

---

---

**Information security — Redaction of  
authentic data —**

**Part 1:  
General**

*Sécurité de l'information — Rédaction de données authentifiées —*

*Partie 1: Généralités*

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

[ISO/IEC 23264-1:2021](https://standards.iteh.ai/catalog/standards/iso/fl1e3e300-a08c-4aea-b669-9108cc01c578/iso-iec-23264-1-2021)

<https://standards.iteh.ai/catalog/standards/iso/fl1e3e300-a08c-4aea-b669-9108cc01c578/iso-iec-23264-1-2021>



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

[ISO/IEC 23264-1:2021](https://standards.iteh.ai/catalog/standards/iso/fl1e3e300-a08c-4aea-b669-9108cc01c578/iso-iec-23264-1-2021)

<https://standards.iteh.ai/catalog/standards/iso/fl1e3e300-a08c-4aea-b669-9108cc01c578/iso-iec-23264-1-2021>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2021

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  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and conventions</b> .....	<b>5</b>
4.1 Symbols.....	5
4.2 Conventions.....	5
<b>5 General model and processes</b> .....	<b>5</b>
5.1 General.....	5
5.2 Parties and processes.....	5
5.3 General model.....	6
5.4 Specification of processes.....	7
5.4.1 Key generation process.....	7
5.4.2 Redactable attestation process.....	7
5.4.3 Redaction process.....	8
5.4.4 Verification process.....	8
<b>6 Cryptographic properties of redactable attestation schemes</b> .....	<b>9</b>
6.1 Required cryptographic properties.....	9
6.1.1 Correctness.....	9
6.1.2 Unforgeability.....	9
6.1.3 Privacy.....	9
6.2 Optional cryptographic properties.....	10
6.2.1 Undetectability of redactions.....	10
6.2.2 Detectability of redactions.....	10
6.2.3 Unlinkability of redactions.....	10
6.2.4 Disclosure control.....	10
6.2.5 Consecutive redaction control.....	10
6.2.6 Mergeability.....	10
<b>Bibliography</b> .....	<b>11</b>