
**Financial services — Key-
management-related data element —
Application and usage of ISO 8583-1
data elements for encryption**

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13492:2019

<https://standards.iteh.ai/catalog/standards/iso/b64301f9-cb68-4d1c-9988-c8fc3e49a096/iso-13492-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 13492:2019

<https://standards.iteh.ai/catalog/standards/iso/b64301f9-cb68-4d1c-9988-c8fc3e49a096/iso-13492-2019>



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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Data representation	3
6 Requirements for key-management-related data element	3
6.1 Introduction.....	3
6.2 Data element structure.....	4
6.2.1 Data element structure for field 53 and 96.....	4
6.2.2 Data element structure for field 50, 110, 111.....	6
6.3 Key-set identifier concepts.....	10
7 Security related control information usage format	11
7.1 Control field format.....	11
7.2 Key-set identifier.....	11
7.2.1 Format A.....	11
7.2.2 Format B.....	11
7.3 Algorithm field.....	11
7.4 Key length (in bytes) field.....	12
7.5 Key protection field.....	12
7.6 Padding method field.....	12
7.7 Encrypted data format field.....	13
Bibliography	14

ISO 13492:2019

<https://standards.iteh.ai/catalog/standards/iso/b64301f9-cb68-4d1c-9988-c8fc3e49a096/iso-13492-2019>

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 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This third edition cancels and replaces the second edition (ISO 13492:2007), which has been technically revised.

The main changes compared to the previous edition are as follows:

— introduction of the support of the AES encryption algorithm, resulting in a complete restructuring and editing of the previous edition.

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.