IEC 62680-1-4

Edition 1.0 2018-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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 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:

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

CONTENTS

TABLES

FIGURES

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	Karthi 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 Borve
	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

	Masahiko Nagata	Chizuru Matsunaga	Toshifumi Yamaoka
ROHM Co., Ltd.	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
	Venkataraghavan 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-I!!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-I!!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-I!!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-I!!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-I!!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-I!!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

SOMMAIRE

TABLEAUX

FIGURES

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 Kuhnis	Steve McGowan
	Andrew Reinders	Purushottam Goel	Karthi 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 Borve
	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

	Masahiko Nagata	Chizuru Matsunaga	Toshifumi Yamaoka
ROHM Co., Ltd.	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
	Venkataraghavan 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-I!!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-I!!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-I!!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-I!!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-I!!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-I!!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-functions — Part 3: Dedicated hash-functions (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*.