

2019

Karty a bezpečnostní zařízení pro osobní identifikaci -
Bezkontaktní objekty s vazbou na blízko -
Část 4: Protokol přenosu

ČSN
ISO/IEC 14443-4

36 9760

Cards and security devices for personal identification - Contactless proximity objects -
Part 4: Transmission protocol

Cartes et dispositifs de sécurité pour l'identification personnelle - Objets sans contact de proximité -
Partie 4: Protocole de transmission

Tato norma je českou verzí mezinárodní normy ISO/IEC 14443-4:2018. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the international Standard ISO/IEC 14443-4:2018. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 7816-3 zavedena v ČSN ISO/IEC 7816-3 (36 9205) Identifikační karty - Karty s integrovanými obvody - Část 3: Karty s kontakty - Elektrické rozhraní a protokoly přenosu

ISO/IEC 7816-4:2013 zavedena v ČSN ISO/IEC 7816-4 (36 9205) Identifikační karty - Karty s integrovanými obvody - Část 4: Organizace, bezpečnost a příkazy pro výměnu

ISO/IEC 14443-2 dosud nezavedena

ISO/IEC 14443-3 zavedena v ČSN ISO/IEC 14443-3 (36 9760) Karty a bezpečnostní zařízení pro osobní identifikaci - Bezkontaktní objekty s vazbou na blízko - Část 3: Inicializace a antikolize

Související ČSN

ČSN ISO/IEC 7810 (36 9725) Identifikační karty - Fyzikální charakteristiky

ČSN ISO/IEC 10536 (soubor) (36 9741) Identifikační karty - Bezkontaktní karty s integrovanými obvody - Karty s těsnou vazbou

ČSN ISO/IEC 13239 (36 9737) Informační technologie - Telekomunikace a výměna informací mezi

systemy - Procedury řízení datového spoje vysoké úrovně (HDLC)

ČSN ISO/IEC 15693-1 (36 9762) Karty a bezpečnostní zařízení pro osobní identifikaci - Bezkontaktní objekty s vazbou na dálku - Část 1: Fyzikální charakteristiky

Vysvětlivky k textu převzaté normy

anglický termín/zkratka	obvyklé termíny/zkratka	použitý termín/zkratka
bit rate	<ul style="list-style-type: none">· (bitová) přenosová rychlost· bitová rychlost	(bitová) přenosová rychlost
bit rate activation	<ul style="list-style-type: none">· bitová rychlost aktivace· rychlost aktivace	bitová rychlost aktivace
enhanced block	<ul style="list-style-type: none">· rozšířený blok· zvětšený blok	rozšířený blok
PPS request	<ul style="list-style-type: none">· žádost o PPS· žádost o výběr protokolu a parametrů	žádost o PPS
PPS response	<ul style="list-style-type: none">· odezva na PPS· odezva na výběr protokolu a parametrů	odezva na PPS
S(WTX) request	<ul style="list-style-type: none">· žádost o S(WTX)· žádost o prodloužení doby čekání	žádost o S(WTX)
S(WTX) response	<ul style="list-style-type: none">· odezva na S(WTX)· odezva na žádost o prodloužení doby čekání	odezva na S(WTX)
SOF high time	<ul style="list-style-type: none">· doba vysoké úrovně SOF	doba vysoké úrovně SOF

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČO 61278386, Dr. Karel Jurák

Technická normalizační komise: TNK 42 Výměna dat

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.240.15

Obsah

Strana

Předmluva.....	6
Úvod.....	7
1..... Předmět normy.....	8
2..... Citované dokumenty.....	8
3..... Termíny a definice.....	8
4..... Značky, zkrácené termíny a způsob zápisu.....	9
4.1..... Značky a zkrácené termíny.....	9
4.2..... Způsob zápisu.....	11
5..... Aktivace protokolu PICC typu A.....	11
5.1..... Aktivační posloupnosti.....	11
5.2..... Žádost o odpověď na výběr.....	

5.3..... Odpověď na výběr.....	13
5.3.1... Struktura bajtů.....	14
5.3.2... Bajt délky.....	14
5.3.3... Bajt formátu.....	14
5.3.4... Bajt rozhraní TA(1).....	14
5.3.5... Bajt rozhraní TB(1).....	15
5.3.6... Bajt rozhraní TC(1).....	16
5.3.7... Historické bajty.....	16
5.4..... Žádost o výběr protokolu a parametrů.....	16
5.4.1... Startovací bajt.....	16
5.4.2... Parametr 0.....	17
5.4.3... Parametr 1.....	17
5.5..... Odezva na výběr protokolu a parametrů.....	17
5.6..... Doba čekání na aktivaci	

rámce.....	18
5.7..... Detekce chyby a zotavení po chybě.....	18
5.7.1... Používání RATS a ATS.....	18
5.7.2... Používání žádosti o PPS a odezvy na PPS.....	18
5.7.3... Používání CID v průběhu aktivace.....	19
6..... Aktivace protokolu pro PICC typu B.....	19
7..... Protokol poloduplexního přenosu po blocích.....	19
7.1..... Prvky a mechanismy.....	19

7.2..... Formát bloku.....	20
7.2.1... Pole délky.....	21
7.2.2... Pole prolog.....	21
7.2.3... Informační pole.....	23
7.2.4... Pole epilog.....	23
7.3..... Doba čekání na rámeček.....	24
7.4..... Prodloužení doby čekání na rámeček.....	24
7.5..... Indikace úrovně příkonu.....	25
7.6..... Činnost protokolu.....	25
7.6.1... Bloky S(PARAMETERS).....	25
7.6.2... Multiaktivace.....	26
7.6.3... Řetězení.....	27
7.6.4... Pravidla pro číslování bloku.....	27

7.6.5... Pravidla pro manipulaci s bloky.....	28
7.6.6... Kontrola přítomnosti PICC.....	29
7.6.7... Detekce chyby a zotavení po chybě.....	29
8..... Protokol deaktivace PICC typu A a typu B.....	29
8.1..... Doba čekání na deaktivací rámec.....	30
8.2..... Detekce chyby a zotavení po chybě.....	30
9..... Aktivace přenosových rychlostí a voleb druhu rámce ve stavu PROTOCOL.....	30
10..... Rámec s opravou chyby.....	32
10.1.... Obecně.....	32
10.2.... Formát rámce PCD typu A pro přenosové rychlosti až do $fc/16$ a vyšší než $fc/2$ a formát rámce PICC typu A pro všechny přenosové rychlosti.....	32
10.3.... Formát rámce PCD typu A pro přenosové rychlosti $fc/8$, $fc/4$ a $fc/2$ a PCD typu B a formát rámce PICC pro všechny přenosové rychlosti.....	32
10.4.... Rozšířený blok s opravou chyby.....	33
10.4.1 Obecně.....	33
10.4.2 Formát modifikovaného Hammingova subbloku.....	33
10.4.3 Hammingův kontrolní	

bajt.....	33
10.4.4 Generující matice <i>A</i> Hammingova kódu.....	33
10.4.5 Výpočet Hammingových kontrolních bitů.....	34
10.4.6 Kontrolní matice <i>H</i> Hammingova kódu.....	34
10.4.7 Oprava chyby.....	34
10.5.... Aktivace rámce s opravou chyby ve stavu PROTOCOL.....	35
Příloha A (informativní) Příklad multiaktivace.....	37
Příloha B (informativní) Scénáře protokolu.....	38
Příloha C (informativní) Přehled kódování bloků a rámců.....	47
Příloha D (úmyslně ponecháno prázdno).....	48
Příloha E (informativní) Kódování CRC_32.....	49
Příloha F (informativní) Rámec s opravou chyby.....	51
Příloha G (informativní) Volba druhu rámce.....	53
Bibliografie.....	54



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2018

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopii nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizací ISO v zemi žadatele.

ISO copyright office

CP 401 · CH. de Blandonnet 8

CH-1214 Vernier, Geneva,

Phone: + 41 22 749 01 11

Fax: + 41 22 749 09 47

Email: copyright@iso.org

Web: www.iso.org

Publikováno ve Švýcarsku

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdrženech ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL:

www.iso.org/iso/foreword.html.

Tento dokument vypracovala ISO/IEC JTC 1 *Informační technologie*, subkomise SC 17 *Karty a bezpečnostní zařízení pro osobní identifikaci*.

Toto čtvrté vydání zrušuje a nahrazuje třetí vydání (ISO/IEC 14443-4:2016), které bylo technicky zrevidováno.

Seznam všech částí souboru ISO/IEC 14443 lze nalézt na webových stránkách ISO.

Úvod

Soubor norem ISO/IEC 14443 popisuje parametry pro identifikaci karet nebo objektů pro mezinárodní výměnu.

Protokol, jak je definován v tomto dokumentu, umožňuje přenášet datové jednotky protokolu aplikace definované v ISO/IEC 7816-4. Tedy datové jednotky aplikačního protokolu a výběr aplikace mohou být použity podle ISO/IEC 7816-4.

Soubor norem ISO/IEC 14443 je určen, aby dovoval činnost karet pro vazbu na blízko v přítomnosti dalších bezkontaktních karet nebo objektů, které splňují soubory norem ISO/IEC 10536 a ISO/IEC 15693 a zařízení pro komunikaci v blízkém poli (NFC), které splňují ISO/IEC 18092 a ISO/IEC 21481.

1 Předmět normy

Tento dokument specifikuje poloduplexní přenosový protokol po blocích, který respektuje speciální potřeby bezkontaktního prostředí a definuje aktivační a deaktivaci posloupnosti protokolu.

Tento dokument musí být používán spolu s dalšími částmi ISO/IEC 14443 a je použitelný pro karty nebo objekty s vazbou na blízko typu A a typu B.

Konec náhledu - text dále pokračuje v placené verzi ČSN.