



SURFACE VEHICLE RECOMMENDED PRACTICE	J1760™	OCT2019
	Issued 2001-12 Stabilized 2019-10	
	Superseding J1760 DEC2001	
Data Security Services		

RATIONALE

This technical report is being stabilized because it covers technology, products, or processes for which technical expertise no longer resides in the owning committee.

STABILIZED NOTICE

This document has been declared "Stabilized" by the SAE Motor Vehicle Council Committee and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2019 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: [SAE J1760_201910](#)

SAE values your input. To provide feedback on this Technical Report, please visit http://standards.sae.org/J1760_201910

Foreword—The ISO/CD 15764 – Road vehicles – Extended data link security International Standard requires Security Services for all data transfer between a vehicle and a diagnostic scan tool. In summary, this standard requires Authentication of the scan tool and the vehicle by a Certification Authority and all communication interchange of data to use an encryption method for every instance or session of use. The objective of this SAE J1760 Recommended Practice is to require the use of these same Security Services modified by the Class of Security required by the data to be exchanged as determined by the Resource Provider. This document requires only a one time Authentication of Security Services for the installation of an IDB Device. For a background discussion on the problem scenarios that require security, see Appendix A.

TABLE OF CONTENTS

1.	Scope	2
1.1	The IDB	3
1.2	IDB Device	3
1.3	Classes of Security.....	3
1.4	Theft Deterrent	3
1.5	Compatible IDB Devices.....	3
1.6	Data Security Service Execution	4
2.	References	4
2.1	Applicable Documents	4
2.2	Related Publications	4
3.	Definitions.....	4
3.1	Access	4
3.2	Authenticated Device	4
3.3	Authentication	4
3.4	Certification Authority	4
3.5	Ciphertext	4
3.6	Classes of Security.....	5
3.7	Decryption	5
3.8	Device Resource Privileges	5
3.9	Eavesdropping	5
3.10	Encryption	5
3.11	Hash Function	5
3.12	IDB Device	5

3.13	IDB Gateway.....	5
3.14	Manipulation	5
3.15	Masquerading	5
3.16	Passwords or PINs	5
3.17	Private Encryption Key	5
3.18	Private Key	5
3.19	Proxy.....	5
3.20	Public Encryption Key.....	5
3.21	Public Key	5
3.22	Resource Provider	5
3.23	Security Breach	5
3.24	Security Service.....	5
3.25	Symmetric Key.....	6
4.	Abbreviations/Acronyms	6
5.	Functional Requirements	6
5.1	Authentication	6
5.2	Access	6
5.3	Message Security	6
5.4	Security Breach Avoidance	6
5.5	Vehicle Device Transfer.....	6
5.6	Usability	7
6.	Security Model	7
6.1	Security Levels of IDB Device Resources	7
6.2	Enabling Security.....	8
6.3	Disabling Security	8
6.4	Process of authentication by Certification Authority	8
6.5	The Process to Establish an Ability to Conduct Secured Communication on the IDB Network between Device Pairs.....	9
Appendix A	Problem Scenarios that Require Security.....	10
A.1	Background	10
A.2	Need for Data Security	10
A.3	Assure Proper Function	10
A.4	Disable and discourage the use of stolen ITS modules	10

- 1. Scope**—The scope of this SAE Recommended Practice is to require the use of the same Security Services as defined by the International Standard ISO/CD 15764, modified by the Class of Security as determined by the resource provider and referenced in Table 1, Extended Data Link Security References.

**TABLE 1—EXTENDED DATA LINK SECURITY INTERNATIONAL
STANDARD ISO/CD 15764 REFERENCES**

Parameter	References	Values
Hashing Function	ISO/IEC 9797-2 ISO/IEC 10118-3	
Symmetric Key	ANSI X 9.52	128 bits
Public Key	ISO/IEC 11770-1 ISO/IEC 11770-3	1024 bits modulus 1024 bits exponent
Private Key	ISO/IEC 11770-1	1024 bits modulus 1024 bits exponent

- 1.1 The IDB Gateway**—The IDB Gateway shall be considered an IDB Device operating on the IDB network. This SAE J1760 Data Security Services Recommended Practice defines security, when deemed necessary, between devices on the IDB, as granted by the resource providers. The Security Services required between the IDB Gateway and the vehicle are not within the scope of this document.
- 1.2 IDB Device Functions**—The device functions may be represented by “proxy”. Therefore devices such as those that are connected to the IDB may be a communication mechanism, external to the bounded vehicle communication system and shall by “proxy” be protected by the Authentication of Security Services required by this document. The Security Services required between the IDB network and outside the bounded vehicle communication system shall be within the scope of this document. (Reference Figure 1 for a data security services system diagram.)
- 1.3 Classes of Security**—Various capabilities (messages) shall be protected by different classes of security as required by 6.1. Security Services, which involve the transmission and/or reception of only Class 0 resources, are not within the scope of this document.
- 1.4 Theft Deterrent**—The data security services shall provide a mechanism that will discourage the theft of IDB Devices

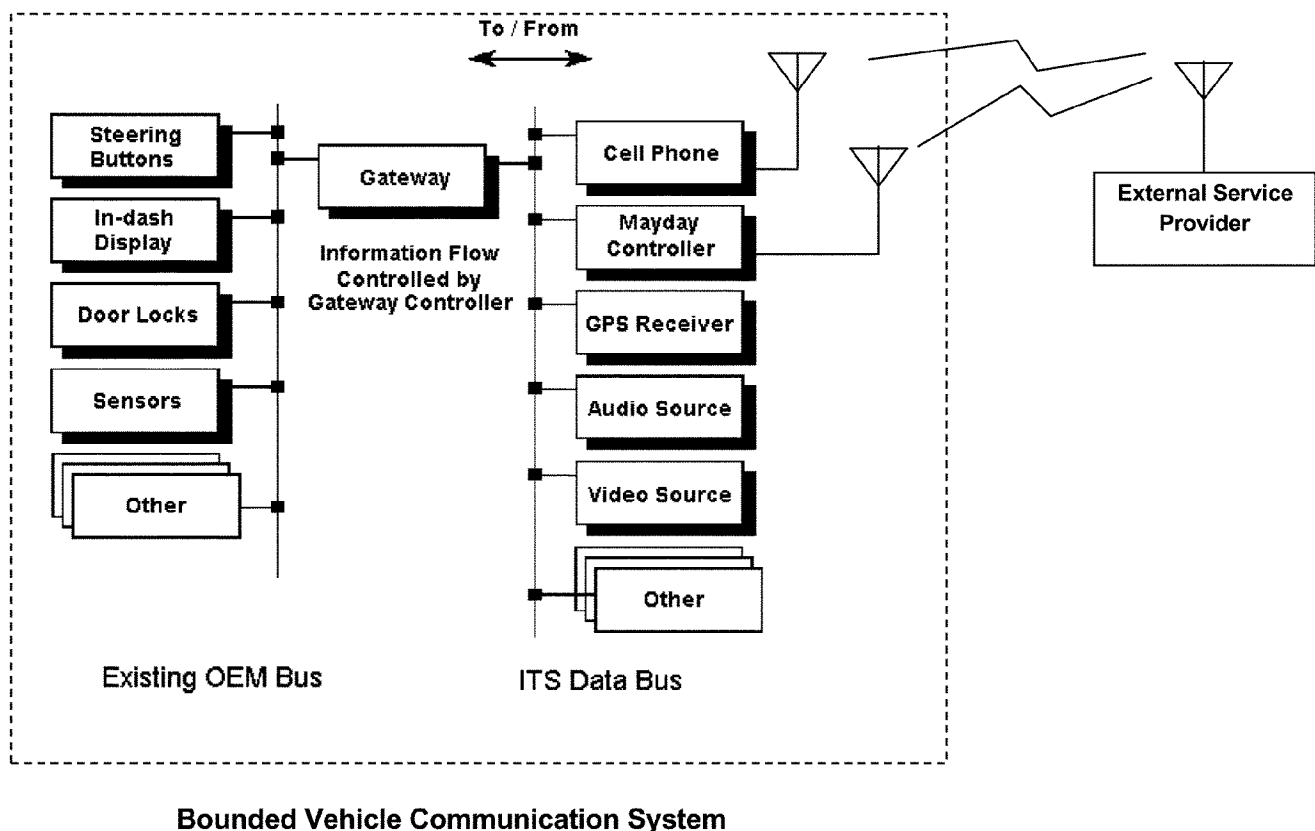


FIGURE 1—DATA SECURITY SERVICE SYSTEM DIAGRAM

- 1.5 Compatible IDB Devices**—All IDB Devices operating on the IDB network that claim to be IDB compatible and utilize resources from an IDB compatible device shall comply with the requirements set forth in this Recommended Practice.