

EXTRAKT z české technické normy

Extrakt nenahrazuje samotnou technickou normu, je pouze informativním materiálem o normě.

ICS 03.220.20, 35.240.60

Elektronický výběr poplatků (EFC) – Komunikace pro kontrolu shody autonomních systémů

ČSN P CEN
ISO/TS
12813

01 8389

44 stran

Úvod

Tato technická specifikace je určena pro OBE pracující v režimu satelitního mýtného. Stanovuje požadavky na komunikaci prostřednictvím vyhrazeného spojení krátkého dosahu (DSRC) mezi palubním zařízením (OBE) a zařízením na straně infrastruktury (RSE). Tato komunikace slouží pro zjištění shody mezi skutečným použitím pozemní komunikace (PK) ze strany OBE a platným režimem mýtného. OBE za tímto účelem zaznamenává údaje o použití PK v zóně systému výběru mýtného.

Tímto způsobem výběrčí mýtného kontrolují, zda jsou pozemní komunikace (PK) využívány v souladu s platným místním režimem mýtného. Jedním ze způsobů provedení této kontroly je sledování projíždějícího vozidla a interakce s jeho OBE.

V interoperabilním prostředí je zásadní, aby kontrolní komunikace byla standardizována tak, aby každý operátor kontrolního zařízení (výběrčí mýtného) mohl kontrolovat všechna projíždějící zařízení OBE. Z tohoto důvodu definuje tato technická specifikace atributy, kterými musí palubní zařízení (OBE) disponovat, aby byla jeho komunikace s kontrolním zařízením možná.

Předpokládá se, že primárním cílem operátora kontrolního zařízení je ověřovat, zda uživatel splnil požadavky na něho kladené, zvláště ověřit,

- zda je palubní zařízení osazeno na správném typu vozidla;
- zda jsou klasifikační data odeslaná palubním zařízením správná;
- zda je palubní zařízení v aktivním provozu, a to jak ve smyslu technickém, tak ve smyslu platnosti smlouvy.

Užití

Tato technická specifikace byla vytvořena za účelem stanovení „minimálních požadavků“ a to tak, že popisuje prvky, které jsou vyžadovány aktuálně provozovanými systémy a budou vyžadovány systémy plánovanými v blízké budoucnosti. Tato specifikace je vhodná pro **výrobce** telematických zařízení pro výběr poplatků tím, že stanovuje minimální požadavky na kontrolní komunikaci mezi OBE a RSE, tedy to co musí OBE splňovat aby mu bylo uděleno prohlášení o shodě. Zároveň bude používána **zkušebními orgány** jako základ pro stanovení interoperability zařízení a prohlášení o shodě.

1 Předmět normy

Norma stanovuje minimální požadavky na komunikaci OBE provozované v systému satelitního výběru mýtného s RSE prostřednictvím DSRC. Tato komunikace, vzhledem k tomu, že se používá pro zjištění shody mezi platným mýtným režimem a nastavením (akcemi) OBE, se nazývá kontrolní komunikace (CCC).

Kontrolní komunikace zahrnuje syntaxi a sémantiku dat, ale ne komunikační sekvenci. Definované atributy a funkce slouží ke kontrole shody pomocí komunikačních služeb DSRC poskytovaných aplikační vrstvou 7 DSRC, pomocí atributů a funkcí CCC, které jsou dostupné pro CCC aplikace na straně infrastruktury i palubní zařízení. Atributy a funkce jsou definovány na úrovni ADU (datové jednotky na aplikační vrstvě).

Všechny zde definované atributy jsou povinné pro veškerá zařízení OBE, která si nárokují shodu s touto technickou specifikací, a to i v případě, že zařízení OBE nedisponuje určitou funkcionalitou. Aby bylo dosaženo kompatibility se stávajícími systémy, kdykoliv je to možné, komunikace využívá atributů definovaných normou ISO 14906.

Požadavky na zkoušení nejsou předmětem této technické specifikace.

2 Související normy

EN ISO 14906 Dopravní telematika – Elektronický výběr poplatků – Definice aplikačního rozhraní pro radiový přenos na krátkou vzdálenost (DSRC) a

EN 15509:2007 Dopravní telematika – Elektronický výběr poplatků (EFC) – Aplikační profil interoperability pro DSRC

Zkoušení parametrů je řešeno v CEN ISO TS 13143-1 a 2.

3 Termíny a definice

V této kapitole je stanoveno 14 termínů, mezi jinými i

3.12 kontext mýtného (*toll context*) logický pohled na konkrétní režim mýtného definovaný atributy a funkcemi

3.13 režim mýtného (*toll regime*) sada pravidel definující mýtné schéma, tj. pravidla definující zpoplatnění a proces zpoplatnění pro specifické opatření zpoplatňující silničního uživatele

4 Zkratky

AC_CR access credentials – Pověření k přístupu

CCC Compliance Check Communication – Komunikace pro kontrolu shody, kontrolní komunikace

ADU Application Data Unit – Datová jednotka aplikační vrstvy

5 Architektura aplikačního rozhraní

Tato kapitola obsahuje základní informace o architektuře komunikace CCC. Identifikuje služby poskytované aplikacím CCC a funkce, které tyto služby implementují. Také definuje principy vztahující se k atributům a použití základních prvků komunikace DSRC. Podrobný popis funkcí je obsahem kapitoly 6; podrobný seznam atributů je uveden v kapitole 7.

Aplikační rozhraní CCC bylo vyvinuto tak, aby mohlo využívat sestavu protokolů CEN-DSRC prostřednictvím aplikační vrstvy specifikované normou ISO 15628 a EN 12834. Informace o mapování odpovídajících služeb pro další identifikovaná komunikační média DSRC jsou uvedeny v přílohách (viz tabulka 1). Aplikační rozhraní CCC poskytuje aplikacím CCC tyto služby:

- přístup ke kontrolním atributům tak, aby zařízení RSE mohlo ověřit, zda OBE splňuje požadavky,
- vzájemná autentizace zařízení RSE a OBE prostřednictvím výměny ověřovacích údajů;
- příkaz vydaný zařízením OBE sdělující uživateli výsledek kontroly

Výše uvedené služby jsou realizovány pomocí výměny protokolů prostřednictvím komunikačních služeb a transakcí, jak je popsáno v kapitole 8. RSE může z OBE načítat libovolnou kombinaci atributů. Atributy jsou identifikovány a zjišťovány pomocí mechanismů definovaných normou ISO 14906.

Tabulka 1 – Podporované sestavy komunikačních protokolů na krátkou vzdálenost

Médium	Aplikační vrstva	Nižší vrstvy	Detailní specifikace
CEN-DSRC	EN 12834 a ISO 15628	EN 12795 EN 12253	Specifikace viz 5.5.2
Italská UNI DSRC	UNI 10607-4:2007 UNI 10607-3:2007	UNI 10607-2:2007 UNI 10607-1:2007	Příklad implementace v příloze C
ISO CALM IR	EN 12834 a ISO 15628	ISO 21214	Příklad implementace v příloze D
ARIB DSRC	ARIB STD-T75 a ISO 15628	ARIB STD-T75 ITU-R.M1453-2	Příklad implementace v příloze E

6 Funkce

V této kapitole jsou definovány funkce, které musí být dostupné pro OBU. V rámci CEN-DSRC jsou funkce zabezpečovány aplikační vrstvou DSRC podle normy ISO 15628 a EN 12834 (služby 'INITIALISATION', 'GET' a 'RELEASE') nebo jsou implementovány podle příslušných funkcí EFC, jak specifikuje norma ISO 14906 (funkce 'GET_STAMPED', 'SET_MMI' a 'ECHO').

V článcích této kapitoly jsou definovány funkce výhradně pro CEN-DSRC. Dalším médiím podporovaným v souladu s předchozí kapitolou musí být poskytnuta ekvivalentní funkcionality, viz příloha C pro UNI 5.8 GHZ mikrovlnného DSRC, příloha D pro CALM infračerveného DSRC a příloha E pro ARIB mikrovlnného DSRC.

Funkce definované v této kapitole spadají do následujících kategorií:

- Zahájení komunikace,
- Přístup k datům,
- Autorizovaný přístup k datům,
- Upozornění řidiče,
- Ukončení komunikace a
- Test komunikace.

Tato technická specifikace se zabývá autentizačními službami, které budou pravděpodobně sloužit k ověření identity zdroje dat, integrity dat a zabraňovat jejich zpochybnění. Obsahuje mechanismus kontroly přístupu k datům zařízení OBE pomocí ověřovacích přístupových údajů. Ochrana přístupu rovněž slouží jako ochrana soukromí uživatele.

7 Atributy

Tato kapitola uvádí všechny atributy a datové prvky v kontextu CCC, které musí být dostupné na straně OBE. Jedná se o prvky Atributy CCC podle normy EN 15509 a Specifické atributy CCC

Dále jsou zde specifikovány atributy CCC týkající se identifikace, stavu a vozidla ve smyslu

- názvu datového atributu,
- názvů datových prvků tvořících CCC atribut (žádný CCC atribut neobsahuje volitelný datový prvek),
- sémantické definice datového prvku, a
- informativních poznámek, včetně odkazů na jiné normy.

8 Transakční model

V této kapitole jsou odkazovány požadavky na transakční model související s aplikačním rozhraním LAC pro DSRC. Ten musí splňovat požadavky EN ISO 14906, kapitoly 6, s omezeními a doplňky definovanými v přílohách pro implementace používající sestavu komunikačních protokolů CEN DSRC.

Dále kapitola obsahuje popis 2 fází transakčního modelu: inicializace a transakce.

Příloha A (normativní) Specifikace datových typů CCC

Tato příloha obsahuje ASN.1 definice:

- datových typů souvisejících s funkcemi CCC, jak je specifikováno v kapitole 6;
- datových typů souvisejících s atributy CCC, popsány v kapitole 7;
- typy kontejnerů ASN.1 pro ISO aplikační vrstvu 7,

používající metodu abstraktního syntaktického zápisu (ASN.1) podle ISO/IEC 8824-1. Pravidla zhuštěného kódování musí být aplikována podle ISO/IEC 8825-2.

Příloha B (normativní) Formulář PICS pro datové prvky v atributu

Pro posouzení shody konkrétní implementace je nutné mít prohlášení o tom, jaké schopnosti a možnosti byly implementovány. Takové prohlášení se nazývá Prohlášení o shodě implementace (ICS) nebo přesnější pro případ, kdy pokrývá transakce, Prohlášení o shodě implementace protokolu

(PICS). Cílem tohoto formuláře PICS je poskytnout mechanismus, kterým by dodavatel implementace podle požadavků definovaných v této technické specifikaci, mohl podávat informace o implementaci standardizovaným způsobem.

Formulář PICS je rozdělen do článků podle těchto kategorií informací:

- identifikace implementace;
- identifikace protokolu;
- souhrnné prohlášení o shodě;
- tabulky formuláře PICS.

Tato příloha se zabývá použitím formuláře Prohlášení o shodě implementace protokolu (PICS) pro atributy definované v kapitole 7 a příloze A.

Příloha C (informativní) Použití sestavy komunikačních protokolů UNI DSRC pro aplikace CCC

Tato rozsáhlá příloha obsahuje požadavky na aplikaci CCC využívající jako komunikační médium zásobník UNI DSRC definovaný dle normy UNI 10607. Ukazuje, jak zobecněné funkce komunikace CCC mapovat do základních funkcí služby UNI DSRC a uvádí příklad, jak lze uchovávat typy informací CCC a získávat informace od zařízení OBE kompatibilního se standardem UNI DSRC.

Měly by být použity bezpečnostní algoritmy a kalkulace, transakční model, jak je specifikováno normou UNI 11310, [UNI Profile], týkající se interoperability DSRC.

Příloha D (informativní) Použití sestavy komunikačních protokolů CALM IR pro aplikace CCC

Tato příloha velmi stručně specifikuje použití sestavy komunikačních protokolů IR v CALM pro aplikace CCC podle ISO 21214.

Příloha E (informativní) Použití sestavy komunikačních protokolů ARIB DSRC pro aplikace CCC

Tato příloha velmi stručně specifikuje, jak aplikace CCC používá ARIB mikrovlnné DSRC na frekvenci 5.8 GHz.

Příloha F (informativní) Příklady transakce CCC

Tato příloha obsahuje příklad transakce komunikace CCC, při níž dojde k načtení všech dat a poskytnutí podpisů zaručujících integritu/autenticitu dat OBE a jejich ochranu proti zpochybnění.

Příloha G (informativní) Doporučení týkající se zabezpečení

Tato příloha obsahuje všeobecné informace, důvody pro použití a příklad použití zabezpečovacích funkcionalit komunikace CCC popsanych v této technické specifikaci.

Požadavky na zabezpečení komunikace CCC vyplývající z těchto hlavních požadavků výběřčího mýtného:

- výběřčí mýtného si klade za cíl donucovat k plnění svých povinností ty uživatele, kteří nesplňují povinnost spolupráce (např. deklarováním správné třídy a dohlížením na stav OBE);
- výběřčí mýtného si klade za cíl donucovat k plnění svých povinností ty uživatele, kteří záměrně ovlivňují proces výběru poplatků v OBE;
- výběřčí mýtného si může volitelně přát využívat tento kontrolní mechanismus ke kontrole dat o použití poskytovatele služby a ověřování jejich pravosti, tj. porovnávání dat o použití s událostí detekovanou na straně kontrolní stanice.