
**Intelligent transport systems —
ITS station security services for
secure session establishment and
authentication between trusted devices**





COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
5 Overview	3
5.1 Goals	3
5.2 Architecture and functional entities	4
5.3 Cryptomaterial handles	7
5.4 Session IDs and state	7
5.5 Access control and authorisation state	8
5.6 Application level non-repudiation	8
5.7 Service primitive conventions	8
6 Process flows and sequence diagrams	9
6.1 General	9
6.2 Overview of process flows	9
6.3 Sequence diagram conventions	10
6.4 Configure	11
6.5 Start Session	12
6.6 Send data	14
6.7 Send access control PDU	17
6.8 Receive PDU	18
6.9 Secure connection brokering	23
6.9.1 Goals	23
6.9.2 Prerequisites	24
6.9.3 Overview	24
6.9.4 Detailed specification	25
6.10 Force end session	33
6.11 Session terminated at session layer	35
6.12 Deactivate	35
6.13 Secure session example	36
7 Security Subsystem: interfaces and data types	38
7.1 General	38
7.2 Access control policy and state	39
7.3 Enhanced authentication	40
7.3.1 Definition and possible states	40
7.3.2 States for owner role enhanced authentication	40
7.3.3 State for accessor role enhanced authentication	41
7.3.4 Use by Access Control	42
7.3.5 Methods for providing enhanced authentication	42
7.3.6 Enhanced authentication using SPAKE2	42
7.4 Extended authentication	43
7.5 Data types	44
7.5.1 General	44
7.5.2 Imports	44
7.5.3 Iso21177AccessControlPdu	44
7.5.4 AccessControlResult	44
7.5.5 ExtendedAuthPdu	44
7.5.6 ExtendedAuthRequest	45
7.5.7 InnerExtendedAuthRequest	45
7.5.8 AtomicExtendedAuthRequest	46