

**SLOVENSKI STANDARD**  
**SIST EN IEC 62680-1-4:2019**

**01-februar-2019**

---

**Vmesniki univerzalnega serijskega vodila za prenos podatkov in napajanje - 1-4.  
del: Skupne komponente - Specifikacija za avtentikacijo USB tipa C™ (IEC 62680-1  
-4:2018)**

Universal Serial Bus interfaces for data and power - Part 1-4: Common Components -  
USB Type-C(tm) Authentication Specification (IEC 62680-1-4:2018)

Schnittstellen des Universellen Seriellen Busses für Daten und Energie - Teil 1-4:  
Gemeinsame Bauteile - Festlegung für USB-Typ-CTM-Authentifizierung (IEC 62680-1-  
4:2018)

**SIST EN IEC 62680-1-4:2019**  
Interfaces de bus série universel (USB) pour les données et l'alimentation - Partie 1-4 :  
Composants communs - Spécification d'authentification USB Type-C(tm) (IEC 62680-1-  
4:2018)

**Ta slovenski standard je istoveten z: EN IEC 62680-1-4:2018**

---

**ICS:**

35.200	Vmesniška in povezovalna oprema	Interface and interconnection equipment
--------	------------------------------------	--

**SIST EN IEC 62680-1-4:2019** en,fr,de

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN IEC 62680-1-4:2019](#)

<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

**EUROPEAN STANDARD**  
**NORME EUROPÉENNE**  
**EUROPÄISCHE NORM**

**EN IEC 62680-1-4**

June 2018

ICS 35.200

English Version

**Universal Serial Bus interfaces for data and power - Part 1-4:  
 Common Components - USB Type-C(tm) Authentication  
 Specification  
 (IEC 62680-1-4:2018)**

Interfaces de bus série universel (USB) pour les données et  
 l'alimentation - Partie 1-4 : Composants communs -  
 Spécification d'authentification USB Type-C(tm)  
 (IEC 62680-1-4:2018)

Schnittstellen des Universellen Seriellen Busses für Daten  
 und Energie - Teil 1-4: Gemeinsame Bauteile - Festlegung  
 für USB-Typ-CTM-Authentifizierung  
 (IEC 62680-1-4:2018)

This European Standard was approved by CENELEC on 2018-05-15. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

**iTeh STANDARD PREVIEW**  
 Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.  
**(standards.iteh.ai)**

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization  
 Comité Européen de Normalisation Electrotechnique  
 Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

**EN IEC 62680-1-4:2018 (E)****European foreword**

The text of document 100/2981/CDV, future edition 1 of IEC 62680-1-4, prepared by technical area 14: "Interfaces and methods of measurement for personal computing equipment", of IEC/TC 100: "Audio, video and multimedia systems and equipment" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62680-1-4:2018.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2019-02-15
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2021-05-15

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

**Endorsement notice**

The text of the International Standard IEC 62680-1-4:2018 was approved by CENELEC as a European Standard without any modification.

**THE STANDARD PREVIEW  
(standards.iteh.ai)**

[SIST EN IEC 62680-1-4:2019](#)  
<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>



# INTERNATIONAL STANDARD



**Universal serial bus interfaces for data and power –  
Part 1-4: Common components – USB Type-C™ Authentication Specification  
(standards.iteh.ai)**

[SIST EN IEC 62680-1-4:2019](#)  
<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

ICS 35.200

ISBN 978-2-8322-5533-9

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

## UNIVERSAL SERIAL BUS INTERFACES FOR DATA AND POWER –

**Part 1-4: Common components – USB Type-C™ Authentication Specification**

## FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62680-1-4 has been prepared by technical area 14: Interfaces and methods of measurement for personal computing equipment, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

The text of this standard was prepared by the USB Implementers Forum (USB-IF). The structure and editorial rules used in this publication reflect the practice of the organization which submitted it.

The text of this International Standard is based on the following documents:

CDV	Report on voting
100/2981/CDV	100/3046/RVC

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

A list of all parts in the IEC 62680 series, published under the general title *Universal serial bus interfaces for data and power*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

## iTeh STANDARD PREVIEW

**IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.**

SIST EN IEC 62680-1-4:2019

<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

## INTRODUCTION

The IEC 62680 series is based on a series of specifications that were originally developed by the USB Implementers Forum (USB-IF). These specifications were submitted to the IEC under the auspices of a special agreement between the IEC and the USB-IF.

This standard is the USB-IF publication USB Type-C™ Authentication Specification Revision 1.0.

The USB Implementers Forum, Inc.(USB-IF) is a non-profit corporation founded by the group of companies that developed the Universal Serial Bus specification. The USB-IF was formed to provide a support organization and forum for the advancement and adoption of Universal Serial Bus technology. The Forum facilitates the development of high-quality compatible USB peripherals (devices), and promotes the benefits of USB and the quality of products that have passed compliance testing.

**ANY USB SPECIFICATIONS ARE PROVIDED TO YOU "AS IS, "WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE USB IMPLEMENTERS FORUM AND THE AUTHORS OF ANY USB SPECIFICATIONS DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY PROPRIETARY RIGHTS, RELATING TO USE OR IMPLEMENTATION OR INFORMATION IN THIS SPECIFICAITON.**

**THE PROVISION OF ANY USB SPECIFICATIONS TO YOU DOES NOT PROVIDE YOU WITH ANY LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS.**

Entering into USB Adopters Agreements may, however, allow a signing company to participate in a reciprocal, RAND-Z licensing arrangement for compliant products. For more information, please see:

SIST EN IEC 62680-1-4:2019

<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

[http://www.usb.org/developers/docs/devclass\\_docs#approved](http://www.usb.org/developers/docs/devclass_docs#approved)

IEC DOES NOT TAKE ANY POSITION AS TO WHETHER IT IS ADVISABLE FOR YOU TO ENTER INTO ANY USB ADOPTERS AGREEMENTS OR TO PARTICIPATE IN THE USB IMPLEMENTERS FORUM."

# Universal Serial Bus Type-C™ Authentication Specification

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[SIST EN IEC 62680-1-4:2019](https://standards.iteh.ai/1.0/)  
**Revision 1.0 with ECN and Errata through February 2, 2017**  
[1347eb612696/sist-en-iec-62680-1-4-2019](https://standards.iteh.ai/1.0/standards/jst/01c3b43e-003f-4086-8901-1347eb612696/sist-en-iec-62680-1-4-2019)

**Copyright © 2017, USB 3.0 Promoter Group  
All rights reserved.****INTELLECTUAL PROPERTY DISCLAIMER**

THIS SPECIFICATION IS PROVIDED TO YOU “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE AUTHORS OF THIS SPECIFICATION DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY PROPRIETARY RIGHTS, RELATING TO USE OR IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. THE PROVISION OF THIS SPECIFICATION TO YOU DOES NOT PROVIDE YOU WITH ANY LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS.

All product names are trademarks, registered trademarks, or service marks of their respective owners.

USB Type-C™ and USB-C™ are trademarks of USB Implementers Forum.

**iTeh STANDARD PREVIEW  
(standards.iteh.ai)**

[SIST EN IEC 62680-1-4:2019](#)  
<https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019>

## CONTENTS

Specification Work Group Chairs / Specification Editors .....	12
Specification Work Group Contributors .....	12
Revision History .....	14
1 Introduction .....	15
1.1 Scope .....	15
1.2 Overview .....	15
1.3 Related Documents .....	16
1.4 Terms and Abbreviations .....	18
1.5 Conventions .....	19
1.5.1 Precedence .....	19
1.5.2 Keywords .....	19
1.5.3 Numbering .....	20
1.5.4 Byte Ordering .....	20
2 Overview .....	20
2.1 Topology .....	20
2.2 Cryptographic Methods .....	21
2.2.1 Random Numbers .....	21
2.3 Security Overview .....	22
2.3.1 Periodic Re-Authentication .....	22
2.3.2 Secret Key Storage and Protection .....	22
2.3.3 Security Evaluation Criteria .....	22
2.4 Impact to Existing Ecosystem .....	22
2.4.1 Proxy Capabilities (PD traversing the Hub topology) .....	23
3 Authentication Architecture .....	23
3.1 Certificates .....	23
3.1.1 Format .....	23
3.1.2 Textual Format .....	23
3.1.3 Attributes and Extensions .....	23
3.2 Certificate Chains .....	25
3.2.1 Provisioning .....	25
3.3 Private Keys .....	26
4 Authentication Protocol .....	26
4.1 Digest Query .....	26
4.2 Certificate Chain Read .....	26
4.3 Authentication Challenge .....	27
4.4 Errors and Alerts .....	27
4.4.1 Invalid Request .....	27
4.4.2 Unsupported Protocol Version .....	27
4.4.3 Busy .....	27

4.4.4	Unspecified .....	27
5	Authentication Messages .....	27
5.1	Header .....	28
5.1.1	USB Type-C Authentication Protocol Version .....	28
5.1.2	Message Type .....	28
5.1.3	Param1 .....	28
5.1.4	Param2 .....	28
5.2	Authentication Requests .....	28
5.2.1	GET_DIGESTS .....	29
5.2.2	GET_CERTIFICATE .....	29
5.2.3	CHALLENGE .....	30
5.3	Authentication Responses .....	30
5.3.1	DIGESTS .....	31
5.3.2	CERTIFICATE .....	31
5.3.3	CHALLENGE_AUTH .....	32
5.3.4	ERROR .....	33
6	Authentication of PD Products .....	34
6.1	Transfers less than or equal to <i>MaxExtendedMsgLen</i> .....	34
6.2	Transfers greater than <i>MaxExtendedMsgLen</i> .....	35
6.3	Timing Requirements for PD Security Extended Messages .....	38
6.3.1	Authentication Initiator .....	38
6.3.2	Authentication Responder .....	39
6.4	Context Hash .....	40
7	Authentication of USB Products .....	40
7.1	Descriptors .....	40
7.1.1	Authentication Capability Descriptor .....	40
7.2	Mapping Authentication Messages to USB .....	41
7.2.1	Authentication IN .....	41
7.2.2	Authentication OUT .....	42
7.3	Authentication Protocol .....	42
7.3.1	Digest Query .....	42
7.3.2	Certificate Read .....	43
7.3.3	Authentication Challenge .....	43
7.3.4	Errors .....	44
7.4	Timing Requirements for USB .....	44
7.4.1	USB Host Timing Requirements .....	44
7.4.2	USB Device Timing Requirements .....	45
7.5	Context Hash .....	46
8	Protocol Constants .....	46
A	ACD .....	47
A.1.	ACD Formatting .....	47

A.1.1.	Version TLV .....	47
A.1.2.	XID TLV .....	48
A.1.3.	Power Source Capabilities TLV .....	48
A.1.4.	Power Source Certifications TLV .....	49
A.1.5.	Cable Capabilities TLV .....	50
A.1.6.	Security Description TLV .....	50
A.1.7.	Playpen TLV .....	54
A.1.8.	Vendor Extension TLV .....	55
A.1.9.	Extension TLV .....	55
A.2.	ACD for a PD Product .....	55
A.3.	ACD for a USB Product .....	56
B	Cryptographic Examples .....	57
B.1.	Example Authentication Sequence .....	57
B.2.	Example Certificate Chain Topology .....	57
B.2.1.	Certificate Chain .....	57
B.2.2.	Root Certificate .....	62
B.2.3.	Key Pairs .....	63
B.3.	Example Authentication Signature Verification .....	64
B.3.1.	CHALLENGE Request .....	64
B.3.2.	CHALLENGE_AUTH Response .....	64
C	Potential Attack Vectors .....	65
<b>SIST EN IEC 62680-1-4:2019</b>		
<a href="https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist_en_iec_62680-1-4-2019_TABLES">https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist_en_iec_62680-1-4-2019_TABLES</a>		
Table 1-1: Terms and Abbreviations .....		18
Table 2-1: Summary of Cryptographic Methods .....		21
Table 3-1: Certificate Chain Format .....		25
Table 5-1: Authentication Message Header .....		28
Table 5-2: USB Type-C Authentication Protocol Version .....		28
Table 5-3: Authentication Request Types .....		29
Table 5-4: GET_DIGESTS Request Header .....		29
Table 5-5: GET_CERTIFICATE Request Header .....		29
Table 5-6: GET_CERTIFICATE Request Payload .....		30
Table 5-7: CHALLENGE Request Header .....		30
Table 5-8: CHALLENGE Request Payload .....		30
Table 5-9: Authentication Response Types .....		30
Table 5-10: DIGESTS Response Header .....		31
Table 5-11: DIGESTS Response Payload .....		31
Table 5-12: CERTIFICATE Response Header .....		31
Table 5-13: CERTIFICATE Response Payload .....		32

Table 5-14: CHALLENGE_AUTH Response Header .....	32
Table 5-15: CHALLENGE_AUTH Response Payload .....	33
Table 5-16: Message Contents for ECDSA Digital Signature .....	33
Table 5-17: ERROR Response Header .....	34
Table 5-18: ERROR Codes .....	34
Table 6-1: Timeout Values for a PD Authentication Initiator .....	38
Table 6-2: Timing Requirements for PD Authentication Responder .....	39
Table 7-1: Authentication Capability Descriptor .....	40
Table 7-2: Authentication Capability Descriptor Types .....	41
Table 7-3: Authentication Message <i>bRequest</i> Values .....	41
Table 7-4: Authentication IN Control Request Fields .....	41
Table 7-5: Authentication Message Header Mapping .....	41
Table 7-6: Authentication OUT Control Request Fields .....	42
Table 7-7: GET_DIGESTS Authentication IN Control Request Fields .....	42
Table 7-8: GET_CERTIFICATE Authentication OUT Control Request Fields .....	43
Table 7-9: CERTIFICATE Authentication IN Control Request Fields .....	43
Table 7-10: CHALLENGE Authentication OUT Control Request Fields .....	43
Table 7-11: CHALLENGE_AUTH Authentication IN Control Request Fields .....	44
Table 7-12: Authentication Initiator Timeout Values .....	44
Table 7-13: Authentication Responder Response/Times .....	45
Table 8-1: Protocol Constants .....	46
Table A-1: TLV General Format .....	47
Table A-2: TLV Types .....	47
Table A-3: Version TLV Fields .....	47
Table A-4: ACD Version Encoding .....	48
Table A-5: XID TLV Fields .....	48
Table A-6: Power Source Capabilities TLV Fields .....	48
Table A-7: Power Source Capabilities TLV Data .....	49
Table A-8: Power Source Certifications TLV Fields .....	49
Table A-9: Cable Capabilities TLV Fields .....	50
Table A-10: Cable Capabilities TLV Data .....	50
Table A-11: Security Description TLV Fields .....	50
Table A-12: Security Data .....	50
Table A-13: FIPS/ISO Level Identifiers .....	51
Table A-14: Vulnerability Assessment .....	51
Table A-15: EAL Encodings .....	52
Table A-16: Protection Profile Encoding .....	52

Table A-17: Development Security .....	53
Table A-18: Certification Maintenance .....	53
Table A-19: Testing Method Encoding .....	54
Table A-20: Vulnerability Assessment .....	54
Table A-21: Playpen TLV Fields .....	55
Table A-22: Vendor Extension TLV Fields .....	55
Table A-23: Vendor Extension TLV Data .....	55
Table A-24: Extension TLV Fields .....	55
Table A-25: PD Product ACD TLVs .....	56
Table A-26: USB Product ACD TLVs .....	56
Table B-1: Version TLV Fields .....	61
Table B-2: XID TLV Fields .....	61
Table B-3: Power Source Capabilities TLV Fields .....	61
Table B-4: Security Description TLV Fields .....	61
Table B-5: Playpen TLV Fields .....	62
Table B-6: Vendor Extension TLV Fields .....	62

**STANDARD PREVIEW****(standards.iteh.ai)****FIGURES**

Figure 2-1 Sample Topology .....	<a href="#">SIST EN IEC 62680-1-4:2019</a> <a href="https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019">https://standards.iteh.ai/catalog/standards/sist/91c3b43e-903f-4086-890b-1347eb612696/sist-en-iec-62680-1-4-2019</a>	21
Figure 6-1 Example Security Transfer Process for an Authentication Initiator .....	36	
Figure 6-2 Example Security Transfer Process for an Authentication Responder .....	37	
Figure 6-3 Example 612-Byte Certificate Chain Read .....	38	
Figure A-1: Bitmap of Version TLV Data .....	48	
Figure A-2: Bitmap of the Common Criteria Identifier .....	51	
Figure A-3: Bitmap of the Security Analysis Identifier .....	53	