

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

Vejkøretøjer – Netværkstjenester for netværksforbundne køretøjer (ExVe) – Resultat af risikovurderingen fra ISO 20078-serien

Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078 series

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01

Tel: +45 39 96 61 01

dansk.standard@ds.dk

www.ds.dk

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

DS projekt: M333405

ICS: 43.040.15

Første del af denne publikations betegnelse er:

DS/ISO/TR, hvilket betyder, at det er en international teknisk rapport, der har status som DS-information.

Denne publikations overensstemmelse er:

IDT med: ISO/TR 23791:2019

DS-publikationen er på engelsk.

DS-publikationstyper

Dansk Standard udgiver forskellige publikationstyper.

Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard

- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information

- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog

- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte

- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives

- tillæg og rettelsesblade

DS-publikationsform

Publikationstyperne udgives i forskellig form som henholdsvis

- fuldttekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publikationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

DS-betegnelse

Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandard, eller at det er indført i hovedstandard.

DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:

Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD

- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modificeret i forhold til en given publikation.

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

First edition
2019-09-18

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

*Véhicules routiers — Web services du véhicule étendu (ExVe) —
Résultats de l'évaluation des risques de la série de normes ISO 20078*



Reference number
ISO/TR 23791:2019(E)

© ISO 2019

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

This is a preview of "DS/ISO/TR 23791:2019". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	3
4 General result of the risk assessment	3
5 Categories of the assessed risks	3
6 Assessment of the risks related to the safety of the persons and the goods during the ExVe life cycle	3
6.1 Safety risks considered.....	3
6.2 Analysis of the situation presented by the ISO 20078 series.....	4
6.2.1 SAFE 1: Possible overload of the electronic system of the moving vehicle (numerous requests).....	4
6.2.2 SAFE 2: Possible overload of the electronic system of the moving vehicle (frequent requests).....	4
6.2.3 SAFE 3: Possible overload of the electronic system of the moving vehicle (unexpected requests).....	5
6.2.4 SAFE 4: Possible illicit or malicious remote control of vehicles.....	5
6.2.5 SAFE 5: Lack of compatibility with the existing systems and mechanisms.....	5
6.2.6 SAFE 6: Failures of the remote communication solution itself of the ExVe (including the back-end system of the manufacturer).....	6
6.2.7 SAFE 7: Lack of consideration of the complete ExVe life cycle.....	6
6.2.8 SAFE 8: Risks related to the design validation process.....	6
6.2.9 SAFE 9: Lack of misuse prevention.....	6
6.2.10 SAFE 10: Lack of, or inappropriate measures aiming at reducing the risks in case of illicit or malicious remote control of vehicles.....	7
6.3 Conclusion: Assessment of the safety risks possibly originating from the ISO 20078 series.....	8
7 Assessment of the risks associated to the security of the ExVe communication system	8
7.1 Security risks considered.....	8
7.2 Analysis of the situation presented by the ISO 20078 series.....	8
7.2.1 General considerations relative to the specification of the OAuth2 framework.....	8
7.2.2 General consideration related to cybersecurity.....	8
7.2.3 SEC 1: Risks related to integrity and authenticity.....	9
7.2.4 SEC 2: Security risks at vehicle systems that are not located at the moving vehicle.....	9
7.2.5 SEC 3: Risks related to the consequences of a complete or partial cybersecurity breach (this includes safety, security, competition, confidentiality and data protection risks).....	9
7.2.6 SEC 4: Lack of misuse prevention measures.....	10
7.3 Conclusion: Assessment of the security risks possibly originating from the ISO 20078 series.....	10
8 Assessment of the risks associated to the fair competition among the concerned actors	10
8.1 Competition risks considered.....	10
8.2 Analysis of the situation presented by the ISO 20078 series.....	10
8.2.1 Involved actors.....	10
8.2.2 FAIR 1: Possible misuse of the acquired knowledge.....	11

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

8.2.3	FAIR 2: Possible gaining of unique knowledge of the market through monitoring.....	11
8.2.4	FAIR 3: Possible gaining of unique knowledge of the customer's behaviour through monitoring.....	12
8.2.5	FAIR 4: Competition risks among the involved parties	12
8.2.6	FAIR 5: Risk of excluding competitors from playing roles.....	12
8.2.7	FAIR 6: Risks related to the development of new after-sales applications	13
8.2.8	FAIR 7: Competition risks among manufacturers and/or vehicle components (systems) suppliers.....	13
8.3	Conclusion: Assessment of the competition risks possibly originating from the ISO 20078 series.....	14
9	Assessment of the risks related to the responsibility of the concerned actors	14
9.1	Liability and responsibility	14
9.2	Analysis of the situation presented by the ISO 20078 series.....	14
9.3	Conclusion: Assessment of the risks related to the responsibility of the concerned actors possibly originating from the ISO 20078 series.....	15
10	Assessment of the risks related to the protection of the resources owned by the resource owner (data protection).....	15
10.1	Data protection risks considered.....	15
10.2	Analysis of the situation presented by the ISO 20078 series.....	15
10.3	Conclusion: Assessment of the risks related to the protection of the resources owned by the resource owner and possibly originating from the ISO 20078 series (data protection risks).....	16
Annex A (informative) Assessment of safety risks.....		17
Annex B (informative) Assessment of security risks.....		26
Annex C (informative) Assessment of competition risks		29
Annex D (informative) Assessment of the risks related to responsibility and liability of the concerned actors.....		35
Annex E (informative) Assessment of data protection risks.....		37
Bibliography		39

This is a preview of "DS/ISO/TR 23791:2019". Click here to purchase the full version from the ANSI store.

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

Introduction

The [ISO 20078 series](#) specifies a possible web service to implement a certain web interface of the Extended Vehicle, depending on the concerned use case.

The development of this series has revealed several fears about possible risks related to safety, security, competition, liability, and data protection that may originate from that interface.

To address these fears, a list of criteria was first developed to be considered independently of the considered interface. This list is the object of [ISO/TR 23786](#).

This list was then used for assessing the risks originating from the [ISO 20078 series](#) and concept to issue this document.

Finally, the risk assessment demonstrated that there are no risks resulting from the [ISO 20078 series](#) itself, however, there may be risks resulting from an implementation of that series.

This is a preview of "DS/ISO/TR 23791:2019". [Click here to purchase the full version from the ANSI store.](#)

Road vehicles — Extended vehicle (ExVe) web services — Result of the risk assessment on ISO 20078 series

1 Scope

This document presents the assessment of the safety, security, competition, responsibilities, and data protection risks that can originate from the [ISO 20078](#) series.

In particular, the following risks are outside the scope of this assessment, because they relate to elements that are excluded from the scope of the [ISO 20078 series](#):

- the risks associated with the implementation of the [ISO 20078 series](#);
- the risks associated with the process that the accessing parties or any other parties would later on use to communicate the information they obtained;
- the risks associated with the process used by the resource owner to provide, modify, or revoke their authorization to pass information;
- the risks associated with the mitigation of the risks, should such a mitigation be necessary.

2 Normative references

There are no normative references in this document.