International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 31
(09/2017)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things

ITU-T X-series Recommendations – Supplement 31

International
Telecommunication
Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed legder technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 31 to ITU-T X-series Recommendations

ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things

Summary

Supplement 31 to the ITU-T X-series Recommendations provides guidelines on how to use object identifiers (OIDs) to identify objects in the Internet of things (IoT). It includes guidelines on how to structure OIDs, how to implement resolution systems as well as how to establish management procedures based on existing ITU-T Recommendations and international standards.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X Suppl. 31	2017-09-06	17	11.1002/1000/13411

Keywords

Internet of things, object identifiers, OID, identification system.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 31 to ITU-T X-series Recommendations

ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things

1 Scope

This Supplement includes the following items:

- requirements for identifying objects in the Internet of things (IoT) and how object identifiers (OIDs) satisfy these requirements;
- general procedures for establishing OID-based IoT identification systems;
- detailed considerations for establishing OID-based IoT identification systems, including considerations when designing/choosing identification schemes for OIDs, considerations when establishing a resolution system and considerations when establishing OID authorities and operational procedures.

2 References

[ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*

[ITU-T X.672] Recommendation ITU-T X.672 (2010) | ISO/IEC 29168-1:2011, *Information technology – Open systems interconnection – Object identifier resolution system (ORS).*

[ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

[ITU-T Y.4801] Recommendation ITU-T Y.4801/F.748.1 (2014), *Requirements and common characteristics of IoT identifier for the IoT service.*

[ISO/IEC 10646] ISO/IEC 10646:2014, *Information technology Universal Coded Character Set (UCS).*

[ISO/IEC 29168-2] ISO/IEC 29168-2:2011, *Information technology – Open systems interconnection – Part 2: Procedures for the object identifier resolution system operational agency.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 application-specific OID resolution process [ITU-T X.672]: Actions by an application to retrieve application-specific information from the information returned by the general OID resolution process.

3.1.2 general OID resolution process [ITU-T X.672]: That part of the ORS where an ORS client obtains information from the DNS (recorded in a zone file) about any specified OID and returns it to an application.

3.1.3 object identifier [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.4 registration [ITU-T X.660]: The assignment of an unambiguous name to an object in a way which makes the assignment available to interested parties.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

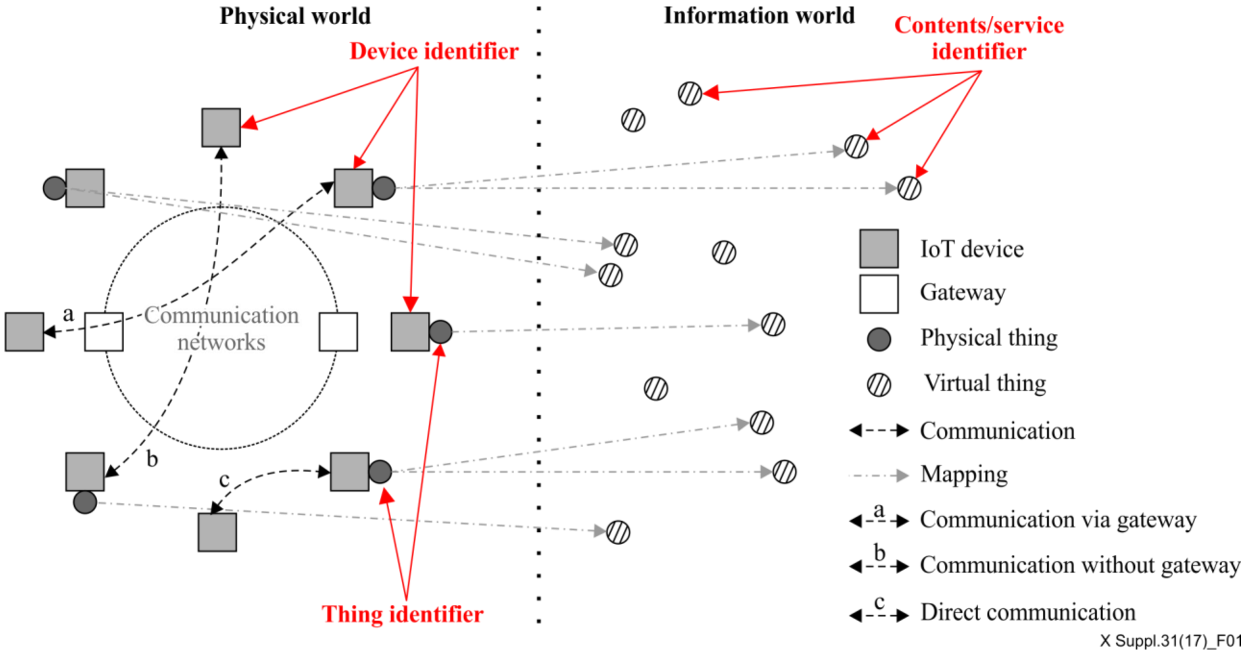
AIDC	Automatic Identification and Data Collection
APP	Application
DNS	Domain Name System
IoT	Internet of Things
OID	Object Identifier
OID-IRI	Object Identifier – Internationalized Resource Identifier
ORS	OID Resolution System
RFID	Radio Frequency Identification
SNMP	Simple Network Management Protocol

5 Conventions

None.

6 The target and requirements of identifying objects in the IoT

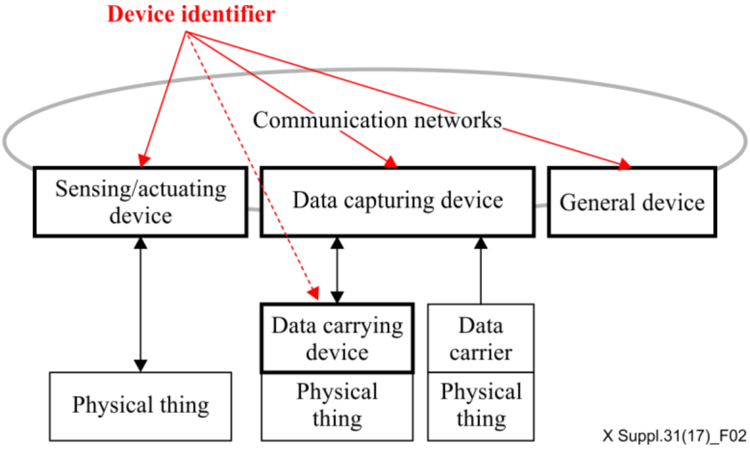
In IoT, every "thing" should be identified by a globally or locally unique identifier to be accessed as shown in Figure 1. There are some special situations where these "things" do not need global and unique identifiers, but they have to be unique in a local environment.



Source: Modified from [ITU-T Y.2060].

Figure 1 – Targets of identification in the IoT

There are some typical IoT devices that are used to support the connection of every "thing" to the IoT, and these devices are identified as shown in Figure 2, according to [ITU-T Y.2060]. Among these four types of devices, data carrying devices can be identified by radio frequency identification (RFID) since these will be attached to physical things such as boxes and bottles.



Source: modified from [ITU-T Y.2060].

Figure 2 – Types of devices to be identified in the IoT

The requirements of identifying objects in IoT are specified in [ITU-T Y.4801].

7 Characteristics of object identifiers useful for IoT

7.1 Overview

Object identifiers (OIDs) are jointly developed by ISO/IEC and ITU-T, and have many characteristics. OIDs satisfy the requirements of clause 6 as explained below.

7.2 Identifying anything

An OID has a hierarchical tree structure, which can flexibly extend its layers and the length of the identifiers. An OID is able to identify anything (physical or virtual, devices or non-devices), and is able to connect them with global information and communication infrastructures.

7.3 Communication between things

An OID has independent arcs under its top level, and can accommodate short-range communication technologies.

An OID is also used to identify things in which communication capabilities are unnecessary, such as digital certificates, algorithms and organizations. Thus, an OID is able to provide a harmonized way to integrate the identifiers of devices, which need communication capabilities, and the identifiers of things, which do not.

7.4 Association between physical and virtual objects

An OID can be used for tag-based identification to associate a physical object with its information stored in servers. OIDs have also been used extensively in network device management and various data and data structures. The concept of OIDs integrates the identifiers of physical objects and the identifiers of virtual objects.

7.5 Networking technology independency of IoT devices

In IoT environments, numerous devices may connect to each other using different networking technologies. OIDs are independent of networking technologies and have been widely used to identify objects in different networking contexts, such as simple network management protocol (SNMP)-enabled network management systems, data structures of databases, cloud storage objects of cloud computing, etc.

7.6 Mapping identifiers to objects

An OID is a type of universal identifier that can be used to identify things from different layers, including identifier schemes which are used to identify different kinds of things, such as radio frequency identification (RFID), 2-dimensional (2D) barcode, etc. The character encoding technology specified in [ISO/IEC 10646] could be used with OIDs to offer various formats of characters, such as the object identifier - internationalized resource identifier (OID-IRI). OIDs can be supported by various OID resolution services as specified in [ITU-T X.672]. Therefore, an OID satisfy the requirement of mapping identifiers to objects in different layers and can integrate them easily.

8 General procedure for establishing OID-based IoT identification systems

This clause introduces the general procedure for establishing an OID-based IoT identifier system for a specific application area, as follows:

Step 1: Analysis of business requirements: Analyse what kind of objects should be identified.

Step 2: Classification of objects: Categorize the objects in IoT according to their characteristics.

Step 3: Design for the structure of OID: More details for step 1, step 2 and step 3 can be found in clause 9.

Step 4: Deployment of OID resolution system (ORS): Address how to establish resolution systems and how to deploy distributed servers. More details can be found in clause 10.

Step 5: Establishing authorities and procedures: Administrative authorities and operational procedures should be established. Additional details can be found in clause 11.

The general procedure for establishing OID-based IoT identifier systems is described in Figure 3.

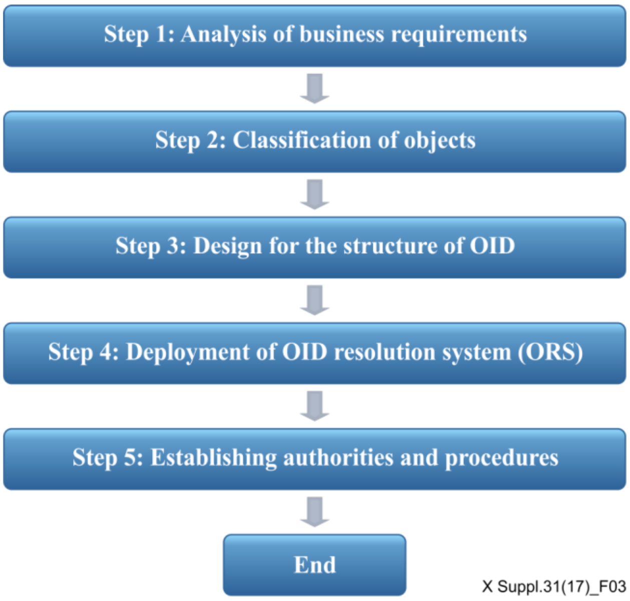

Step 1: Analysis of business requirements
Step 2: Classification of objects
Step 3: Design for the structure of OID
Step 4: Deployment of OID resolution system (ORS)
Step 5: Establishing authorities and procedures
End
X Suppl.31(17)_F03

Figure 3 – General procedure of establishing OID-based IoT identification systems

9 Considerations when designing/choosing identification schemes for OIDs

9.1 Factors considered for identification schemes

There are many factors that should be considered when designing/choosing identification schemes for OIDs.

Before designing OID identification schemes for IoT objects, the business requirements of the IoT application should be analysed first. The kind of objects that need to be identified should be determined.

Normally, objects in IoT can be classified into two types, that is, physical things and virtual things. Typical physical things include people, organizations, products, vehicles, etc. Virtual things generally include metadata, algorithms, etc.

Generally, identifiers assigned to IoT things will be either permanent or temporary (i.e., vanish after their time-to-live). For each IoT object, its OID should remain unchanged for its whole lifetime, no matter how long its lifetime is.

Existing identification situations and management mechanisms in the IoT applications should be analysed as sometimes, different identifier systems have already been used in those applications. In such a case, OIDs should be compatible with the existing identification schemes. If there are no existing identification schemes, new identification schemes should be designed based on the management mechanism and characteristics of objects.

9.2 Recommended structures of OIDs in IoT

9.2.1 Various situations for structures of OIDs

In general, there are two types of structures of OIDs that are recommended in IoT.

There is one type of OID structure that is used for identification schemes that are widely applied to identify various objects, such as organizations, goods, persons, vehicles, etc. Clause 9.2.2 defines a method that can be used to transform other identifiers from existing identification schemes into OIDs. In addition, there are strict limits for identification schemes which should contain numeric characters compatible with OID syntax, since an OID is an ordered list of primary integer values.

The second type of OID structure is used for new identification schemes, and the details of the procedure are given in clause 9.2.3.

9.2.2 Existing identification schemes to be a part of OID

If an identifier that consists of numeric characters that are compatible with an OID syntax and is used in a particular field is to be transformed into an OID, there are many ways to achieve this goal. Below are three examples:

1) get an assignment under the OID arc of a particular field;

2) get an assignment under any OID arcs that are available in each country – a tag-based scheme could be assigned an OID under the OID arc of its owner's country;

3) publish an ITU-T Recommendation | International Standard for that existing identification scheme, which can then obtain an OID arc under `{iso(1) standard(0)}` or `{itu-t(0) recommendation(0)}`.

9.2.3 New identification schemes designed under an OID arc

There are several key factors that should be considered as constituent parts of a new OID assignment scheme, such as registration authority ID, category ID, entity ID, etc. A complete OID would be a combination of these key factors and each constituent part is separated from one another by "." Flat management is recommended to be used for each constituent part.

Detailed information of OID constituent parts is given in Table 1.

Table 1 – Detailed information of OID constituent parts

Constituent part	Mandatory/ optional	Hierarchical layers recommended	Interpretation
Registration authority ID	M	Consistent with actual management structure	Registration authority ID (could include a country ID or combination of country ID, province ID and city ID). Each level of registration authority ID should be allocated by the upper level registration authority.
Category ID	O	One or more layers	Category (and subcategories) of an object in application field, such as people, departments, standards, etc.
Entity ID	M	One layer	Unique number allocated to an entity (usually as a combination of batch number and product ID).

If a new identification scheme is designed, then the recommended OID structure should be as shown in Figure 4.

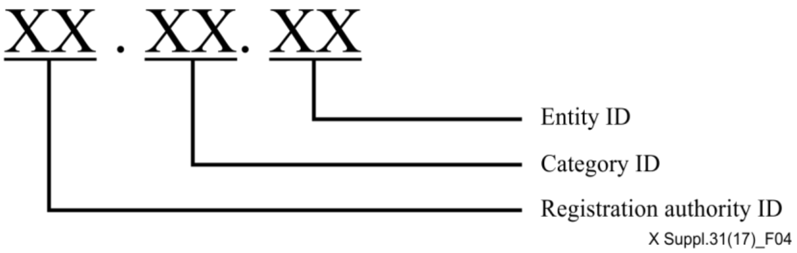


Figure 4 – Structure of OIDs for objects managed by multiple levels of registration authorities

OID may be used in auto identification and data collection (AIDC) technologies for unique identification of any physical things. Different AIDC technologies have their own characteristics. For example, RFID can capture data automatically and rapidly, but has higher costs, whereas a 2D barcode could be scanned more easily and has lower cost. Thus, RFID is more often adopted by objects with high values while two-dimension code is adopted for objects with lower values. The proper choice of AIDC technologies should be based on actual business requirements.

10 Considerations when establishing resolution systems and deploying distributed servers

10.1 Necessity of resolution systems for IoT applications

Nowadays with the high expansion speed of the integrated circuits industry, more and more smart devices have powerful computation and network connection capabilities, but with low prices which allows a great number of people to enjoy the achievements of IoT applications and to use these devices for intelligent services.

IoT intelligent services of the future are expected to provide integration of various services and require more powerful resolution systems for support. Unlike traditional resolution systems, IoT resolution systems should be more intelligent, refined, object-oriented and comprise many more sub-resolution systems to process information of "things" in specific areas.

10.2 Basic principles for the development of IoT resolution systems

To accelerate the connection of "things" with the Internet, there are two issues that should be considered.

First, things that have been connected to the Internet such as computers, reconstruction of the existing resolution systems, such as transmission control protocol/Internet protocol (TCP/IP), domain name system (DNS), etc., should be completed. ORS development works should follow the principles detailed in [ITU-T X.672] and make the resolution architecture of existing computer communication systems more suitable for IoT; that is, establish a closer link with "the things" of IoT.

Second, in the case of new smart devices or new things without communication abilities that would be used with some AIDC technologies, technologies that support IoT resolution systems are diversified, including cloud platforms and open-APIs. IoT resolution systems should be deployed as distributed to connect many specialized platforms and systems that use OIDs to identify their objects, and should be compatible with the characteristics of objects and the management mechanisms of actual authorities. Also, IoT resolution systems should provide the proper services and security mechanisms to meet the requirements of IoT applications.

11 Considerations when establishing OID-based authorities and operational procedures

Many factors should be considered when establishing OID-based authorities and operational procedures. The following three steps are recommended:

Step 1: Decide whether to build OID-based hierarchical authorities: If all the objects are managed centrally, only one registration authority is needed. If some of the objects are managed by multiple levels of authorities, hierarchical registration authorities should be established.

Step 2: Decide what kinds of OID services the authorities should provide. Many kinds of services are related to OIDs, such as electronic authentication service, automatic identification service, system integration service, etc.

Step 3: Establish operational procedures. The operational procedures should include, but are not limited to: procedure of registration of an OID, procedure of dealing with arguments and procedure of maintenance of OID resolution systems.

It is suggested that registration authorities could provide OID services through various means, such as web portals, applications (Apps), etc.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019