ČESKÁ TECHNICKÁ NORMA

ICS 03.220.20; 35.240.60

Květen 2019

Elektronický výběr mýtného – Stanovení aplikačního rozhraní pro vyhrazenou komunikaci krátkého dosahu (DSRC)

ČSN
EN ISO 14906

01 8382

idt ISO 14906:2018

Electronic fee collection – Application interface definition for dedicated short-range communication

Perception du télépéage – Définition de l,interface d,application relative aux communications dédiées a courte portée

Tato norma je českou verzí evropské normy EN ISO 14906:2018. Překlad byl zajištěn Českou agenturou pro stan-
dardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO 14906:2018. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO 14906 (01 8382) z února 2012.

Národní předmluva

Změny proti předchozí normě

Viz Předmluva na straně 8.

Informace o citovaných dokumentech

ISO 612 dosud nezavedena

ISO 1176 zavedena v ČSN ISO 1176 (30 0030) Silniční vozidla. Hmotnosti. Terminologie a kódy

ISO 3166-1 zavedena v ČSN EN ISO 3166-1 (97 1002) Kódy pro názvy zemí a jejich částí – Část 1: Kódy zemí

ISO 3779 dosud nezavedena

ISO 4217 dosud nezavedena

ISO/IEC 7812-1 zavedena v ČSN ISO/IEC 7812-1 (36 9732) Identifikační karty – Identifikace vydavatelů karet – Část 1: Systém číslování

ISO/IEC 8825-2 dosud nezavedena

ISO/IEC 9797-1:2011 zavedena v ČSN ISO/IEC 9797-1:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

ISO 14816:2005 zavedena v ČSN EN ISO 14816:2007 (01 8338) Dopravní telematika – Automatická identifikace vozidel a zařízení – Číslování a struktura dat

ISO 15628:2013 dosud nezavedena

ISO/IEC 18033-3:2010 dosud nezavedena

EN 12834:2003 zavedena v ČSN EN 12834:2004 (01 8202) Dopravní telematika (RTTT) – Vyhrazené spojení krátkého dosahu (DSRC) – Aplikační vrstva

Souvisící ČSN

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ČSN ISO 17573 (01 8383) Elektronický výběr poplatků (EFC) – Architektura systémů zpoplatňujících vozidla

ČSN P CEN ISO/TS 17574 (01 8384) Elektronický výběr poplatků – Směrnice pro systém bezpečnosti

ČSN EN ISO 12813 (01 8389) Elektronický výběr poplatků (EFC) – Komunikace pro kontrolu shody autonomních systémů

ČSN EN ISO 25110 (01 8387) Elektronický výběr poplatků – Definice rozhraní pro palubní účet používající platební kartu s integrovaným obvodem (ICC)

ČSN ISO/IEC 8824-1 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace základního způsobu zápisu

Souvisící předpisy

Směrnice Rady 1999/37/ES ze dne 29. dubna 1999 o registračních dokladech vozidel

Směrnice komise 2003/127/ES ze dne 23. prosince 2003, kterou se mění směrnice Rady 1999/37/ES o registračních dokladech vozidel

Směrnice evropského parlamentu a rady 2014/46/EU ze dne 3. dubna 2014, kterou se mění směrnice Rady 1999/37/ES o registračních dokladech vozidel

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Upozornění na národní poznámku

Do této normy byla k tabulce C.4 doplněna národní poznámka.

Vypracování normy

Zpracovatel: SILMOS s. r. o. – CTN, IČO 45276293, spolupráce: ČVUT v Praze, Mgr. Jakub Rajnoch

Technická normalizační komise: TNK 136 Dopravní telematika

Pracovník České agentury pro standardizaci: Ing. Jan Křivka

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.

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 14906

Prosinec 2018

ICS 35.240.60; 03.220.20

Nahrazuje EN ISO 14906:2011

Elektronický výběr mýtného – Stanovení aplikačního rozhraní pro vyhrazenou komunikaci krátkého dosahu (DSRC) (ISO 14906:2018)

Electronic fee collection – Application interface definition for dedicated short-range communication (ISO 14906:2018)

Perception du télépéage – Définition de l,interface d,application relative aux communications dédiées a courte portée (ISO 14906:2018)

Elektronische Gebührenerhebung – Anwendungsschnittstelle zur dezidierten Nahbereich-Kommunikation (ISO 14906:2018)

Tato evropská normy byla schválena CEN dne 2018-09-06.

Členové CEN jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy. Aktualizované seznamy a biblio-
grafické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru CEN-CENELEC nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung
Řídicí centrum CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO 14906:2018 E

Členy CEN jsou národní normalizační orgány Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Evropská předmluva

Tento dokument (EN ISO 14906:2018) vypracovala technická komise ISO/TC 204 *Inteligentní dopravní systémy* ve spolupráci s technickou komisí CEN/TC 278 *Inteligentní dopravní systémy,* jejíž sekretariát zajišťuje NEN.

Této evropské normě je nutno nejpozději do června 2019 dát status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do června 2019.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CEN nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument nahrazuje EN ISO 14906:2011.

Tento dokument byl vypracován na základě mandátu uděleného CEN Evropskou komisí a Evropským sdružením volného obchodu a podporuje splnění základních požadavků směrnice (směrnic) EU.

Podle vnitřních předpisů CEN/CENELEC jsou povinny zavést tuto evropskou normu národní normalizační orgány následujících zemí: Belgie, Bulharska, Bývalé jugoslávské republiky Makedonie, České Republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemí, Norska, Kypru, Polska, Portugalsko, Rakouska, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska, a Turecka.

Oznámení o schválení

Text ISO 14906:2018 byl schválen CEN jako EN ISO 14906:2018 bez jakýchkoliv modifikací.

Obsah

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

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

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou 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 obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená 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 technická komise ISO/TC 204 *Inteligentní dopravní systémy*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO 14906:2011), které bylo technicky revidováno. Druhé vydání zahrnuje opravu ISO 14906:2011/Cor1:2013 a změnu ISO 14906:2011/Amd1:2015.

Hlavní změny oproti původní verzi jsou následující:

– začlenění výpočtů bezpečnosti podle šifrovacího algoritmu AES, dle doporučení CEN/TR 16968 ohledně bezpečnostních mechanismů (revize kapitoly 7 a nově vložené přílohy F, G, H a I);

– aktualizace kapitoly citované dokumenty, termíny a definice, zkratky a bibliografie;

– konverze modulu v notaci ASN.1 na vložení elektronicky;

– revize přílohy C;

– odstranění přílohy D (informativní) Funkční požadavky.

Jakékoli připomínky nebo dotazy k tomuto dokumentu nechť jsou mířeny na národní normalizační úřad. Úplný seznam těchto národních normalizačních úřadů lze nalézt na
www.iso.org/members.html.

Úvod

Tento dokument stanoví aplikační rozhraní pro systémy elektronického výběru mýtného (EFC), které využívají DSRC (vyhrazenou komunikaci krátkého dosahu). Podporuje interoperabilitu mezi systémy EFC na úrovni aplikačního rozhraní EFC-DSRC. Tento dokument je určena pro aplikace zpoplatnění pomocí DSRC, ale konkrétní definice datových prvků EFC platí i pro jiné zpoplatnění, než přes rozhraní DSRC zpoplatnění a mohly by být použity pro jiné aplikace DSRC (například komunikaci pro kontrolu shody) a/nebo na jiná rozhraní (například aplikační rozhraní pro autonomní systémy).

Tento dokument poskytuje specifikace pro transakční model EFC, datové prvky EFC (uváděné jako atributy) a funkce, z nichž může být transakce EFC vytvořena. Transakční model EFC poskytuje mechanismus umožňující zvládnout různé verze transakcí EFC a jim přidružené smlouvy. Jak je stanoveno v tomto dokumentu, konkrétní EFC transakce obsahuje určitou sadu funkcí a EFC atributů. Nepředpokládá se, že každá část zařízení EFC, palubního zařízení (OBE) nebo zařízení na infrastruktuře (RSE), bude obsahovat kompletní sadu EFC atributů a funkcí.

Tento dokument poskytuje základ pro dohody mezi provozovateli, které jsou nutné pro dosažení interoperability. Na základě nástrojů stanovených v tomto dokumentu může být interoperabilita mezi provozovateli dosažena vzájemným uznáním svých EFC transakcí (včetně výměny bezpečnostních algoritmů a klíčů) a vzájemnou implementací těchto EFC transakcí do RSE ostatních provozovatelů, nebo stanovením nové transakce (a smlouvy), které budou společné pro obě strany. Každý provozovatel musí zvážit, jestli je implementace dodatečných EFC transakcí v možnostech jím provozovaného RSE.

Provozovatelé se v zájmu zajištění interoperability musí shodnout na:

– doplňkových funkcích, které jsou ve skutečnosti implementovány a používány;

– přístupových právech a vlastnictví aplikačních dat EFC umístěných v OBE;

– bezpečnostní politice (včetně kódovacích algoritmů a správě bezpečnostních klíčů, pokud je to vhodné);

– provozních záležitostech, jako například počtu možných uložených stvrzenek s ohledem na zabezpečení soukromí, počtu stvrzenek nezbytných pro provoz systému (například vstupní bloček (stvrzenka), nebo doklad o zaplacení);

– dohodách mezi provozovateli, jak regulovat vyřizování různých EFC transakcí.

V tomto vydání normy jsou uživatelé vystaveni řešení otázky zpětné kompatibility. Tento problém lze řešit těmito prostředky:

– modulem EfcModule ASN.1, obsahujícím číslo verze;

– Efc-ContextMark (včetně ContextVersion) označující verzi implementace, poskytující prostředky pro vzájemnou existenci různých verzí implementace pomocí vyhledávací tabulky a souvisejícího příslušného zpracování transakce. Software RSE tak může stanovit verzi OBE a jeho schopnost přijmout nové znaky této verze ISO 14906.

Příloha A uvádí normativní specifikaci použitých datových typů podle ASN.1 (akční parametry a atributy EFC).

Příloha B uvádí informativní příklad transakce založený na specifikaci CARDME obsahující výpis

transakce na bitové úrovni.

Příloha C uvádí informativní příklady typů EFC transakcí používajících různé funkce a atributy.

Příloha D uvádí informativní tabulku namapování LatinAlphabetNo2 & 5 na LatinAlphabetNo1, která slouží poskytovateli služeb k snazšímu použití LatinAlphabetNo1 pro kódování dat konkrétního OBE, která jsou psána ve formátu non-Latin1.

Příloha E uvádí informativní tabulku namapování atributů EFC dat o vozidle a evropských registračních certifikátů, pro usnadnění úkolu poskytovatele služeb při personalizaci konkrétního OBE obdržením dat o vozidle.

Příloha F uvádí výpočty bezpečnosti podle šifrovacího algoritmu DES. Tato příloha je založena na EN 15509:2014, příloha B.

Příloha G uvádí příklady výpočtů bezpečnosti pro DES. Tato příloha je založena na EN 15509:2014, příloha E.

Příloha H uvádí výpočty bezpečnosti pro šifrovací algoritmus AES. Tato příloha je založena na adaptaci
EN 15509:2014, přílohy B pro případ AES.

Příloha I uvádí příklady výpočtů bezpečnosti pro AES. Tato příloha je založena na adaptaci EN 15509:2014, přílohy E
pro případ AES.

Tuto definici aplikačního rozhraní lze také použít s jiným médiem DSRC, které nepoužívá aplikační vrstvu (vrstvu 7) podle ISO 15628/EN 12834. Jakékoliv médium DSRC, které poskytuje služby pro čtení a zápis dat k inicializaci komunikace a k provedení akcí, je vhodné k použití jako základ pro toto aplikační rozhraní. Adaptace jsou medium-specifické a nejsou touto normou řešeny. Podle podrobného popisu, v příloze B, transakce pro systémy centrálního účtu lze tento dokument použít také pro systémy palubního účtu, ve spojení s ISO 25110, která poskytuje příklady systémů založených na palubních účtech.

1 Předmět normy

Tento dokument stanoví aplikační rozhraní v kontextu systémů elektronického výběru mýtného (EFC), používající DSRC.

Aplikační rozhraní EFC je rozhraní mezi aplikačním procesem EFC a aplikační vrstvou DSRC, jak je znázorněno na obrázku 1. Působnost tohoto dokumentu zahrnuje specifikace:

– atributů EFC (tj. informací o aplikaci EFC), které lze použít pro jiné aplikace a/nebo rozhraní,

– postupů adresování atributů a (hardwarových) komponent EFC (například ICC a MMI),

– aplikačních funkcí EFC, tj. podrobnější popis akcí pomocí stanovení příslušných služeb, přidělení přidružených hodnot ActionType a obsahu a významu parametrů daných činností,

– transakčního modelu EFC stanovujícího společné prvky a kroky jakékoliv transakce EFC,

– chování rozhraní tak, aby byla zabezpečena interoperabilita na úrovni aplikačního rozhraní EFC-DSRC.

Obrázek 1 – Aplikační rozhraní EFC

Tato rozhraní specifikující norma dodržuje filosofii propojených otevřených systémů (OSI) (viz ISO/IEC 7498-1) a je nezávislá na konkrétní implementaci na obou stranách rozhraní.

Tento dokument poskytuje rámec (pro data a funkce) umožňující implementaci zabezpečených transakcí EFC. Konkrétní volba bezpečnostní politiky (včetně specifických šifrovacích algoritmů a správy bezpečnostních klíčů) zůstává plně v kompetenci poskytovatele EFC a je tudíž mimo předmět tohoto dokumentu.