



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Universal serial bus interfaces for data and power –
Part 1-4: Common components – USB Type-C™ Authentication Specification**

**Interfaces de bus universel en série pour les données et l'alimentation
électrique –
Partie 1-4: Composants communs – Spécification relative à l'authentification
USB Type-C™**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 35.200

ISBN 978-2-8322-6494-2

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

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.

This bilingual version (2019-01) corresponds to the English version, published in 2018-04.

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.

The French version of this standard has not been voted upon.

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.

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.

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 SPECIFICATION.

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:

<http://www.usb.org/developers/docs/>

http://www.usb.org/developers/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

Revision 1.0 with ECN and Errata through February 2, 2017

**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.

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 |

TABLES

| | | |
|-------------|--|----|
| 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 |

FIGURES

| | |
|--|----|
| Figure 2-1 Sample Topology | 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 |

Specification Work Group Chairs / Specification Editors

| | | |
|---------------------------|----------|-------------------|
| Renesas Electronics Corp. | Co-Chair | Bob Dunstan |
| Intel Corporation | Co-Chair | Abdul Ismail |
| | Editor | Stephanie Wallick |

Specification Work Group Contributors

| | | | |
|---------------------------|--------------------------|--------------------|---------------------|
| Advanced Micro Devices | Jason Hawken | Joseph Scanlon | |
| Apple | Colin Whitby-Strevens | Robert Walsh | Reese Schreiber |
| | David Conroy | David Sekowski | |
| Atmel Corporation | Kerry Maletsky | Stephen Clark | Michel Guellec |
| | Ronald Ih | | |
| Cypress Semiconductor | Subu Sankaran | Jagadeesan Raj | Anup Nayak |
| | Jan-Willem van der Waert | | |
| Dell Inc. | Sean O'Neal | Mohammed Hijazi | Frank Molsberry |
| | Dan Hamlin | Rick Martinez | |
| DisplayLink (UK) Ltd. | Richard Petrie | Pete Burgers | Dan Ellis |
| Fresco Logic Inc. | Bob McVay | Tom Burton | Christopher Meyers |
| | Thomas Huang | | |
| Google Inc. | Adam Langley | William Richardson | Adam Rodriguez |
| | David Schneider | Mark Hayter | Ken Wu |
| | Will Drewry | Jerry Parson | Sanjay Krishnan |
| HP Inc. | Alan Berkema | Jim Waldron | Daniel Hong |
| Infineon Technologies | Thomas Poeppelmann | Wolfgang Furtner | Harald Hewel |
| | Wieland Fischer | Sie Boo Chiang | |
| Intel Corporation | Brad Saunders | David Johnston | Chia-Hung Kuo |
| | Christine Krause | Rolf Kuhnis | Steve McGowan |
| | Andrew Reinders | Purushottam Goel | Karthy Vadivelu |
| Lattice Semiconductor | Hoon Choi | Thomas Watzka | |
| MCCI Corporation | Terry Moore | | |
| Microchip Technology Inc. | Richard Wahler | Mark Bohm | Atish Ghosh |
| | Robert Schoepflin | | |
| Microsoft Corporation | Niels Ferguson | Nathan Sherman | Martin Borge |
| | Kinshumann Kinshumann | Vivek Gupta | Toby Nixon |
| | Kai Inha | Robbie Harris | Andrea Keating |
| | Fred Bhesania | Jayson Kastens | Rahul Ramadas |
| NXP Semiconductors | Vijendra Kuroodi | Joe Salvador | Alicia da Conceição |
| | Krishnan TN | | |
| Renesas Electronics Corp. | Philip Leung | Hideyuki Tanaka | Yuji Asano |
| | Kentaro Omata | Yoshiyuki Tomoda | Kiichi Muto |

| | | | |
|-------------------------------|------------------------|---------------------|-------------------|
| ROHM Co., Ltd. | Masahiko Nagata | Chizuru Matsunaga | Toshifumi Yamaoka |
| | Ruben Balbuena | Kris Bahar | Nobutaka Itakura |
| | Takashi Sato | | |
| Samsung Electronics Co., Ltd. | Tong Kim | Jagoun Koo | Soondo Kim |
| STMicroelectronics | Enrico Gregoratto | Guido Bertoni | Sylvie Wuidart |
| | Yannick Teglia | Anis Ben-Abdallah | Massimo Panzica |
| | Andrew Marsh | Joris Delclef | Nathalie Ballot |
| | Joel Huloux | Bernard Kasser | Dragos Davidescu |
| | Christophe Lorin | | |
| Synopsys, Inc. | Eric Huang | Morten Christiansen | Gervais Fong |
| | Venkataraman Krishnan | Nivin George | Aaron Yang |
| | Subramaniam Aravindhan | Bala Babu | Satya Patnala |
| | Kevin Heilman | John Youn | Zongyao Wen |
| Texas Instruments | Charles Campbell | Deric Waters | Scott Jackson |
| Total Phase | Chris Yokum | | |
| VIA Technologies | Terrance Shih | Jay Tseng | Fong-Jim Wang |
| | Benjamin Pan | | |

Revision History

| Revision | Date | Description |
|----------------------|------------------|--|
| 1.0 | March 25, 2016 | Initial Release |
| 1.0 + ECN and Errata | February 2, 2017 | Includes ECN and errata through February 2, 2017 |

1 Introduction

This specification provides a means for authenticating Products with regard to identification and configuration. Authentication is performed via USB Power Delivery message communications and/or via USB data bus control transactions.

USB Type-C™ Authentication allows an organization to set and enforce a Policy with regard to acceptable Products. This will permit useful security assurances in real world situations. For example:

- A vendor, concerned about product damage resulting from substandard charging devices, can set a Policy requiring that only certified PD Products be used for charging.
- A user, concerned about charging his phone at a public terminal, can set a Policy in his phone requiring that the phone only charge from certified PD Products.
- An organization, concerned about unidentifiable storage devices gaining access to corporate PC assets, can set a Policy in its PCs requiring that only USB storage devices that have been verified and signed by corporate IT are used.

1.1 Scope

This specification defines the architecture and methodology for unilateral Product Authentication. It is intended to be fully compatible with and extend existing PD and USB infrastructure. Information is provided to allow for Policy enforcement, but individual Policy decisions are not specified.

The Authentication of USB Type-C products that support Alternate Modes is allowed. However, the methods to do so are outside the scope of this specification.

1.2 Overview

This specification provides primitives for unilateral Authentication. The security model defined by this specification permits assurances that a Product is:

- Of a particular type from a particular manufacturer with particular characteristics
- Owned and controlled by a particular organization

Local Policy will determine which features need to be present in an attached Product before accessing or providing a resource (e.g. power, storage, etc.).

Product vendors can add security features beyond those listed in this specification, but the definition and implementation of those features is up to the vendor. Added features cannot alter the base specifications defined herein.

1.3 Related Documents

- **USB2.0** – Universal Serial Bus Specification, Revision 2.0, (including errata and ECNs through August 11, 2014) (referred to in this document as the USB 2.0 Specification) (available at: <http://www.usb.org/developers/docs>.)
- **USB3.1** – Universal Serial Bus 3.1 Specification, Revision 1.0, (including errata and ECNs through August 11, 2014) (referred to in this document as the USB 3.1 Specification) (available at: <http://www.usb.org/developers/docs>.)
- **USBPD** – Universal Serial Bus Power Delivery Specification, Revision 3, Version 1.0a, March 25, 2016 (referred to in this document as the USB PD Specification) (available at: <http://www.usb.org/developers/docs>.)
- **USBTYPEC** – Universal Serial Bus Type-C Cable and Connector Specification, Revision 1.2, March 25, 2016 (referred to in this document as the USB Type-C Specification)(available at: <http://www.usb.org/developers/docs>.)
- **USBTYPEC BRIDGE** Universal Serial Bus Type-C Bridge Specification, Revision 1.0, March 25, 2016, (available at <http://www.usb.org/developers/docs>.)
- **ASN.1** - ISO-822-1-4;
 - ITU-T X.680 (available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.680-201508-!!!PDF-E&type=items);
 - ITU-T X.681 (available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.681-201508-!!!PDF-E&type=items);
 - ITU-T X.682 (Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.682-201508-!!!PDF-E&type=items);
 - ITU-T X.683 (Available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.683-201508-!!!PDF-E&type=items.)
- **DER** - ISO-8825-1; ITU-T X.690 (available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.690-201508-!!!PDF-E&type=items.)
- **X509v3** - ISO-9594-8; ITU-T X.509 (available at: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-201210-!!!PDF-E&type=items.)
- **Common Criteria**:
 - Common Criteria for Information Technology Security Evaluation, Parts 1-3, Version 3.1, Revision 4, September 2010 (available at: <https://www.commoncriteriaportal.org/cc/#supporting>)
 - ISO/IEC 15408 Evaluation criteria for IT security Parts 1-3
- **ECDSA**:
 - ANSI X9.62; NIST-FIPS-186-4, Section 6 (available at: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.)
 - ISO/IEC 14888-3 Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms (Clause 6.6)
- **NIST P256, secp256r1**:
 - Certicom-SEC-2 (available at: <http://www.secg.org/sec2-v2.pdf>); NIST-Recommended-EC (available at: <http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>.)

- ISO/IEC 15946 Cryptographic techniques based on elliptic curves (NIST P-256 is included as example)
 - *Notes: ISO/IEC 15946 series treat elliptic curves differently from FIPS 186-4. ISO/IEC 15946-5 is about elliptic curve generation. That is, based on the method in part 5, each application and implementation can generate its own curves to use. In other words, no ISO/IEC recommended curves. P-256 is considered an example in ISO/IEC 15946. Note that Elliptic Curve signatures and key establishment schemes have been moved to ISO/IEC 14888 and ISO/IEC 11770 respectively together with other discrete log based mechanisms. Test vectors (examples) using P-256 are included for each parts for those mechanisms.*
- **SHA256:**
 - NIST-FIPS-180-4 (available at:
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.)
 - ISO/IEC 10118-3 Hash-functions – Part 3: Dedicated hash-functions (Clause 10)
- **OID** - ITU-T X.402 (available at: <https://www.itu.int/rec/T-REC-X.402-199906-I/en.>)
- **SP800-90A:**
 - NIST-SP-800-90A (available at:
<http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf>.)
 - *Note: NIST-SP-800-90A was withdrawn June 2015 and replaced by NIST-SP-800-90A Revision 1*
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>
- **SP800-90B** – NIST-SP-800-90B (available at:
http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf.)¹

¹ Note that this document is still in DRAFT phase.

² Unless specified otherwise, all standards specified, including those from ISO, ITU, and NIST, refer to the version or edition which is more recent, as of 1 January 2016.

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

INTERFACES DE BUS UNIVERSEL EN SÉRIE POUR LES DONNÉES ET L'ALIMENTATION ÉLECTRIQUE –

Partie 1-4: Composants communs – Spécification relative à l'authentification USB Type-C™

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC - entre autres activités - publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62680-1-4 a été établie par le Domaine technique 14: Interfaces et méthodes de mesure pour les équipements d'ordinateur personnel, du comité d'études 100 de l'IEC: Systèmes et équipements audio, vidéo et services de données.

Le texte de cette norme a été élaboré par l'USB Implementers Forum (USB-IF). Les règles structurelles et éditoriales utilisées dans la présente publication reflètent les pratiques en vigueur au sein de l'organisme responsable de sa soumission.

La présente version bilingue (2019-01) correspond à la version anglaise monolingue publiée en 2018-04.

Le texte anglais de cette norme est issu des documents 100/2981/CDV et 100/3046/RVC.

Le rapport de vote 100/3046/RVC donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Une liste de toutes les parties de la série IEC 62680, publiées sous le titre général *Interfaces de bus universel en série pour les données et l'alimentation électrique*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La série IEC 62680 est issue d'une série de spécifications initialement établies par l'USB Implementers Forum (USB-IF). Ces spécifications ont été soumises à l'IEC dans le cadre d'un accord particulier conclu entre l'IEC et l'USB-IF.

La présente norme est la spécification relative à l'authentification USB Type-C™, révision 1.0, publiée par l'USB-IF.

L'USB Implementers Forum, Inc. (USB-IF) est un organisme à but non lucratif fondé par le groupe de sociétés qui a développé la spécification du bus universel en série. L'USB-IF a été créé dans le but de proposer un organisme et un forum à même de favoriser la progression et l'adoption de la technologie USB. Le forum facilite le développement de périphériques (dispositifs) USB compatibles et de haute qualité et promeut les avantages de la technologie USB et la qualité des produits qui ont été validés par des essais de conformité.

L'ENSEMBLE DES SPÉCIFICATIONS USB CI-APRÈS VOUS SONT FOURNIES "EN L'ÉTAT", SANS GARANTIE D'AUCUNE SORTE, EN CE COMPRIS TOUTE GARANTIE DE QUALITÉ MARCHANDE, DE NON-VIOLATION OU D'ADAPTATION À UN USAGE PARTICULIER. L'USB IMPLEMENTERS FORUM ET LES AUTEURS DE L'ENSEMBLE DES SPÉCIFICATIONS USB CI-APRÈS DÉCLINENT TOUTE RESPONSABILITÉ, Y COMPRIS TOUTE RESPONSABILITÉ RELATIVE À LA VIOLATION DE DROITS DE PROPRIÉTÉ, EN CE QUI CONCERNE L'UTILISATION OU LA MISE EN ŒUVRE DES INFORMATIONS CONTENUES DANS LA PRÉSENTE SPÉCIFICATION.

LA MISE À DISPOSITION D'UNE SPÉCIFICATION USB, QUELLE QU'ELLE SOIT, N'IMPLIQUE L'OCTROI D'AUCUNE LICENCE, EXPRESSE OU IMPLICITE, PAR PERCLUSION OU AUTRE, SUR AUCUN DROIT DE PROPRIÉTÉ INTELLECTUELLE.

La conclusion des accords des adoptants de l'USB peut toutefois permettre à une société signataire de participer à un accord de licence réciproque RAND-Z pour les produits conformes. Pour plus d'informations, se rendre sur:

<http://www.usb.org/developers/docs/>

http://www.usb.org/developers/devclass_docs#approved

L'IEC NE PREND PAS POSITION SUR LA QUESTION DE SAVOIR S'IL VAUT LA PEINE QUE VOUS CONCLUIEZ UN QUELCONQUE ACCORD USB ADOPTERS AGREEMENT OU QUE VOUS PARTICIPIEZ À L'USB IMPLEMENTERS FORUM.

Bus universel en série Spécification relative à l'authentification USB Type-C™

Révision 1.0 avec ECN et errata au 2 février 2017

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

DÉNI DE RESPONSABILITÉ SUR LA PROPRIÉTÉ INTELLECTUELLE

LA PRÉSENTE SPÉCIFICATION VOUS EST FOURNIE "EN L'ÉTAT", SANS GARANTIE D'AUCUNE SORTE, EN CE COMPRIS TOUTE GARANTIE DE QUALITÉ MARCHANDE, DE NON-VIOLATION OU D'ADAPTATION À UN USAGE PARTICULIER. LES AUTEURS DE LA PRÉSENTE SPÉCIFICATION DÉCLINENT TOUTE RESPONSABILITÉ, Y COMPRIS TOUTE RESPONSABILITÉ RELATIVE À LA VIOLATION DE DROITS DE PROPRIÉTÉ, EN CE QUI CONCERNE L'UTILISATION OU LA MISE EN ŒUVRE DES INFORMATIONS CONTENUES DANS LA PRÉSENTE SPÉCIFICATION. LA DISPOSITION DE LA PRÉSENTE SPÉCIFICATION N'IMPLIQUE L'OCTROI D'AUCUNE LICENCE, EXPRESSE OU IMPLICITE, PAR PERCLUSION OU AUTRE, SUR AUCUN DROIT DE PROPRIÉTÉ INTELLECTUELLE.

Tous les noms de produits sont des marques, des marques déposées ou des marques de service de leurs propriétaires respectifs.

USB Type-C™ et USB-C™ sont des marques déposées de l'USB Implementers Forum.

SOMMAIRE

| | |
|--|----|
| Présidence du groupe de travail/Editeurs de la spécification | 76 |
| Contributeurs du groupe de travail de la spécification | 76 |
| Historique des révisions | 78 |
| 1 Introduction..... | 79 |
| 1.1 Domaine d'application | 79 |
| 1.2 Vue d'ensemble..... | 79 |
| 1.3 Documents connexes | 80 |
| 1.4 Termes et acronymes..... | 82 |
| 1.5 Conventions | 83 |
| 1.5.1 Priorité..... | 83 |
| 1.5.2 Mots-clés | 83 |
| 1.5.3 Numérotation | 84 |
| 1.5.4 Ordonnancement des octets..... | 84 |
| 2 Vue d'ensemble | 84 |
| 2.1 Topologie | 84 |
| 2.2 Méthodes cryptographiques..... | 85 |
| 2.2.1 Nombres aléatoires | 86 |
| 2.3 Présentation de la sécurité..... | 86 |
| 2.3.1 Authentification périodique..... | 86 |
| 2.3.2 Stockage et protection des clés secrètes | 86 |
| 2.3.3 Critères d'évaluation de sécurité | 87 |
| 2.4 Impact sur l'écosystème existant..... | 87 |
| 2.4.1 Capacités de proxy (PD traversant la topologie du hub) | 87 |
| 3 Architecture d'authentification | 87 |
| 3.1 Certificats..... | 87 |
| 3.1.1 Format | 87 |
| 3.1.2 Format texte..... | 87 |
| 3.1.3 Attributs et extensions..... | 88 |
| 3.2 Chaînes de certificats..... | 90 |
| 3.2.1 Approvisionnement | 90 |
| 3.3 Clés privées | 90 |
| 4 Protocole d'authentification | 91 |
| 4.1 Demande de condensé..... | 91 |
| 4.2 Lecture d'une chaîne de certificats | 91 |
| 4.3 Essai d'authentification..... | 92 |
| 4.4 Erreurs et alertes | 92 |
| 4.4.1 Requête invalide | 92 |
| 4.4.2 Version de protocole non prise en charge | 92 |
| 4.4.3 Occupé | 92 |

| | | |
|--------|--|-----|
| 4.4.4 | Non spécifié | 92 |
| 5 | Messages d'authentification | 92 |
| 5.1 | En-tête | 93 |
| 5.1.1 | Version de protocole d'authentification USB Type-C..... | 93 |
| 5.1.2 | Type de messages | 93 |
| 5.1.3 | Param1 | 93 |
| 5.1.4 | Param2 | 93 |
| 5.2 | Requêtes d'authentification | 93 |
| 5.2.1 | GET_DIGESTS | 94 |
| 5.2.2 | GET_CERTIFICATE..... | 94 |
| 5.2.3 | CHALLENGE | 95 |
| 5.3 | Réponses d'authentification..... | 95 |
| 5.3.1 | DIGESTS | 96 |
| 5.3.2 | CERTIFICATE..... | 97 |
| 5.3.3 | CHALLENGE_AUTH | 97 |
| 5.3.4 | ERROR..... | 99 |
| 6 | Authentification des produits PD | 99 |
| 6.1 | Transferts inférieurs ou égaux à <i>MaxExtendedMsgLen</i> | 99 |
| 6.2 | Transferts supérieurs à <i>MaxExtendedMsgLen</i> | 100 |
| 6.3 | Exigences temporelles pour messages PD de sécurité étendue | 103 |
| 6.3.1 | Initiateur d'authentification | 103 |
| 6.3.2 | Répondeur d'authentification..... | 104 |
| 6.4 | Context Hash | 105 |
| 7 | Authentification des produits USB | 105 |
| 7.1 | Descripteurs | 105 |
| 7.1.1 | Descripteur de capacités d'authentification | 106 |
| 7.2 | Mise en correspondance des messages d'authentification sur USB | 106 |
| 7.2.1 | Authentification IN..... | 107 |
| 7.2.2 | Authentification OUT | 108 |
| 7.3 | Protocole d'authentification | 108 |
| 7.3.1 | Demande de condensé | 108 |
| 7.3.2 | Lecture d'un certificat..... | 108 |
| 7.3.3 | Essai d'authentification | 109 |
| 7.3.4 | Erreurs..... | 110 |
| 7.4 | Exigences temporelles applicables à l'USB | 110 |
| 7.4.1 | Exigences temporelles applicables à l'hôte USB | 110 |
| 7.4.2 | Exigences temporelles applicables au dispositif USB | 112 |
| 7.5 | Context Hash | 113 |
| 8 | Constantes de protocole | 113 |
| A.1. | Formatage ACD..... | 114 |
| A.1.1. | TLV Version | 114 |

| | | |
|--------|--|-----|
| A.1.2. | TLV XID | 115 |
| A.1.3. | TLV Power Source Capabilities | 115 |
| A.1.4. | TLV Power Source Certifications | 116 |
| A.1.5. | TLV Cable Capabilities..... | 117 |
| A.1.6. | TLV Security Description..... | 117 |
| A.1.7. | TLV Playpen | 122 |
| A.1.8. | TLV Vendor Extension | 122 |
| A.1.9. | TLV Extension..... | 122 |
| A.2. | ACD pour un produit PD | 122 |
| A.3. | ACD pour un produit USB..... | 123 |
| B.1. | Exemple de séquence d'authentification | 124 |
| B.2. | Exemple de topologie de chaîne de certificats | 125 |
| B.2.1. | Chaîne de certificats | 125 |
| B.2.2. | Certificat d'origine | 130 |
| B.2.3. | Paires de clés | 130 |
| B.3. | Exemple de vérification de la signature d'authentification | 132 |
| B.3.1. | Requête CHALLENGE | 132 |
| B.3.2. | Réponse CHALLENGE_AUTH..... | 132 |

TABLEAUX

| | | |
|---------------|--|----|
| Tableau 1-1: | Termes et acronymes | 82 |
| Tableau 2-1: | Résumé des méthodes cryptographiques..... | 86 |
| Tableau 3-1: | Format de chaîne de certificats | 90 |
| Tableau 5-1: | En-tête de message d'authentification | 93 |
| Tableau 5-2: | Version de protocole d'authentification USB Type-C | 93 |
| Tableau 5-3: | Types de requêtes d'authentification..... | 94 |
| Tableau 5-4: | En-tête de requête GET_DIGESTS | 94 |
| Tableau 5-5: | En-tête de requête GET_CERTIFICATE..... | 94 |
| Tableau 5-6: | Charge utile de requête GET_CERTIFICATE | 95 |
| Tableau 5-7: | En-tête de requête CHALLENGE | 95 |
| Tableau 5-8: | Charge utile de requête CHALLENGE..... | 95 |
| Tableau 5-9: | Types de réponses d'authentification | 96 |
| Tableau 5-10: | En-tête de réponse DIGESTS | 96 |
| Tableau 5-11: | Charge utile de réponse DIGESTS..... | 96 |
| Tableau 5-12: | En-tête de réponse CERTIFICATE..... | 97 |
| Tableau 5-13: | Charge utile de réponse CERTIFICATE | 97 |
| Tableau 5-14: | En-tête de réponse CHALLENGE_AUTH | 97 |
| Tableau 5-15: | Charge utile de réponse CHALLENGE_AUTH..... | 98 |
| Tableau 5-16: | Contenu du message pour la signature numérique ECDSA | 98 |

| | |
|---|-----|
| Tableau 5-17: En-tête de réponse ERROR | 99 |
| Tableau 5-18: Codes ERROR..... | 99 |
| Tableau 6-1: Valeurs du délai d'expiration pour initiateur d'authentification PD | 104 |
| Tableau 6-2: Exigences temporelles pour répondeur d'authentification PD | 105 |
| Tableau 7-1: Descripteur de capacités d'authentification | 106 |
| Tableau 7-2: Types de descripteurs de capacités d'authentification..... | 106 |
| Tableau 7-3: Valeurs du message d'authentification <i>bRequest</i> | 107 |
| Tableau 7-4: Champs d'une requête de contrôle d'authentification IN..... | 107 |
| Tableau 7-5: Mise en correspondance d'en-tête de message d'authentification | 107 |
| Tableau 7-6: Champs d'une requête de contrôle d'authentification OUT | 108 |
| Tableau 7-7: Champs d'une requête de contrôle d'authentification IN GET_DIGESTS..... | 108 |
| Tableau 7-8: Champs d'une requête de contrôle d'authentification OUT GET_CERTIFICATE | 109 |
| Tableau 7-9: Champs d'une requête de contrôle d'authentification IN CERTIFICATE | 109 |
| Tableau 7-10: Champs d'une requête de contrôle d'authentification OUT CHALLENGE..... | 109 |
| Tableau 7-11: Champs d'une requête de contrôle d'authentification IN CHALLENGE_AUTH..... | 110 |
| Tableau 7-12: Valeurs du délai d'expiration de l'initiateur d'authentification..... | 111 |
| Tableau 7-13: Délais de réponse du répondeur d'authentification | 112 |
| Tableau 8-1: Constantes de protocole | 113 |
| Tableau A-1: Format de TLV général..... | 114 |
| Tableau A-2: Types de TLV | 114 |
| Tableau A-3: Champs du TLV Version..... | 114 |
| Tableau A-4: Codage de l'ACD Version | 115 |
| Tableau A-5: Champs du TLV XID..... | 115 |
| Tableau A-6: Champs du TLV Power Source Capabilities | 115 |
| Tableau A-7: Données du TLV Power Source Capabilities..... | 116 |
| Tableau A-8: Champs du TLV Power Source Certifications | 116 |
| Tableau A-9: Champs du TLV Cable Capabilities | 117 |
| Tableau A-10: Données du TLV Cable Capabilities | 117 |
| Tableau A-11: Champ du TLV Security Description | 117 |
| Tableau A-12: Données de sécurité..... | 117 |
| Tableau A-13: Identificateurs de niveau FIPS/ISO | 118 |
| Tableau A-14: Estimation des vulnérabilités | 119 |
| Tableau A-15: Codage EAL | 119 |
| Tableau A-16: Codage de Protection Profile | 119 |
| Tableau A-17: Sécurité de développement | 120 |

| | |
|---|-----|
| Tableau A-18: Maintenance de la certification | 120 |
| Tableau A-19: Codage de la méthode d'essai..... | 121 |
| Tableau A-20: Estimation des vulnérabilités | 121 |
| Tableau A-21: Champs du TLV Playpen | 122 |
| Tableau A-22: Champs du TLV Vendor Extension | 122 |
| Tableau A-23: Données du TLV Vendor Extension | 122 |
| Tableau A-24: Champs du TLV Extension | 122 |
| Tableau A-25: TLV ACD de produit PD..... | 123 |
| Tableau A-26: TLV ACD de produit USB | 123 |
| Tableau B-1: Champs du TLV Version..... | 128 |
| Tableau B-2: Champs du TLV XID..... | 128 |
| Tableau B-3: Champs du TLV Power Source Capabilities..... | 129 |
| Tableau B-4: Champs du TLV Security Description | 129 |
| Tableau B-5: Champs du TLV Playpen | 129 |
| Tableau B-6: Champs du TLV Vendor Extension | 129 |

FIGURES

| | |
|--|-----|
| Figure 2-1 Exemple de topologie | 84 |
| Figure 6-1 Exemple de transfert de sécurité pour initiateur d'authentification | 101 |
| Figure 6-2 Exemple de transfert de sécurité pour répondeur d'authentification | 102 |
| Figure 6-3 Exemple de lecture d'une chaîne de certificats de 612 octets | 103 |
| Figure A-1: Bitmap du champ Data du TLV Version..... | 115 |
| Figure A-2: Bitmap de l'identificateur de critère commun | 118 |
| Figure A-3: Bitmap de l'identificateur d'analyse de sécurité | 121 |

Présidence du groupe de travail/Editeurs de la spécification

| | | |
|---------------------------|--------------|-------------------|
| Renesas Electronics Corp. | Co-président | Bob Dunstan |
| Intel Corporation | Co-président | Abdul Ismail |
| | Editeur | Stephanie Wallick |

Contributeurs du groupe de travail de la spécification

| | | | |
|---------------------------|--------------------------|--------------------|---------------------|
| Advanced Micro Devices | Jason Hawken | Joseph Scanlon | |
| Apple | Colin Whitby-Strevens | Robert Walsh | Reese Schreiber |
| | David Conroy | David Sekowski | |
| Atmel Corporation | Kerry Maletsky | Stephen Clark | Michel Guellec |
| | Ronald Ih | | |
| Cypress Semiconductor | Subu Sankaran | Jagadeesan Raj | Anup Nayak |
| | Jan-Willem van der Waert | | |
| Dell Inc. | Sean O'Neal | Mohammed Hijazi | Frank Molsberry |
| | Dan Hamlin | Rick Martinez | |
| DisplayLink (UK) Ltd. | Richard Petrie | Pete Burgers | Dan Ellis |
| Fresco Logic Inc. | Bob McVay | Tom Burton | Christopher Meyers |
| | Thomas Huang | | |
| Google Inc. | Adam Langley | William Richardson | Adam Rodriguez |
| | David Schneider | Mark Hayter | Ken Wu |
| | Will Drewry | Jerry Parson | Sanjay Krishnan |
| HP Inc. | Alan Berkema | Jim Waldron | Daniel Hong |
| Infineon Technologies | Thomas Poeppelmann | Wolfgang Furtner | Harald Hewel |
| | Wieland Fischer | Sie Boo Chiang | |
| Intel Corporation | Brad Saunders | David Johnston | Chia-Hung Kuo |
| | Christine Krause | Rolf Kuhn | Steve McGowan |
| | Andrew Reinders | Purushottam Goel | Karthy Vadivelu |
| Lattice Semiconductor | Hoon Choi | Thomas Watzka | |
| MCCI Corporation | Terry Moore | | |
| Microchip Technology Inc. | Richard Wahler | Mark Bohm | Atish Ghosh |
| | Robert Schoepflin | | |
| Microsoft Corporation | Niels Ferguson | Nathan Sherman | Martin Borge |
| | Kinshumann | Vivek Gupta | Toby Nixon |
| | Kai Inha | Robbie Harris | Andrea Keating |
| | Fred Bhesania | Jayson Kastens | Rahul Ramadas |
| NXP Semiconductors | Vijendra Kuroodi | Joe Salvador | Alicia da Conceição |
| | Krishnan TN | | |
| Renesas Electronics Corp. | Philip Leung | Hideyuki Tanaka | Yuji Asano |
| | Kentaro Omata | Yoshiyuki Tomoda | Kiichi Muto |

| | | | |
|-------------------------------|------------------------|---------------------|-------------------|
| ROHM Co., Ltd. | Masahiko Nagata | Chizuru Matsunaga | Toshifumi Yamaoka |
| | Ruben Balbuena | Kris Bahar | Nobutaka Itakura |
| | Takashi Sato | | |
| Samsung Electronics Co., Ltd. | Tong Kim | Jagoun Koo | Soondo Kim |
| STMicroelectronics | Enrico Gregoratto | Guido Bertoni | Sylvie Wuidart |
| | Yannick Teglia | Anis Ben-Abdallah | Massimo Panzica |
| | Andrew Marsh | Joris Delclef | Nathalie Ballot |
| | Joel Huloux | Bernard Kasser | Dragos Davidescu |
| | Christophe Lorin | | |
| Synopsys, Inc. | Eric Huang | Morten Christiansen | Gervais Fong |
| | Venkataraman Krishnan | Nivin George | Aaron Yang |
| | Subramaniam Aravindhan | Bala Babu | Satya Patnala |
| | Kevin Heilman | John Youn | Zongyao Wen |
| Texas Instruments | Charles Campbell | Deric Waters | Scott Jackson |
| Total Phase | Chris Yokum | | |
| VIA Technologies | Terrance Shih | Jay Tseng | Fong-Jim Wang |
| | Benjamin Pan | | |

Historique des révisions

| Révision | Date | Description |
|------------------------|--------------------------|--|
| 1.0 | vendredi 25 mars 2016 | Publication initiale |
| 1.0 + ECN et errata | jeudi 2 février 2017 | Inclut l'ECN et les errata au 2 février 2017 |

1 Introduction

La présente spécification fournit un moyen d'authentifier les produits au regard de l'identification et de la configuration. L'authentification est réalisée par communication de messages USB Power Delivery et/ou par transactions de contrôle du bus de données USB.

L'authentification USB Type-C™ permet à une entreprise de définir et d'appliquer une Politique concernant les produits acceptables. Cela constitue un gage de sécurité pratique dans des situations concrètes. Par exemple:

- un fournisseur préoccupé par les dommages matériels induits par des dispositifs de chargement insuffisants peut définir une Politique exigeant que seuls les produits certifiés PD soient utilisés à des fins de chargement;
- un utilisateur préoccupé par le chargement de son téléphone sur un terminal public peut définir une Politique sur son téléphone exigeant un chargement uniquement à partir de produits certifiés PD;
- une entreprise préoccupée par l'accès des dispositifs de stockage non identifiables aux ressources PC professionnelles peut définir une Politique sur ses ordinateurs exigeant l'utilisation exclusive de dispositifs de stockage USB ayant été vérifiés et validés par son service informatique.

1.1 Domaine d'application

La présente spécification définit l'architecture et la méthodologie d'une authentification produit unilatérale. Elle est destinée à être intégralement compatible avec les infrastructures PD et USB existantes et à les développer. Certaines informations sont fournies en vue d'assurer l'application des Politiques; néanmoins, les décisions individuelles à ce sujet ne sont pas spécifiées.

L'authentification des produits USB Type-C prenant en charge les modes alternatifs est admise. Toutefois, les méthodes afférentes ne relèvent pas du domaine d'application de la présente spécification.

1.2 Vue d'ensemble

La présente spécification fournit les fondamentaux de l'authentification unilatérale. Le modèle de sécurité défini par la présente spécification offre l'assurance qu'un produit est:

- d'un type particulier, d'un fabricant particulier et de caractéristiques particulières;
- détenu et géré par une entreprise spécifique.

La Politique locale détermine quelles fonctionnalités ont besoin d'être présentes sur un produit connecté avant d'accéder à ou de fournir une ressource (alimentation, stockage, etc.).

Les fournisseurs de produits peuvent ajouter des fonctionnalités de sécurité au-delà de celles répertoriées dans la présente spécification; toutefois, la définition et la mise en œuvre de ces fonctionnalités incombent au fournisseur. Les fonctionnalités supplémentaires ne peuvent modifier les spécifications de base définies dans la présente spécification.

1.3 Documents connexes

- **USB2.0** — Universal Serial Bus Specification, révision 2.0 (avec errata et ECN au 11 août 2014) (disponible en anglais seulement) (désigné dans le présent document comme la spécification USB 2.0) (disponible à l'adresse: <http://www.usb.org/developers/docs.>)
- **USB3.1** — Universal Serial Bus 3.1 Specification, révision 1.0 (avec errata et ECN au 11 août 2014) (disponible en anglais seulement) (désigné dans le présent document comme la spécification USB 3.1) (disponible à l'adresse: <http://www.usb.org/developers/docs.>)
- **USBPD** — Universal Serial Bus Power Delivery Specification, révision 3, version 1.0a du 25 mars 2016 (disponible en anglais seulement) (désigné dans le présent document comme la spécification USB PD) (disponible à l'adresse: <http://www.usb.org/developers/docs.>)
- **USBTYPEC** — Universal Serial Bus Type-C Cable and Connector Specification, révision 1.2 du 25 mars 2016 (disponible en anglais seulement) (désigné dans le présent document comme la spécification USB Type-C) (disponible à l'adresse: <http://www.usb.org/developers/docs.>)
- **USBTYPEC BRIDGE** — Universal Serial Bus Type-C Bridge Specification, révision 1.0 du 25 mars 2016 (disponible en anglais seulement) (disponible à l'adresse: <http://www.usb.org/developers/docs.>)
- **ASN.1** — ISO-822-1-4:
 - ITU-T X.680 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.680-201508-!!!PDF-E&type=items)
 - ITU-T X.681 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.681-201508-!!!PDF-E&type=items)
 - ITU-T X.682 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.682-201508-!!!PDF-E&type=items)
 - ITU-T X.683 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.683-201508-!!!PDF-E&type=items.)
- **DER** — ISO-8825-1; ITU-T X.690 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.690-201508-!!!PDF-E&type=items.)
- **X509v3** — ISO-9594-8; ITU-T X.509 (disponible à l'adresse: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.509-201210-!!!PDF-E&type=items.)
- **Critères communs:**
 - Critères Communs pour l'évaluation de la sécurité des technologies de l'information, Parties 1-3, version 3.1, révision 4 de septembre 2010 (disponible à l'adresse: <https://www.commoncriteriaportal.org/cc/#supporting>)
 - ISO/IEC 15408, Critères d'évaluation pour la sécurité TI, Parties 1-3
- **ECDSA:**
 - ANSI X9.62; NIST-FIPS-186-4, section 6 (disponible à l'adresse: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.>)
 - ISO/IEC 14888-3, Signatures numériques avec appendice — Partie 3: Mécanismes basés sur un logarithme discret (Paragraphe 6.6)

- **NIST P256, secp256r1:**
 - Certicom-SEC-2 (disponible à l'adresse: <http://www.secg.org/sec2-v2.pdf>); NIST-Recommended-EC (disponible à l'adresse: <http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>.)
 - ISO/IEC 15946, Techniques cryptographiques fondées sur les courbes elliptiques (NIST P-256 incluse à titre d'exemple)
 - *Notes: La série ISO/IEC 15946 aborde les courbes elliptiques différemment de la FIPS 186-4. L'ISO/IEC 15946-5 traite de la génération de courbes elliptiques. Aussi, chaque application et chaque mise en œuvre peut générer ses propres courbes à utiliser à partir de la méthode de la Partie 5. En d'autres termes, il n'existe pas de courbes recommandées par l'ISO/IEC. La P-256 est abordée comme un exemple dans l'ISO/IEC 15946. Noter que les schémas d'établissement des signatures et clés des courbes elliptiques ont été respectivement déplacés vers l'ISO/IEC 14888 et l'ISO/IEC 11770 avec les autres mécanismes basés sur un logarithme discret. Des vecteurs d'essai (exemples) utilisant la P-256 sont inclus pour chaque partie de ces mécanismes.*
- **SHA256:**
 - NIST-FIPS-180-4 (disponible à l'adresse: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.)
 - ISO/IEC 10118-3, Hash-fonctions — Part 3: Dedicated hash-fonctions (Article 10) (disponible en anglais seulement)
- **OID** — ITU-T X.402 (disponible à l'adresse: <https://www.itu.int/rec/T-REC-X.402-199906-I/en>.)
- **SP800-90A:**
 - NIST-SP-800-90A (disponible à l'adresse: <http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf>.)
 - *Note: La NIST-SP-800-90A a été annulée en juin 2015 et remplacée par la NIST-SP-800-90A, révision 1*
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>
- **SP800-90B** — NIST-SP-800-90B (disponible à l'adresse: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf.)¹

¹ Le présent document est toujours en phase d'avant-projet.

² Sauf indication contraire, toutes les normes spécifiées, y compris celles de l'ISO, de l'UIT ou du NIST, renvoient à la version ou à l'édition la plus récente au 1er janvier 2016.