtheit anwenden.

Abschnitt 1 – Geltungsbereich und Begriffsbestimmungen

4. Die Vorschriften des Unterabschnitts 5.4.0.2 RID/ADR/ADN gelten unter den in den Anlagen festgelegten Bedingungen als erfüllt. Für die Zwecke dieses Leitfadens ist ein elektronisches Beförderungspapier eine elektronische Dokumentation der im Beförderungspapier gemäß Abschnitt 5.4.1 des RID/ADR/ADN vorgeschriebenen Angaben.
5. RID-Vertragsstaaten und/oder ADR- und/oder ADN-Vertragsparteien, die diesen Leitfaden anwenden, werden im Folgenden als "Teilnehmer" bezeichnet.
6. Die Teilnehmer stimmen darin überein, die in der Anlage A und in den technischen Unterlagen skizzierte Modell- und Systemarchitektur verwenden zu wollen.
7. Nachstehende Gründe finden Erwägung:
 - a) Die in der Anlage A umrissene Systemarchitektur basiert auf dem Konzept von zwei unterschiedlichen Systemen zur Leistungserbringung, die als *Trusted Party* (vertrauenswürdige Stelle) TP1 und TP2 bezeichnet werden. Das Modell sieht eine Reihe von TP1 und TP2 vor.
 - b) Eine TP2 verwaltet die gemäß Abschnitt 5.4.1 des RID/ADR/ADN erforderlichen Daten. Eine TP2 kann vom Beförderer selbst oder von einem Drittanbieter für den Beförderer betrieben werden.
 - c) Eine TP1 ermöglicht auf Anfrage eine Weitergabe dieser Daten von der TP2 an Behörden oder Einsatzkräfte.
 - d) Eine TP1 leitet auf Anfrage auch Daten von der TP2 an andere TP1 weiter.

- e) "eDG Transport Information" ist die Abkürzung für die technischen Elemente, die das auf dem UML-Modell (*Unified Modelling Language* – vereinheitlichte Modellierungssprache), der XSD (*Extended Markup Language Schema Definition* – Schema-Definition der erweiterten Auszeichnungssprache) und den WSDL-Webdiensten (*Web Service Description Language* – Beschreibungssprache für Netzwerkdienste) basierende Austauschformat beschreiben.

Abschnitt 2 – Pflichten der Teilnehmer

8. Der Teilnehmer teilt dem Sekretariat der OTIF/UNECE die Anwendung des Leitfadens mit. Er benachrichtigt auch die TP1 (falls vorhanden), die gemäß Anlage A benannt wurden.
9. Die Teilnehmer akzeptieren elektronische Beförderungsinformationen in Übereinstimmung mit dem Leitfaden und dessen Anlage A.

Abschnitt 3 – Veröffentlichung des Leitfadens und Liste der Teilnehmer

10. Die OTIF und die UNECE werden die Liste der Teilnehmer und die von den Teilnehmern mitgeteilten TP1 veröffentlichen.
11. Der Leitfaden wird auf den Websites der OTIF und der UNECE sowie in den UML-, XSD- und WSDL-Referenzdateien mit der Bezeichnung "eDG Transport Information" zur Verfügung gestellt.

Abschnitt 4 – Datensicherheit und technische Wartung

12. Die TP1 treffen geeignete technische und organisatorische Maßnahmen, um die Datensicherheit zu gewährleisten. Sie dürfen vertrauliche Daten nicht für andere als die in diesem Leitfaden beschriebenen Zwecke (z. B. Missbrauch durch Data-Mining (Datengewinnung)) verwenden.
13. Die TP1 sind verantwortlich für die tägliche Wartung und Verwaltung des Systems und arbeiten in einer technischen Arbeitsgruppe zusammen, die sie bei diesen Arbeiten unterstützt. Die Wartung umfasst auch technische Aktualisierungen, die aus Änderungen am RID/ADR/ADN resultieren.
14. Bei schwerwiegenden Kommunikationsproblemen werden technische Änderungen an "eDG Transport Information" (beschränkt auf die UML-, XSD-, WSDL-Referenzdateien), die für die Funktion des Systems von wesentlicher Bedeutung sind und die von der technischen Arbeitsgruppe angenommen wurden, unmittelbar genehmigt.
15. Die technische Arbeitsgruppe informiert alle TP1 über die an "eDG Transport Information" vorgenommenen Aktualisierungen und das Anwendungsdatum und legt diese dem Sekretariat der OTIF/UNECE zur Veröffentlichung auf den Websites der OTIF und der UNECE vor.

Abschnitt 5 – Grundsätze für die Änderung des Leitfadens

16. Änderungen des Leitfadens werden von den Teilnehmern entweder im Rahmen eines schriftlichen Verfahrens mit Konsens oder auf einer Sitzung nach den von der Sitzung festzulegenden Regeln angenommen. Auch andere Vertragsstaaten/Vertragsparteien können Änderungen vorschlagen.
17. Änderungen an der Systemarchitektur können nur von der technischen Arbeitsgruppe vorgeschlagen werden und müssen von der Gemeinsamen Tagung angenommen werden.

1. Grundsätze für die Kommunikation zwischen verschiedenen TP1 und TP2 sowie zuständigen Behörden zu Beförderungsdokumenten

a) Eine TP1 kann öffentlich oder privat betrieben werden. Ein TP1-Betreiber darf nicht an der Beförderung gefährlicher Güter beteiligt sein (insbesondere nicht als Absender, Beförderer, Empfänger, Verloader, Verpacker, Befüller, Betreiber eines Tankcontainers oder eines ortsbeweglichen Tanks oder Entlader). Ein TP1-Betreiber hat unter den unter b) festgelegten Zertifizierungsbedingungen zu arbeiten. Der Zugang zu den Informationen einer TP1 ist für andere TP1 und für Behörden kostenlos. Pro Teilnehmer kann es eine oder mehrere TP1 geben. Die Teilnehmer sind nicht verpflichtet, eine TP1 einzurichten, sie können alternativ beschließen, die Funktionen/Dienste einer oder mehrerer ausländischer TP1 zu nutzen. TP1 ohne eingetragene TP2 sind ebenfalls zugelassen.

b) Qualifizierte TP1-Stellen ("TP1-Zertifizierung"):

(i) Deutschland, Frankreich, Italien und Österreich haben bereits eine erste Anzahl möglicher TP1 bestimmt (aktuell sind dies GBK in Deutschland, NeoGLS und Novacom Services in Frankreich, das Verkehrsministerium und UIRNet in Italien und DiGiDO in Österreich).

Die Teilnehmer können zusätzliche TP1 bestimmen.

(ii) Für den zukünftigen Betrieb sollte diese Liste qualifizierter TP1-Stellen (*TP1 Trusted List*) mit allen für die Identifizierung relevanten Informationen bei der UN-ECE für den Straßenverkehr und die Binnenschifffahrt und eventuell bei der OTIF/UN-ECE für den Eisenbahnverkehr hinterlegt werden; darüber hinaus sollte die OTIF/UN-ECE diese Liste verwalten und in dem für das System erforderlichen Ausmaß Auszüge daraus veröffentlichen. In der Folge erhalten diese Institutionen die Funktion eines Verwalters der "vertrauenswürdigen Liste" (*Trusted List Manager*).

(iii) Alle qualifizierten TP1-Stellen werden über die *TP1 Trusted List* durch die *Trusted List Manager* informiert bzw. auf den neuesten Stand gebracht (d. h. sie wissen, wer die anderen qualifizierten TP1-Stellen sind).

(iv) Detailliertere Anforderungen z. B. in Bezug auf vereinbarte Zertifikate und Sicherheitsrichtlinien, welche die TP1 erfüllen müssen, werden noch festgelegt. Um eine solide Grundlage für die Bestimmung dieser Anforderungen zu schaffen, müssen die oben genannten Unternehmen/Institutionen Vorschriften entwickeln und Berichte vorlegen. Diese Anforderungen für die Anerkennung werden dann von den Teilnehmern diskutiert und bestätigt und müssen auf andere interessierte Unternehmen angewandt werden.

c) Es gelten folgende "Vorschriften":

(i) Ein Teilnehmer darf nur eine TP1 benennen, die ihren Sitz in seinem Hoheitsgebiet hat. Alle qualifizierten TP1-Stellen müssen die gesamten Datenaustauschspezifikationen von "*eDG Transport Information*" unterstützen.

(ii) Die TP1 haben Anfragen anderer TP1 zu akzeptieren.

- (iii) Die TP1 haben alle TP2-Registrierungen zu akzeptieren, sofern diese dem Leitfaden entsprechen und die vertraglichen Verpflichtungen dieser TP1 erfüllen.
 - (iv) Eine TP1 kann für die Dienste, die sie einer TP2 anbietet, Gebühren erheben. Die TP1 kann seine Preispolitik nach eigenem Ermessen festlegen, muss dabei aber einen diskriminierungsfreien Ansatz verfolgen.
 - (v) Die TP1 haben Anfragen auf Registrierung von Behörden, die gemäß Absatz d) in einem Verzeichnis aufgeführt sind, zu akzeptieren.
 - (vi) Die TP1 haben Anfragen aller bei ihr registrierten zuständigen Behörden zu akzeptieren.
 - (vii) Nach ihrer Aufnahme in die *Trusted List* müssen neue TP1 unter Angabe aller vorgeschriebenen Kontaktdaten bei allen bestehenden TP1 registriert werden.
- d) Nationales Verfahren zur Bestimmung der Behörden, die berechtigt sind, Anfragen zu stellen
- (i) Jeder Teilnehmer erstellt sein eigenes Verzeichnis von Behörden (z. B. Vollzugsstellen, Einsatzkräfte), die berechtigt sind, Anfragen an eine TP1 zu stellen. Der Teilnehmer hat darüber hinaus sicherzustellen, dass auch das in Punkt 2 b) genannte entsprechende Zertifikat enthalten ist. Nur in diesem Verzeichnis aufgeführte Behörden dürfen sich bei einer TP1 registrieren.
 - (ii) Der Teilnehmer ist für die Aktualisierung und Verwaltung der Liste zuständig.

2. Von den TP1 im Hinblick auf ihren Betrieb zu erfüllende Anforderungen

- a) TP1-Funktionen
- (i) TP1- und TP2-Funktionen werden in WSDL beschrieben. Von außen zugängliche Funktionen werden hauptsächlich mit ihren Parametern und Rückgabewerten beschrieben.
 - (ii) Die TP1-Funktion *"getDGTDokument"* beschafft ein bestimmtes Beförderungsdokument von einer bestimmten TP2. Die Parameter zur Identifizierung der TP2 und des spezifischen Beförderungsdokuments sind in Punkt 3 a) beschrieben. Diese Funktion steht ausschließlich Einsatzkräften und Vollzugsbehörden zur Verfügung (siehe Punkt 1 d)). Die Behörde darf bei der TP1 nur Informationen zu Fahrzeugen auf ihrem Hoheitsgebiet abfragen. Der Grund für die Beantragung des Zugangs muss durch Auswahl aus einer vorgefertigten Liste (z. B. Einsatzkräfte, Vollzugsstellen) angegeben werden.
 - (iii) In Übereinstimmung mit Unterabschnitt 5.4.4.1 muss jeder Zugriff mindestens drei Monate lang protokolliert werden.
 - (iv) Die TP1 muss den Beginn und das Ende der Beförderung gemäß Punkt 3 a) speichern, damit der TP2-Datensatz für jede Beförderung auf Anfrage den Vollzugsstellen oder Einsatzkräften übermitteln werden kann.

b) Zertifikate

- (i) Die TP1 müssen ein HTTPS-Protokoll verwenden. Die TP1 müssen eine feste IP-Adresse und ein X509-V3-Zertifikat haben, das in die *Trusted List* eingetragen wird. Die Authentifizierung muss durch Überprüfung von IP-Adresse und Zertifikat erfolgen. Der Datenschutz muss mit http über das kryptographische TLS-Protokoll gesichert werden. Zertifikate müssen in Übereinstimmung mit den nationalen Vorschriften der Teilnehmer erstellt werden. Die Zertifikate müssen direkt über sichere Kanäle ausgetauscht werden.

c) Registrierung von Behörden und TP2 bei einer TP1

- (i) Zur Ermöglichung der intermaschinellen Kommunikation muss die TP1 ein Registrierungsverfahren festlegen, das manuell oder automatisch erfolgen kann.

Ein maschinelles Verfahren muss auf der Methode beruhen, die in der unter Punkt 1 c) (i) genannten Webservice-Beschreibung enthalten ist. Insbesondere gilt Folgendes:

- TP2-Kandidaten benutzen die Methode *"sendTP2Registration-Request"* mit folgenden Mindestdaten:
 - URL: TP2-Zugangspunkt für die TP1
 - öffentlicher Schlüssel des TP2-Zertifikats
 - Name und Adresse (Straße, Postleitzahl, Ort) der TP2
 - Name, E-Mail und Telefonnummer der verantwortlichen Kontaktperson
- Öffentliche Einrichtungen wenden die Methode *"sendPublicServiceRegistrationRequest"* mit folgenden Mindestdaten an:
 - öffentlicher Schlüssel des Zertifikats für öffentliche Einrichtungen
 - Name und Adresse der öffentlichen Einrichtung (Straße, Postleitzahl, Ort)
 - Name, E-Mail und Telefonnummer der verantwortlichen Kontaktperson
 - Art des Akteurs: zuständige Behörden (z. B. Einsatzkräfte, Vollzugsstellen).

- (ii) Das Registrierungsverfahren für die TP2 ist von der TP1 festzulegen.

- (iii) Handelt es sich bei der die Registrierung beantragenden Stelle um eine Behörde, müssen ihr Name und ihr Zertifikat in der Liste in Punkt 1 d) aufgeführt sein und die Überprüfung kann automatisch oder manuell erfolgen.

Handelt es sich bei der die Registrierung beantragenden Stelle um eine TP2, sind zwei Methoden möglich:

- Der offizielle Vertreter der TP2 unterbreitet eine digital signierte Erklärung, einschließlich des öffentlichen Schlüssels, die offline geprüft wird, oder
- die TP1 vertraut dem Unterzeichner des Zertifikats auf der Grundlage nationaler Gesetze, öffentlicher Register oder spezifischer Vereinbarungen, woraufhin die Überprüfung automatisch erfolgt.

3. Erstellung und Verfügbarkeit der zwischen TP2, TP1 und den Behörden/Einsatzkräften zu verwendenden Datensätzen

- a) Der folgende Datensatz für jede Beförderung muss an eine TP1 übermittelt werden:
 - (i) RID: eindeutige Fahrzeugnummer¹
ADR: Ländercode(s) (Wiener Übereinkommen), Kennzeichen und Fahrgestellnummer(n) des Zugfahrzeugs und des Anhängers (der Anhänger)
ADN: ENI-Nummer
 - (ii) BIC-Code für Container (wenn verfügbar oder geregelt)
 - (iii) Status: Beginn/Ende der Beförderung.
- b) Zusammenarbeit zwischen einer TP2- und einer TP1-Stelle:
 - (i) Für jede Beförderung arbeitet eine TP2 mit lediglich einer TP1 zusammen.
- c) Die Angaben des Beförderungspapiers, welche die TP2 an die TP1 übermittelt, müssen digital signiert sein.

4. Anforderungen während der Übergangsphase

Solange nicht alle Einsatzkräfte und zuständigen Behörden an das TP1/TP2-System angeschlossen sind, sind auch Informationen an Bord erforderlich.

Zusätzliche Anforderungen betreffend Datenspeicherung und Datenausgabe an Bord der Züge/Fahrzeuge/Binnenschiffe

- a) Der im Bord-Datenendgerät verwendete Datenträger muss geeignet sein, alle relevanten Gefahrgutangaben gemäß Abschnitt 5.4.1 des RID/ADR/ADN für die Dauer der Beförderung dauerhaft zu speichern. Zu diesem Zweck müssen in allen Datenendgeräten (z. B. Tablets, Scanner, Smartphones, Bordgeräte) nichtflüchtige Speichermedien (derzeit EEPROM- oder Flash-Speicher) verwendet werden. Die in den Datenendgeräten installierten Datenträger müssen vor den während der Beförderung auftretenden Beanspruchungen geschützt sein.
- b) Für den Eisenbahn- und Straßenverkehr ist ein tragbares Datenendgerät und für die Binnenschifffahrt ein tragbares Datenendgerät oder ein fest installiertes Bord-Datenendgerät zu verwenden. Wenn nur ein bis drei verschiedene gefährliche Güter (UN-Nummern) in Tanks oder in loser Schüttung in Fahrzeugen befördert werden, die den Kennzeichnungsvorschriften des Absatzes 5.3.2.1.2 oder 5.3.2.1.4 ADR unterliegen, ist ein fest installiertes Datenendgerät auch für den Straßenverkehr zugelassen.

Das Datenendgerät muss so ausgelegt sein, dass bei einer Unterbrechung der Energieversorgung kein Datenverlust auftreten kann. Der Energiespeicher muss für die Dauer der Beförderung Energie bereitstellen oder während der Beförderung mit Hilfe von Bordgeräten wieder aufgeladen werden können.

¹ Eindeutige Fahrzeugnummer gemäß den Einheitlichen technischen Vorschriften zur Fahrzeugnummer und entsprechende Kennbuchstaben: Kennzeichnung von Eisenbahnfahrzeugen (ETV Kennzeichnung 2015) der Einheitlichen Rechtsvorschriften APTU (Anhang F zum COTIF 1999) (siehe www.otif.org) und Europäische Fahrzeugnummer gemäß Entscheidung der Kommission 2007/756/EG zur Annahme einer gemeinsamen Spezifikation für das nationale Einstellungsregister nach Artikel 14 Absätze 4 und 5 der Richtlinien 96/48/EG und 2001/16/EG.

- c) Die Daten müssen auf einem Bildschirm angezeigt werden, der unter unterschiedlichen Lichtverhältnissen sowohl hinsichtlich der Zeichengröße als auch der Lesbarkeit Papierformat entspricht (visuelle Darstellung ohne Layoutvorgaben (z. B. PDF-Format) auf einem Bildschirm von mindestens 10 Zoll oder eine optimierte und strukturierte Darstellung, die es ermöglicht, auf dem jeweiligen Bildschirm (mindestens 3,5 Zoll) alle vorgeschriebenen stoffbezogenen Angaben einer Gefahrguteintragung darzustellen). Die Bedienung des Lesegeräts muss einfach und intuitiv sein und dem Kontrollpersonal/den Einsatzkräften uneingeschränkter Zugang zu allen relevanten Gefahrgutangaben ermöglichen.
- d) Der Triebfahrzeugführer/Fahrzeugführer/Schiffsführer muss in der Lage sein, das Datenendgerät zu bedienen und den Vollzugsbehörden oder Einsatzkräften die erforderliche Unterstützung zu leisten. Beispielsweise müssen sie auf Verlangen das Kontrollpersonal in die Bedienung des Datenendgeräts einweisen oder während der Kontrolle mit dem Datenendgerät begleiten. Dies gilt auch für Notfälle, in denen ein derartiges Vorgehen noch möglich ist.
- e) Bei fehlender mobiler Konnektivität muss akzeptiert werden, dass bei der Synchronisierung der Daten an Bord mit den Daten bei der TP2 Verzögerungen auftreten können.

5. Übergangsvorschriften für den Straßenverkehr

Im Führerhaus sind Anweisungen für den Zugriff auf die elektronischen Gefahrgutdaten bei Handlungsunfähigkeit des Fahrers anzubringen.

Vorder- und Rückseite des Fahrzeugs müssen mit einem Hinweis auf die Verwendung eines elektronischen Beförderungsdokuments gekennzeichnet sein. Wenn es aus baulichen oder anderen offensichtlichen Gründen nicht möglich ist, dieses Kennzeichen an der Fahrzeugrückseite anzubringen, darf es auch an beiden Zugängen zum Führerhaus angebracht werden. Je nach Einsatzart des Fahrzeugs darf das Kennzeichen abnehmbar (klappbare oder magnetische Kennzeichen dürfen verwendet werden) oder dauerhaft befestigt (fixiert) sein. Das Kennzeichen besteht aus einer Illustration (Piktogramm wie in der Anlage B dieses Leitfadens dargestellt).

Anlage B

Piktogramm "e" für die Verwendung eines elektronischen Beförderungspapiers


