INTERNATIONAL STANDARD

ISO/IEC 23000-21

First edition
2019-07

Information technology — Multimedia application format (MPEG-A) —

Part 21: Visual identity management application format

Technologies de l'information — Format pour application multimédia (MPEG-A) —

Partie 21: Format pour application de gestion d'identité visuelle

Reference number
ISO/IEC 23000-21:2019(E)

Documents
Document Sharing Hub

© ISO/IEC 2019

Full document details: ISO IEC 23000-21-2019

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

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO IEC 23000-21-2019

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **2**

5 System for identity privacy management ... **2**
- 5.1 General framework ... 2
- 5.2 Applying privacy protection in ISO/IEC 21000-22 ... 4
  - 5.2.1 General description ... 4
  - 5.2.2 User description ... 5
  - 5.2.3 Context description ... 9
  - 5.2.4 Service description ... 12

6 Content sensitive encryption ... **14**
- 6.1 Overview of content sensitive encryption ... 14
- 6.2 Content sensitive encryption for Rec. ITU-T H.264 | ISO/IEC 14496-10 ... 15
  - 6.2.1 General ... 15
  - 6.2.2 Content sensitive encryption with CAVLC entropic coding ... 15
  - 6.2.3 Content sensitive encryption with CABAC entropic coding ... 16
- 6.3 Content sensitive encryption for HEVC ... 17
- 6.4 Content sensitive encryption for region encryption ... 17
  - 6.4.1 General ... 17
  - 6.4.2 AVC ... 17
  - 6.4.3 HEVC ... 20

7 Support for protected streams at system level ... **21**
- 7.1 Signalization of protected stream ... 21
- 7.2 Signal of multiple access in protected stream ... 22
- 7.3 Signal of content sensitive encryption ... 27
  - 7.3.1 Definition of content sensitive encryption ... 27
  - 7.3.2 Content sensitive encryption applied to a video NAL unit ... 28
  - 7.3.3 `'sve1'` AES-CTR sensitive encryption scheme ... 28

Annex A (normative) **Content sensitive encryption scheme** ... **30**

Bibliography ... **39**

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO IEC 23000-21-2019

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 and IEC 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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

A list of all parts in the ISO/IEC 23000 series can be found on the ISO website.

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.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

Introduction

The main goal of the ISO/IEC 23000 series (also known as "MPEG-A") is to facilitate the swift development of innovative, standards-based multimedia services and applications by selecting and combining readily tested and verified tools taken from the MPEG body of standards.

Visual identity management is designed to enable users to control and manage privacy protection by defining a new framework and tools. It also provides to industry a coherent and consistent approach to manage privacy protection in order to be implemented in a variety of scenarios, applications or systems.

The main objective of preserving privacy protection is to enable security and confidentiality in the multimedia content chain. Many usages of image/video communication services, social networking and video sharing platforms have led to an increasing interest to protect users' privacy.

Traditionally, multimedia data security is achieved by cryptography solutions, which deal with encryption of data. This approach is called Naive Encryption Algorithm (NEA) and it treats the video bitstream as text data without paying attention to the structure of the compressed video. To this end, MPEG common encryption has been standardized in order to support encryption and key mapping methods for file format in ISO/IEC 23001-7 and for transport streaming in ISO/IEC 23001-9[3]. Consequently, bitstreams encrypted by those documents are decodable only after a correct decryption process even when only parts of the video are encrypted. Nevertheless, none of these formats allow signalling the encryption of a part of the picture (region), or indicating to the decoder that the encrypted bitstream can be partially decoded.

Moreover, all the access control is provided and performed globally without taking into account the image/video content and context. To restore citizens' confidence in online data collection practices, submitted media should be encrypted to protect privacy and only viewed with limited access that the user chooses: group of people, purpose of sharing, time, date, metadata, etc.

In order to provide privacy protection over processing and sharing of multimedia content, a flexible, effective and scalable mechanism is required to provide users a way to express their control desires in a form that can be processed and monitored systematically, consistently and persistently throughout the lifecycle of the multimedia content. There is currently no standardized format to represent privacy description information (PDI), hindering the interoperability between secured systems.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

Documents
Document Sharing Hub

Full document details: ISO IEC 23000-21-2019

Information technology — Multimedia application format (MPEG-A) —

Part 21: Visual identity management application format

1 Scope

This document specifies the standard representation of the set of signalling and data used in the process of preserving privacy for storage sharing image/video.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Rec. ITU-T H.264 | ISO/IEC 14496-10:—[1], *Information technology — Coding of audio-visual objects — Part 10: Advanced Video Coding*

ISO/IEC 14496-15, *Information technology — Coding of audio-visual objects — Part 15: Carriage of network abstraction layer (NAL) unit structured video in the ISO base media file format*

ISO/IEC 23001-7:2016, *Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files*

Rec. ITU-T H.265 | ISO/IEC 23008-2:—[2], *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 2: High efficiency video coding*

ISO/IEC 23008-12, *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 12: Image File Format*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 14496-10, ISO/IEC 23008-2, ISO/IEC 23008-12 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
CSE
content sensitive encryption
selective encryption
image or video content protection scheme that can encrypt only a subset of the compressed bitstream data, preserving format compliant

1) Under preparation. Stage at the time of publication: ISO/IEC/DIS 14496-10:2018.

2) Under preparation. Stage at the time of publication: ISO/IEC/DIS 23008-2:2018.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

3.2
privacy description management
entity capable of managing the access control of different regions and associated with different authorizations

3.3
ROI
region of interest
sample or subset of an image within a media, identified for a particular purpose

4 Abbreviated terms

AVC	advanced video coding (as specified by Rec. ITU-T H.264 | ISO/IEC 14496-10)
CABAC	context-adaptive binary arithmetic coding (as specified in Rec. ITU-T H.264 | ISO/IEC 14496-10 and in Rec. ITU-T H.265 | ISO/IEC 23008-2)
CAVLC	context-adaptive variable-length coding (as specified in Rec. ITU-T H.264 | ISO/IEC 14496-10)
CTU	coding transform unit (as specified by Rec. ITU-T H.265 | ISO/IEC 23008-2)
HEVC	high efficiency video coding (as specified by Rec. ITU-T H.265 | ISO/IEC 23008-2)
MB	Macroblock unit (as specified by Rec. ITU-T H.264 | ISO/IEC 14496-10)
MPEG 21 UD	MPEG 21 user description (as specified by ISO/IEC 21000-22)
NAL	network abstraction layer (as specified in Rec. ITU-T H.264 | ISO/IEC 14496-10 and in Rec. ITU-T H.265 | ISO/IEC 23008-2)
SEI	supplemental enhancement information (as specified in Rec. ITU-T H.264 | ISO/IEC 14496-10 and in Rec. ITU-T H.265 | ISO/IEC 23008-2)

5 System for identity privacy management

5.1 General framework

To protect privacy content, stored and/or shared media should be encrypted by the service's user and should only be viewed with a well-defined limited access (group of people, purpose of sharing, time, date, metadata, etc.). Consequently, some particular regions of the video (e.g. human faces, text data) can only be seen by the authorized users, regardless of who captures and shares the video. Additionally, since multiple regions sometimes need different protections (e.g. multiple faces shown in the video), there is also a need to manage different control access (i.e. different key identifiers) within the same video bitstream, potentially for each frame, as shown in Figure 1.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

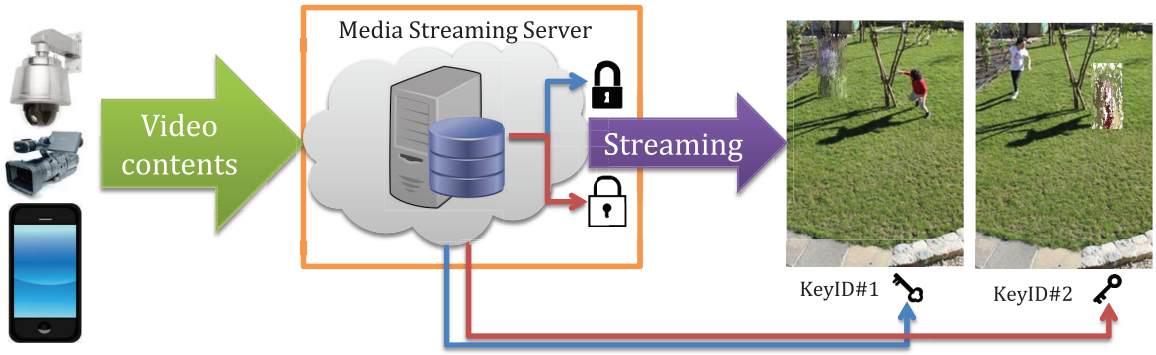

Figure 1 — Privacy management in multimedia streaming applications

Figure 2 illustrates an example of framework for managing the privacy of users when pictures or videos are taken and shared among users with different keys.

NOTE Key management is outside the scope of this document.

The steps of the privacy protection mechanism can be expressed as follows (see also Figure 2):

1. User 1:
   a. Capture a media.
   b. Select part of the media considered as 'private' or/and let an application detect and recognize automatically faces.
   c. Transmit information to the privacy description management.
2. Privacy description management:
   a. Get information and manage access control thanks to privacy policy defined by User 1 with the different relative user descriptions, potentially taking into account context descriptions and/ or service descriptions through the recommendation engine.
   b. Send a unique ID of the media, and a list of encryption keys associated to different part of the media.
3. User 1:
   a. Generation (i.e. compression and encapsulation) of media file with an encryption scheme fed by the list of encryption keys and their locations.
   b. Storage or transmission to dedicated server for media sharing.
4. User 2:
   a. Get media file.
   b. Send the ID of media and associated context and user description to privacy description management.
5. Privacy description management:
   a. Use the transmitted information through the recommendation engine to evaluate whether the user can be totally or partially authorized to render the associated media.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

b. Send decryption keys adapted to the users that are allowed or not to see each part of the media.

6. User 2:

a. Get decryption keys.

b. Render (i.e. de-capsulate and decompress) media with an appropriated decryption scheme depending on associated authorization.

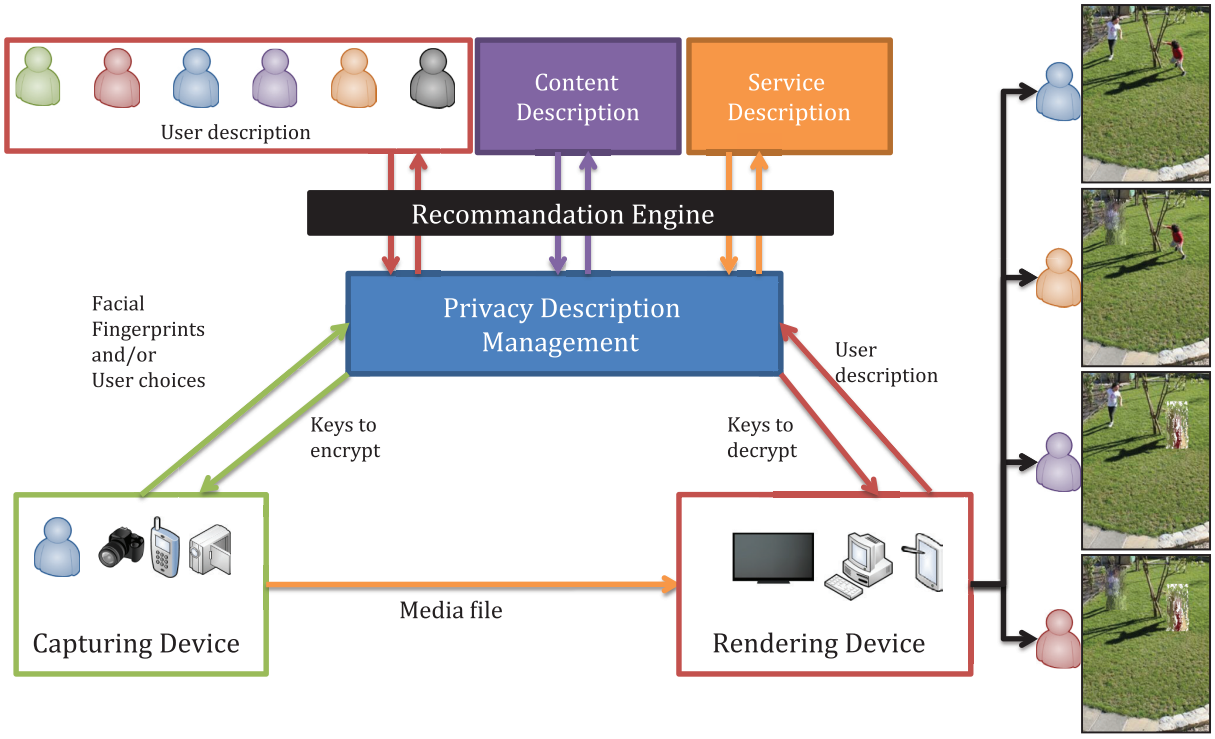

Figure 2 — Proposed framework for privacy management of media

ISO/IEC 15938-13[5] should be used to represent the fingerprint of the face of a user in a picture. For video, compact descriptors for video analysis (ISO/IEC 15938-15[6][3]) can be used. To define the area that needs to be protected, it can be selected manually or automatically, but this process is out of the scope of this document.

5.2 Applying privacy protection in ISO/IEC 21000-22

5.2.1 General description

5.2.1.1 General

This subclause refers to ISO/IEC 21000-22:—[2][4], Clause 4, that defines basic properties of each sub-element for UD (user description), CD (context description), SD (service description) and RD (recommendation description).

NOTE To consider privacy issues, several modifications and new specific types have been added to fit the requirements of ISO/IEC 21000-22.

3) Under preparation. Stage at the time of publication: ISO/IEC/FDIS 15938-15:2019.

4) Under preparation. Stage at the time of publication: ISO/IEC/FDIS 21000-22:2019.

© ISO/IEC 2019 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

5.2.1.2 InformationAccessUserGroup

5.2.1.2.1 Syntax

This syntax is `InformationAccessUserGroup` type.

```
<complexType name="InformationAccessUserGroup">
   <sequence>
      <element name="UserID" type="mpeg7:UserIdentifierType" maxOccurs="unbounded"/>
   </sequence>
   <attribute name="GroupID" type="anyURI"/>
</complexType>
```

`InformationAccessUserGroup` type has `InformationAccessID` type. `InformationAccessID` describes the list of other users who can access private information.

5.2.1.2.2 Semantics

Semantics of the `InformationAccessUserGroup` is given in Table 1.

Table 1 — Semantics of the `InformationAccessUserGroup`

Name	Definition
`InformationAccessUserGroup`	Describes the group of other users who can access private information.
`UserID`	Specifies the list of user's ID belonging to the group that can access private information.
`GroupID`	Specifies the identifier of the group.

5.2.2 User description

5.2.2.1 General

This subclause specifies user description (UD), which contains root elements at the basis of individual use cases.

5.2.2.2 BaseUserType

5.2.2.2.1 General

`BaseUserType` was created in `UserDescription`, and `InformationAccessID` and `InformationAccessID` were added to `BaseUserType`.

`InformationAccessID` describes the list of other users who can access private information of a given user. `InformationAccessGroupURI` references groups of users who can access private information.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

5.2.2.2.2 Syntax

This syntax is `BaseUserType` type.

```
<complexType name="BaseUserType" abstract="true">
   <sequence>
      <element name="InformationAccessID" type="mpeg7:UserIdentifierType" minOccurs="0"
maxOccurs="unbounded"/>
      <element name="InformationAccessGroupURI" type="anyURI" minOccurs="0"
maxOccurs="unbounded"/>
   </sequence>
</complexType>
```

5.2.2.2.3 Semantics

Semantics of the `BaseUserType` type is given in Table 2.

Table 2 — Semantics of the `BaseUserType`

Name	Definition
`BaseUserType`	`BaseUserType` is an abstract type providing a base for description of each element.
`InformationAccessID`	Specifies the list of user's ID of other users who can access private information.
`InformationAccessGroupURI`	References groups of users who can access private information through the specification of its URI. Refer to the `GroupID` of `InformationAccessUserGroup` in `General Description`.

5.2.2.3 UserDescriptionType

5.2.2.3.1 General

This subclause describes a structure of `UserDescriptionType` data type. The `UserDescriptionType` contains several elements as the `InformationAccessGroup` that has been added and which specifies a list of users who can access the privacy information.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

5.2.2.3.2 Syntax

```
<complexType name="UD">
  <complexContent>
     <extension base="ud:BaseUserType">
             <sequence>
                  <element name="InformationAccessGroup"
type="ct:InformationAccessUserGroup" minOccurs="0" maxOccurs="unbounded"/>
                  <element name="ClassificationSchemeAlias"
type="ct:ClassificationSchemeAliasType" minOccurs="0" maxOccurs="unbounded"/>
                  <element name="UserID" type="mpeg7:UniqueIDType"/>
                  <element name="UserProfile" type="ud:UserProfileType" minOccurs="0"/>
                  <element name="UsageHistory" type="ud:UsageHistoryType" minOccurs="0"/>
                  <element name="Preference" type="ud:PreferenceType" minOccurs="0"/>
                  <element name="Emotion" type="ud:EmotionType" minOccurs="0"/>
                  <element name="Schedule" type="ud:ScheduleType" minOccurs="0"/>
                  <element name="Activity" type="ud:ActivityType" minOccurs="0"/>
                  <element name="Representation" type="ct:ObjectType" minOccurs="0"/>
                  <element name="Intention" type="ud:IntentionType" minOccurs="0"/>
                  <element name="Knowledge" type="ud:KnowledgeType" minOccurs="0"/>
                  <element name="ObjectSharing" type="ud:ObjectSharingType"
minOccurs="0"/>
                  <element name="ServiceUsagePattern" type="ud:UsagePatternType"
minOccurs="0"/>
                  <element name="LoudnessPreferences" type="ud:LoudnessPreferencesType"/>
                  <element name="VisualExpressionPreference" type="ud:
VisualExpressionPreferenceType"/>
            </sequence>
            <attributeGroup ref="ct:commonAttributes"/>
     </extension>
  </complexContent>
</complexType>
```

5.2.2.3.3 Semantics

Semantics of the `UserDescriptionType` is given in Table 3.

Table 3 — Semantics of the `UserDescriptionType`

Name	Definition
`UD`	Serves as the root element of the MPEG 21 UD format. The `UD` element shall be used as the topmost element to make user description in an instance of MPEG 21 UD format.
`UserDescriptionType`	Specifies the syntax of the root element. This datatype is a set of descriptions which may contain static and dynamic information about user. Within this Type, `UserProfile`, `Preference`, `Emotion`, `Schedule` or `Activity` element shall be instantiated.
`InformationAccessGroup`	Describes the group of other users who can access private information.

© ISO/IEC 2019 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019

Table 3 *(continued)*

Name	Definition
`ClassificationSchemeAlias`	Specifies an alias for a `ClassificationScheme` to be referenced within the `UserDescriptionType` by a simplified URI.
`UserID`	Describes the unique identifier of a user.
`UserProfile`	Describes user profile based on `UserProfileType`.
`UsageHistory`	Describes usage history based on `UsageHistoryType`. This element can represent user's history for a given service, such as searching or movie recommendations.
`Preference`	Describes preference based on `PreferenceType`.
`Emotion`	Describes emotion based on `EmotionType`. This type represents user's emotion, including its changes over time.
`Schedule`	Describes schedule based on `ScheduleType`.
`Activity`	Describes user activity based on `ActivityType`.
`Representation`	Describes the representation such as user character and image used by the user. This element can be used to describe user character on the social network.
`Intention`	Describes a list of intentions related to specific actions which a given user may perform with a multimedia object.
`Knowledge`	Describes a piece of knowledge that the user wants to share for recommendation purposes.
`ObjectSharing`	Describes the condition of authority (e.g. ID, ownership and accessibility of object) for the sharing and accessing of object to user or external service.
`UsagePattern`	Describes various patterns about usage of user based on `UsagePatternType`. Users use a lot of applications and services for a variety of reasons. `Usagepattern` can be used to figure out user's characteristics.
`commonAttributes`	Describes a group of attributes for the `CommonAttributes`. The syntax and semantics of `commonAttributes` are specified in General Description (see ISO/IEC 21000-22:—, Clause 4).
`ServiceUsagePattern`	
`LoudnessPreferences`	Describes static or dynamic personal and group audio preferences (e.g. audio levels, audio level history, and song preferences) and the usage history which helps with selecting appropriate audio service.
`VisualExpressionPreference`	A set of data edited by user's intention/emotion or created by recognizing user's situation/condition.

© ISO/IEC 2019 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO IEC 23000-21-2019