
**Information security — Lightweight
cryptography —**

**Part 7:
Broadcast authentication protocols**

*Sécurité de l'information — Cryptographie pour environnements
contraints —*

Partie 7: Protocole d'authentification diffusée

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

[ISO/IEC 29192-7:2019](https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019)

<https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019>



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

[ISO/IEC 29192-7:2019](https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019)

<https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 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 Symbols and abbreviated terms	3
5 TESLA-RD (Timed Efficient Stream Loss-tolerant Authentication — Rapid Disclosure)	4
5.1 General	4
5.2 Initialization	4
5.3 Setup	4
5.4 Sending a message	5
5.5 Receiving a message	5
5.6 Verifying the key	5
5.7 Verifying the message	5
Annex A (normative) Object identifiers	6
Bibliography	7

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

[ISO/IEC 29192-7:2019](https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019)

<https://standards.iteh.ai/catalog/standards/iso/0edec12e-7ff6-41b8-8d35-5cd89c0bbbd6/iso-iec-29192-7-2019>