

DIN EN IEC 62680-1-4

ICS 29.220.01; 33.120.01; 35.200

**Schnittstellen des Universellen Seriellen Busses für Daten und Energie –
Teil 1-4: Gemeinsame Bauteile –
Festlegung für USB-Typ-C™-Authentifizierung
(IEC 62680-1-4:2018);
Deutsche Fassung EN IEC 62680-1-4:2018**

Universal Serial Bus interfaces for data and power –
Part 1-4: Common Components –
USB Type-C™ Authentication Specification
(IEC 62680-1-4:2018);
German version EN 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™
(IEC 62680-1-4:2018);
Version allemande EN IEC 62680-1-4:2018

Gesamtumfang 60 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2018-05-15 angenommene Europäische Norm als DIN-Norm ist 2019-12-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62680-1-4:2018-07.

Für dieses Dokument ist das nationale Arbeitsgremium K 742 „Audio-, Video- und Multimediasysteme, -geräte und -komponenten“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom IEC/TC 100 „Audio, video and multimedia systems and equipment“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieses Dokuments bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu diesem Dokument angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees das Dokument

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

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

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

Diese Europäische Norm wurde von CENELEC am 2018-05-15 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC Management Centre oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

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

Europäisches Vorwort

Der Text des Dokuments 100/2981/CDV, zukünftige 1. Ausgabe der IEC 62680-1-4, erarbeitet vom TA 14: „Interfaces and methods of measurement for personal computing equipment“ des IEC/TC 100: „Audio, video and multimedia systems and equipment“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN IEC 62680-1-4:2018 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2019-02-15
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2021-05-15

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62680-1-4:2018 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Europäisches Vorwort	2
Vorsitzende der Arbeitsgruppe / Autoren	9
Mitglieder der Arbeitsgruppe	9
Revision Historie.....	10
1 Einleitung.....	11
1.1 Anwendungsbereich.....	11
1.2 Überblick	11
1.3 Verwandte Dokumente.....	11
1.4 Begriffe und Abkürzungen.....	14
1.5 Konventionen	15
1.5.1 Prioritäten	15
1.5.2 Schlüsselwörter	15
1.5.3 Zahlen	16
1.5.4 Byte-Reihenfolge.....	16
2 Überblick	16
2.1 Topologie.....	16
2.2 Verschlüsselungsverfahren.....	17
2.2.1 Zufallszahlen	17
2.3 Überblick über die Sicherheit	18
2.3.1 Periodische Wiederholung der Authentifizierung.....	18
2.3.2 Speicherung und Schutz geheimer Schlüssel	18
2.3.3 Kriterien für die Sicherheitsbewertung	18
2.4 Auswirkungen auf das bestehende Ökosystem.....	18
2.4.1 Proxy-Fähigkeiten (die Hub-Topologie durchziehende PD)	19
3 Authentifizierungs-Architektur	19
3.1 Zertifikate.....	19
3.1.1 Format.....	19
3.1.2 Textformat	19
3.1.3 Attribute und Erweiterungen	19
3.2 Zertifikatsketten	21
3.2.1 Bereitstellung	21
3.3 Private Schlüssel.....	21
4 Authentifizierungs-Protokoll	22
4.1 Digest-Abfrage	22
4.2 Lesen einer Zertifikatskette	22
4.3 Authentifizierungs-Challenge	22
4.4 Fehler und Warnungen	23

	Seite
4.4.1 Invalid Request.....	23
4.4.2 Unsupported Protocol Version	23
4.4.3 Busy.....	23
4.4.4 Unspecified.....	23
5 Authentifizierungsnachrichten	23
5.1 Kopf	23
5.1.1 USB-Typ-C-Authentifizierungsprotokollversion.....	24
5.1.2 Nachrichtentyp.....	24
5.1.3 Param1	24
5.1.4 Param2	24
5.2 Authentifizierungsanforderungen	24
5.2.1 GET_DIGESTS	25
5.2.2 GET_CERTIFICATE	25
5.2.3 CHALLENGE.....	25
5.3 Authentifizierungsantworten	26
5.3.1 DIGESTS.....	26
5.3.2 CERTIFICATE	27
5.3.3 CHALLENGE_AUTH.....	27
5.3.4 ERROR.....	29
6 Authentifizierung von PD-Produkten	29
6.1 Übertragungen mit einer Länge kleiner oder gleich <i>MaxExtendedMsgLen</i>	29
6.2 Übertragungen mit einer Länge größer als <i>MaxExtendedMsgLen</i>	30
6.3 Zeitvorgaben für erweiterte PD-Sicherheitsnachrichten.....	32
6.3.1 Authentifizierungs-Initiator	32
6.3.2 Authentifizierungs-Beantworter	32
6.4 Context Hash.....	33
7 Authentifizierung von USB-Produkten.....	33
7.1 Deskriptoren	33
7.1.1 Deskriptor für Authentifizierungsfähigkeiten.....	33
7.2 Zuordnung von Authentifizierungsnachrichten zu USB.....	34
7.2.1 Authentication IN	34
7.2.2 Authentication OUT	35
7.3 Authentifizierungs-Protokoll.....	35
7.3.1 Digest-Abfrage.....	36
7.3.2 Lesen eines Zertifikats	36
7.3.3 Authentifizierungs-Challenge	36
7.3.4 Fehler	37
7.4 Zeitvorgaben für USB	37

	Seite
7.4.1 Zeitvorgaben für USB-Hosts	37
7.4.2 Zeitvorgaben für USB-Geräte	38
7.5 Context Hash.....	39
8 Protokollkonstanten.....	39
A ACD	40
A.1 ACD-Formatierung	40
A.1.1 Versions-TLV.....	40
A.1.2 XID-TLV.....	41
A.1.3 Stromquellenfähigkeiten-TLV	41
A.1.4 Stromquellenzertifizierungs-TLV	42
A.1.5 Kabelfähigkeiten-TLV	42
A.1.6 Sicherheitsbeschreibungs-TLV	43
A.1.6.1 FIPS-/ISO-Bezeichner.....	43
A.1.6.2 Common-Criteria-Bezeichner	44
A.1.6.3 Sicherheitsanalyse-Bezeichner.....	46
A.1.6.4 IC-Anbieter-Bezeichner.....	47
A.1.7 Playpen-TLV.....	47
A.1.8 Anbietererweiterungs-TLV	47
A.1.9 Erweiterungs-TLV	48
A.2 ACD eines PD-Produkts.....	48
A.3 ACD eines USB-Produkts	49
B Verschlüsselungsbeispiele.....	50
B.1 Beispiel für eine Authentifizierungssequenz	50
B.2 Beispiel einer Zertifikatsketten-Topologie	50
B.2.1 Zertifikatskette.....	50
B.2.1.1 Zwischenzertifikat.....	51
B.2.1.2 Leaf-Zertifikat	52
B.2.2 Root-Zertifikat.....	55
B.2.3 Schlüsselpaare.....	56
B.2.3.1 Root-Schlüsselpaar.....	56
B.2.3.2 Zwischenschlüsselpaar	56
B.2.3.3 Leaf-Schlüsselpaar	56
B.3 Beispiel für die Überprüfung einer Authentifizierungssignatur.....	57
B.3.1 CHALLENGE-Anforderung	57
B.3.2 CHALLENGE_AUTH-Antwort	57
C Potenzielle Angriffsvektoren.....	58

Bilder

Bild 2-1 – Beispieltopologie	17
------------------------------------	----

	Seite
Bild 6-1 – Beispiel für einen Sicherheitsübertragungsvorgang vonseiten eines Authentifizierungs-Initiators	30
Bild 6-2 – Beispiel für einen Sicherheitsübertragungsvorgang vonseiten eines Authentifizierungs-Beantworters	31
Bild 6-3 – Beispiel für das Lesen einer 612-Byte-Zertifikatskette	31
Bild A-1 – Bitmap der Versions-TLV-Daten	41
Bild A-2 – Bitmap der Common-Criteria-Bezeichner	44
Bild A-3 – Bitmap der Sicherheitsanalyse-Bezeichner	46

Tabellen

Tabelle 1-1 – Begriffe und Abkürzungen	14
Tabelle 2-1 – Zusammenfassung der Verschlüsselungsverfahren	17
Tabelle 3-1 – Format einer Zertifikatskette	21
Tabelle 5-1 – Authentifizierungsnachrichtenkopf	23
Tabelle 5-2 – USB-Typ-C-Authentifizierungsprotokollversion	24
Tabelle 5-3 – Arten von Authentifizierungsanforderungen	24
Tabelle 5-4 – Kopf einer GET_DIGESTS-Anforderung	25
Tabelle 5-5 – Kopf einer GET_CERTIFICATE-Anforderung	25
Tabelle 5-6 – Nutzdaten einer GET_CERTIFICATE-Anforderung	25
Tabelle 5-7 – Kopf einer CHALLENGE-Anforderung	26
Tabelle 5-8 – Nutzdaten einer CHALLENGE-Anforderung	26
Tabelle 5-9 – Arten von Authentifizierungsantworten	26
Tabelle 5-10 – Kopf einer DIGESTS-Antwort	27
Tabelle 5-11 – Nutzdatum einer DIGESTS-Antwort	27
Tabelle 5-12 – Kopf einer CERTIFICATE-Antwort	27
Tabelle 5-13 – Nutzdaten einer CERTIFICATE-Antwort	27
Tabelle 5-14 – Kopf einer CHALLENGE_AUTH-Antwort	28
Tabelle 5-15 – Nutzdaten einer CHALLENGE_AUTH-Antwort	28
Tabelle 5-16 – Nachrichteninhalt für digitale ECDSA-Signaturen	28
Tabelle 5-17 – Kopf einer ERROR-Antwort	29
Tabelle 5-18 – ERROR-Codes	29
Tabelle 6-1 – Timeout-Werte für einen PD-Authentifizierungs-Initiator	32
Tabelle 6-2 – Zeitvorgaben für PD-Authentifizierungs-Beantworter	32
Tabelle 7-1 – Deskriptor für Authentifizierungsfähigkeiten	34
Tabelle 7-2 – Deskriptortypen für Authentifizierungsfähigkeiten	34
Tabelle 7-3 – <i>bRequest</i> -Werte in Authentifizierungsnachrichten	34
Tabelle 7-4 – Felder einer Authentication-IN-Steuerungsanforderung	35
Tabelle 7-5 – Zuordnung des Authentifizierungsnachrichtenkopfes	35
Tabelle 7-6 – Felder einer Authentication-OUT-Steuerungsanforderung	35

	Seite
Tabelle 7-7 – Felder einer GET_DIGESTS-Authentication-IN-Steuerungsanforderung	36
Tabelle 7-8 – Felder einer GET_CERTIFICATE-Authentication-OUT-Steuerungsanforderung	36
Tabelle 7-9 – Felder einer CERTIFICATE-Authentication-IN-Steuerungsanforderung	36
Tabelle 7-10 – Felder einer CHALLENGE-Authentication-OUT-Steuerungsanforderung	36
Tabelle 7-11 – Felder einer CHALLENGE_AUTH-Authentication-IN-Steuerungsanforderung	37
Tabelle 7-12 – Timeout-Werte für Authentifizierungs-Initiatoren	37
Tabelle 7-13 – Antwortzeiten eines Authentifizierungs-Beantworters	38
Tabelle 8-1 – Protokollkonstanten	39
Tabelle A-1 – Allgemeines TLV-Format	40
Tabelle A-2 – TLV-Typen	40
Tabelle A-3 – Felder des Versions-TLV	40
Tabelle A-4 – Codierung der ACD-Version	41
Tabelle A-5 – Felder des XID-TLV	41
Tabelle A-6 – Felder des Stromquellenfähigkeiten-TLV	41
Tabelle A-7 – Daten des Stromquellenfähigkeiten-TLV	42
Tabelle A-8 – Felder des Stromquellenzertifizierungs-TLV	42
Tabelle A-9 – Felder des Kabelfähigkeiten-TLV	42
Tabelle A-10 – Daten des Kabelfähigkeiten-TLV	43
Tabelle A-11 – Felder des Sicherheitsbeschreibungs-TLV	43
Tabelle A-12 – Sicherheitsdaten	43
Tabelle A-13 – Bezeichner der FIPS-/ISO-Stufe	44
Tabelle A-14 – Gefährdungsbewertung	44
Tabelle A-15 – EAL-Codierung	45
Tabelle A-16 – Schutzprofil-Codierungen	45
Tabelle A-17 – Sicherheit bei der Entwicklung	46
Tabelle A-18 – Zertifizierung Maintenance	46
Tabelle A-19 – Codierung des Prüfverfahrens	47
Tabelle A-20 – Gefährdungsbewertung	47
Tabelle A-21 – Felder des Playpen-TLV	47
Tabelle A-22 – Felder des Anbietererweiterungs-TLV	48
Tabelle A-23 – Daten des Anbietererweiterungs-TLV	48
Tabelle A-24 – Felder des Erweiterungs-TLV	48
Tabelle A-25 – ACD-TLV für PD-Produkte	48
Tabelle A-26 – ACD-TLV für USB-Produkte	49
Tabelle B-1 – Felder des Versions-TLV	53
Tabelle B-2 – Felder des XID-TLV	53
Tabelle B-3 – Felder des Stromquellenfähigkeiten-TLV	54
Tabelle B-4 – Felder des Sicherheitsbeschreibungs-TLV	54

	Seite
Tabelle B-5 – Felder des Playpen-TLV.....	54
Tabelle B-6 – Felder des Anbietererweiterungs-TLV	55

Vorsitzende der Arbeitsgruppe / Autoren

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

Mitglieder der Arbeitsgruppe

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 Kuhnisch	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 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. STMicroelectronics	Tong Kim	Jagoun Koo	Soondo Kim
	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
Synopsys, Inc.	Christophe Lorin		
	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 Historie

Revision	Datum	Beschreibung
1.0	2016-03-25	1. Ausgabe
1.0 + ECN and Errata	2017-02-02	Includes ECN and errata through 2017-02-02

1 Einleitung

Diese Spezifikation beschreibt eine Möglichkeit zur Authentifizierung von Produkten hinsichtlich Identifikation und Konfiguration. Die Authentifizierung findet mittels USB-Power-Delivery-Nachrichtenkommunikation und/oder mittels USB-Datenbus-Kontrolltransaktionen statt.

Die USB-Typ-C™-Authentifizierung ermöglicht es Organisationen, Richtlinien für zulässige Produkte festzulegen und umzusetzen. Dadurch wird die Sicherheit in realen Situationen zweckdienlich sichergestellt. Zum Beispiel:

- Ein Anbieter, der seine Geräte vor Produktschäden durch minderwertige Ladegeräte schützen möchte, kann eine Richtlinie festlegen, nach der das Laden nur mit zertifizierten PD-Produkten möglich ist.
- Ein Anwender, der Bedenken bezüglich des Ladens seines Telefons an öffentlichen Ladestationen hat, kann eine Richtlinie festlegen, nach der das Laden des Telefons nur mit zertifizierten PD-Produkten möglich ist.
- Eine Organisation, die verhindern möchte, dass nicht identifizierbare Speichergeräte auf die PC-Infrastruktur des Unternehmens zugreifen können, können in ihren PCs eine Richtlinie festlegen, nach der nur verifizierte und von der internen IT-Abteilung signierte USB-Speichergeräte verwendet werden können.

1.1 Anwendungsbereich

Diese Spezifikation legt die Architektur und Methodologie für die einseitige Produktauthentifizierung fest. Bei der Erarbeitung wurde eine uneingeschränkte Kompatibilität mit und Erweiterung der bestehenden PD- und USB-Infrastruktur angestrebt. Die Spezifikation enthält Informationen zur Ermöglichung der Anwendung von Richtlinien; einzelne Richtlinienentscheidungen werden jedoch nicht festgelegt.

Die Authentifizierung von USB-Typ-C-Produkten, die Alternativmodi unterstützen, ist erlaubt. Die entsprechenden Verfahren liegen jedoch außerhalb des Anwendungsbereichs dieser Spezifikation.

1.2 Überblick

Diese Spezifikation enthält Primitive für die einseitige Authentifizierung. Das in dieser Spezifikation festgelegte Sicherheitsmodell ermöglicht die Sicherstellung, dass ein Produkt:

- von einer bestimmten Art von einem bestimmten Hersteller ist und bestimmte Eigenschaften aufweist;
- sich im Besitz und unter der Kontrolle einer bestimmten Organisation befindet.

Die lokale Richtlinie legt fest, welche Eigenschaften ein verbundenes Produkt aufweisen muss, bevor es auf eine Ressource zugreifen oder eine Ressource zur Verfügung stellen kann (z. B. Energie, Speicher usw.).

Produktanbieter können Sicherheitsmerkmale hinzufügen, die über die in dieser Spezifikation aufgeführten Merkmale hinausgehen. Die Festlegung und Implementierung dieser Merkmale liegt jedoch in der Verantwortung des Anbieters. Zusätzliche Merkmale dürfen die in diesem Dokument beschriebenen grundlegenden Festlegungen nicht verändern.

1.3 Verwandte Dokumente

- **USB2.0** – Universal-Serial-Bus-Spezifikation, Revision 2.0 (einschließlich Errata und ECNs vom 2014-08-11) (im vorliegenden Dokument als USB-2.0-Spezifikation bezeichnet) (verfügbar unter: <http://www.usb.org/developers/docs>).
- **USB3.1** – Universal-Serial-Bus-3.1-Spezifikation, Revision 1.0 (einschließlich Errata und ECNs vom 2014-08-11) (im vorliegenden Dokument als USB-3.1-Spezifikation bezeichnet) (verfügbar unter: <http://www.usb.org/developers/docs>).
- **USBPD** – Universal-Serial-Bus-Power-Delivery-Spezifikation, Revision 3, Version 1.0a, 2016-03-25 (in diesem Dokument als USB-PD-Spezifikation bezeichnet) (verfügbar unter: <http://www.usb.org/developers/docs>).

- **USBTYPEC** – Spezifikation für Universal-Serial-Bus-Typ-C-Kabel und -Steckverbinder, Revision 1.2, 2016-03-25 (in diesem Dokument als USB-Typ-C-Spezifikation bezeichnet) (verfügbar unter: <http://www.usb.org/developers/docs>).
- **USBTYPEC BRIDGE** Spezifikation für Universal-Serial-Bus-Typ-C-Brücken, Revision 1.0, 2016-03-25 (verfügbar unter: <http://www.usb.org/developers/docs>).
- **ASN.1** – ISO-822-1-4:
 - ITU-T X.680 (verfügbar unter: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.680-201508-!!!PDF-E&type=items);
 - ITU-T X.681 (verfügbar unter: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.681-201508-!!!PDF-E&type=items);
 - ITU-T X.682 (verfügbar unter: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.682-201508-!!!PDF-E&type=items);
 - ITU-T X.683 (verfügbar unter: 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 (verfügbar unter: 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 (verfügbar unter: 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, Teile 1–3, Version 3.1, Revision 4, September 2010 (verfügbar unter: <https://www.commoncriteriaportal.org/cc/#supporting>);
 - ISO/IEC 15408 Evaluation criteria for IT security, Teile 1–3
- **ECDSA**:
 - ANSI X9.62; NIST-FIPS-186-4, Abschnitt 6 (verfügbar unter: <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 (Unterabschnitt 6.6)
- **NIST P256, secp256r1**:
 - Certicom-SEC-2 (verfügbar unter: <http://www.secg.org/sec2-v2.pdf>);
 - NIST-Recommended-EC (verfügbar unter: <http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>).
 - ISO/IEC 15946 Cryptographic techniques based on elliptic curves (enthält NIST P-256 als Beispiel)
 - **ANMERKUNGEN:** Die Reihe ISO/IEC 15946 behandelt elliptische Kurven anders als FIPS 186-4. In ISO/IEC 15946-5 geht es um die Generierung elliptischer Kurven. Das bedeutet, dass alle Anwendungen und Implementierungen ihre eigenen Kurven auf Grundlage des in Teil 5 beschriebenen Verfahrens generieren können. Mit anderen Worten handelt es sich dabei nicht um von ISO/IEC empfohlene Kurven. P-256 wird in ISO/IEC 15946 als Beispiel betrachtet. Signaturen auf Basis von elliptischen Kurven und Schlüsselerstellungsverfahren wurden gemeinsam mit anderen auf diskreten Logarithmen basierenden Mechanismen in ISO/IEC 14888 bzw. ISO/IEC 11770 verschoben. Alle Teile dieser Mechanismen enthalten auf P-256 basierende Prüfvektoren (Beispiele).
- **SHA256**:
 - NIST-FIPS-180-4 (verfügbar unter: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>);
 - ISO/IEC 10118-3 Hash-functions – Part 3: Dedicated hash-functions (Abschnitt 10).

- **OID** – ITU-T X.402 (verfügbar unter: <https://www.itu.int/rec/T-REC-X.402-199906-I/en>).
- **SP800-90A:**
 - NIST-SP-800-90A (verfügbar unter: <http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf>).
 - *ANMERKUNG: NIST-SP-800-90A wurde im Juni 2015 zurückgezogen und durch NIST-SP-800-90A Revision 1 ersetzt.*
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf>
- **SP800-90B** – NIST-SP-800-90B (verfügbar unter: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf).¹

Sofern nichts anderes angegeben ist, beziehen sich alle angegebenen Normen, einschließlich der ISO-, ITU- und NIST-Normen, auf die aktuellste Version oder Ausgabe mit Stand vom 1. Januar 2016.

¹ Dieses Dokument befindet sich noch in der ENTWURFS-Phase.

1.4 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe und Abkürzungen.

Tabelle 1-1 – Begriffe und Abkürzungen

Begriff/Abkürzung	Definition
ACD (en: additional certificate data for a product)	zusätzliche Zertifikatsdaten für ein Produkt
Authentifizierung	Verfahren zur Bestätigung, ob eine Instanz das ist, was sie vorgibt zu sein
Authentifizierungs-Initiator	Produkt, das die Authentifizierung einleitet
Authentifizierungs-Beantworter	Produkt, bei dem ein Authentifizierungs-Initiator versucht, sich zu authentifizieren
Zertifikat (Cert, en: certificate)	digitale Form der Identifikation, die Informationen über die Instanz enthält und die Eigentümerschaft eines bestimmten öffentlichen Schlüssels zertifiziert
Zertifizierungsinstanz (CA) (en: certificate authority)	Instanz, die Zertifikate ausstellt
Zertifikatskette	Reihe von zwei oder mehr Zertifikaten, in der jedes Zertifikat vom vorhergehenden Zertifikat in der Kette signiert ist
Instanz	Produkt oder mit diesem Produkt verbundene(r) Organisation, Anbieter oder Hersteller
Vertrauenswürdigkeitsstufe (EAL) (en: evaluation assurance level)	numerische Bewertung, die die Tiefe und Genauigkeit einer Sicherheitsbewertung beschreibt
Zwischenzertifikat	Zertifikat, das weder ein Root- noch ein Leaf-Zertifikat ist
Leaf-Zertifikat	letztes Zertifikat in einer Zertifikatskette
LSB (en: least significant byte)	niedrigstwertiges Byte
MSB (en: most significant byte)	höchstwertiges Byte
Nonce	Zahl, die in einem bestimmten Schlüsselkontext nur einmal verwendet wird. Kann als N-Once (einmalig verwendete Zahl) interpretiert werden.
OID (en: object identifier)	Objektbezeichner. Weitere Informationen hierzu siehe OID.
PDen: USB Power Delivery	USB-Stromversorgung
PD-Produkt	Quelle, Verbraucher oder Kabel nach USBPD
PDUSB-Produkt	USB-Host oder USB-Gerät, das sowohl PD- als auch USB-Kommunikation unterstützt
Richtlinie	Eine Richtlinie definiert das Verhalten von Produkten. Sie legt die für das Produkt angegebenen Fähigkeiten, seine Authentifizierungsanforderungen und die Ressourcenverfügbarkeit hinsichtlich nicht authentifizierter Produkte fest.
Produkt	bezieht sich auf ein PD-Produkt, USB-Produkt und/oder PDUSB-Produkt
Pseudozufallszahlengenerator (PRNG) (en: pseudorandom number generator)	Deterministischer Algorithmus zur Erzeugung einer Zahl oder Zahlenfolge, die rechnerisch von echt zufälliger Erzeugung nicht zu unterscheiden ist. Weitere Informationen hierzu siehe SP800-90A.
Root-Zertifikat	Erstes Zertifikat in einer Zertifikatskette. Dieses Zertifikat signiert sich selbst.
TLV (en: type, length, value)	Typ, Länge, Wert
USB-Gerät	Gerät (einschließlich Hub) wie in USB2.0 und USB3.1 definiert
USB-Host	Host wie in USB2.0 und USB3.1 definiert
USB-Hub	Hub wie in USB2.0 und USB3.1 definiert
USB-Produkt	USB-Host oder USB-Gerät

1.5 Konventionen

1.5.1 Prioritäten

Besteht ein Widerspruch zwischen Text, Bildern und Tabellen, haben Tabellen Vorrang vor Bildern und Bilder Vorrang vor dem Text.

1.5.2 Schlüsselwörter

Anhand der folgenden Schlüsselwörter wird zwischen verschiedenen Anforderungs- und Optionsstufen unterschieden.

1.5.2.1 Bedingt normativ

Bedingt normativ ist ein Schlüsselwort, das eine Eigenschaft bezeichnet, die dann verpflichtend wird, wenn eine andere verwandte Eigenschaft implementiert wurde. Wurden die abhängigen Eigenschaften implementiert, sind Konstrukteure dazu verpflichtet, alle derartigen Anforderungen zu implementieren, um die Interoperabilität mit anderen konformen Produkten sicherzustellen.

1.5.2.2 Abgelehnt

Abgelehnt ist ein Schlüsselwort, das eine Eigenschaft bezeichnet, die in früheren Ausgaben der Spezifikation unterstützt wurde, nun jedoch nicht mehr unterstützt wird.

1.5.2.3 Informativ

Informativ ist ein Schlüsselwort, das Informationen zu dieser Spezifikation beschreibt, die der Erörterung und Erklärung von Anforderungen und Merkmalen dienen, ohne sie vorzuschreiben.

1.5.2.4 Darf

Darf ist ein Schlüsselwort, das eine Wahlmöglichkeit angibt, ohne einen Vorrang zu implizieren.

1.5.2.5 N/A

N/A ist ein Schlüsselwort, das angibt, dass ein Feld oder Wert nicht zutrifft, daher keinen festgelegten Wert hat und nicht vom Empfänger überprüft oder verwendet werden darf.

1.5.2.6 Normativ

Normativ ist ein Schlüsselwort, das Merkmale beschreibt, die von dieser Spezifikation vorgeschrieben werden.

1.5.2.7 Optional/Optional normativ

Optional und **Optional normativ** sind gleichbedeutende Schlüsselwörter, die Eigenschaften beschreiben, die nicht von dieser Spezifikation vorgeschrieben werden. Wird ein **optionales** Merkmal implementiert, muss es jedoch auf die in dieser Spezifikation festgelegte Weise implementiert werden.

1.5.2.8 Reserviert

Reserviert ist ein Schlüsselwort, das reservierte Bits, Bytes, Wörter, Felder und Codewerte bezeichnet, die für eine zukünftige Normierung vorgemerkt werden. Ihre Verwendung und Interpretation darf in zukünftigen Erweiterungen dieser Norm festgelegt werden und, soweit nicht anders angegeben, darf sie nicht in der Anbieterimplementierung verwendet oder verändert werden. Ein **reserviertes** Bit, Byte, Wort oder Feld muss vom Absender auf null gesetzt und vom Empfänger ignoriert werden. **Reservierte** Feldwerte dürfen nicht vom Absender gesendet werden. Sollten sie empfangen werden, muss der Empfänger sie ignorieren.

1.5.2.9 Muss/Normativ

Muss und **Normativ** sind Schlüsselwörter, die eine verbindliche Anforderung angeben. Konstrukteure sind dazu verpflichtet, alle derartigen Anforderungen zu implementieren, um die Interoperabilität mit anderen konformen Produkten sicherzustellen.

1.5.2.10 Sollte

Sollte ist ein Schlüsselwort, das eine Wahlmöglichkeit mit einer bevorzugten Alternative angibt. Gleichwertig mit der Formulierung „es wird empfohlen, dass“.

1.5.3 Zahlen

Zahlen, auf die unmittelbar der Kleinbuchstabe „b“ folgt (z. B. 01b), sind Binärwerte. Zahlen, auf die unmittelbar der Kleinbuchstabe „h“ folgt (z. B. 3Ah), sind Hexadezimalwerte. Zahlen, auf die unmittelbar weder „b“ noch „h“ folgt, sind Dezimalwerte.

1.5.4 Byte-Reihenfolge

Soweit nicht anders angegeben, werden alle Mehrfach-Byte-Werte in dieser Spezifikation in Little-Endian-Reihenfolge, d. h. vom LSB zum MSB, interpretiert und über den Bus übertragen.

Die Reihenfolge, in der einzelne Bits über einen Bus übertragen werden, ist für PD-Produkte in **USBPD** und für USB-Produkte in **USB2.0** und **USB3.1** festgelegt.

2 Überblick

Dieser Abschnitt enthält keine normativen Anforderungen.

2.1 Topologie

In Bild 2-1 stellt eine Beispieltopologie von USB-Produkten und PD-Produkten dar, die USB-Typ-C-Authentifizierung unterstützen. Diese Darstellung erhebt keinen Anspruch auf Vollständigkeit oder auf die Einbeziehung aller möglichen Topologie-Konfigurationen.