EXTRAKT z české technické normy

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

ICS 35.240.60

Dopravní a cestovní informace (TTI) –TTI zprávy ČSN P pomocí celulárních sítí – Část 5: Vnitřní služby CEN TS 14821-5

01 8254

Platí od 1. 4. 2005 104 stran

Předmluva

Tato technická specifikace sestává z osmi částí. První část popisuje základní architekturu systému, kterou se v tomto případě rozumí architektura klient – server s využitím sítě GSM. Části 2 až 8 popisují jednotlivé aspekty této datové komunikace.

Úvod

Servisní organizace poskytují služby ve formě zprostředkování dopravních a cestovních informací, které získávají a vytvářejí na základě svých vstupních dat. Dopravní a cestovní informace jsou z těchto center služeb šířeny nejrůznějšími komunikačními kanály ke koncovým zařízením. Těmi mohou být statické displeje zobrazující přijaté nápisy či zprávy pomocí piktogramů, přenosné terminály (např. PDA s bezdrátovým připojením), či telematické terminály umístěné ve vozidlech (zde často tyto terminály plní i funkce navigačních systémů).

Tato část číslo 5 se zabývá částí systému, která pro koncového zákazníka nemá žádný přímý užitek, je však nutná pro hladký chod systému, jeho efektivní správu, diagnostiku i pro případné opravy či úpravy.

Užití

Tato technická specifikace definuje funkcionalitu i interface dopravních telematických služeb, založených na použití buňkové radiové sítě. **Výrobcům terminálů** je tímto umožněno, aby vyráběli zařízení kompatibilní s tímto systémem přenosu dopravních informací, což má důležitý vliv na interoperabilitu různých výrobců koncových zařízení, a to i na mezinárodní úrovni. V případě této části se jedná o materiál, který bude mít význam pravděpodobně jen pro výrobce koncových terminálů z hlediska jejich firmwarového vybavení, poskytovatele služeb a servisní firmy.

Souvisící normy

Protože tato část se často odvolává na kryptografické postupy, které jsou svou podstatou velmi složité a není je zde možno (ani to není účelem této normy) podrobně vysvětlit, jsou zde odkazy na normy řešící tuto otázku.

3 Termíny, definice a zkratky

Kapitola 3.1 obsahuje termíny a definice použité v této normě.

Kapitola 3.2 obsahuje popis 61 zkratek, které jsou použity v této části: % ott, ADP, AM, ASN.1, BC, BCS, CA, CAS, CB, CBC, CLI, CRM, CSD, DES, DRM, DSC, ELB, FCD, FCDGM, FCDPM, FCDNSM, FCDRM, FCDVDSUM, GATS, GEM, GPS, GSM, IE, ICV, L_max, MAC, MNA, MF, MO, MT, MV, N_min, OBU, OF, OV, PDU, PFA, PMD, RSA, SAE, SMS, SMSC, SV, TEG, TINFO, TOC, TRP, TT, TTI, TTFF, UTC, VDS, vel, V, VIN, WAP. WGS 84. Některé z nich jsou obecně platné, název jiných se však někdy kryje s jinými běžně používanými zkratkami, a proto je u všech stručně vysvětlen obsah.

4 Specifikace vnitřních služeb – konfigurace a Master data

Úkoly vnitřních služeb se dají shrnout do tří základních bodů:

- Administrace přístupu, diagnostika funkcí a parametrů pro všechny služby;

- Administrace přístupu ke specifickým parametrům pouze pro vybrané služby;
- Základní test funkcionality.

Typickou funkcí, která může být přístupná pouze vybrané množině, je možnost změny údajů Master data, což jsou identifikační údaje vztahující se k vyrobenému vozidlu.

5 Specifikace správy klíčů a zajištění bezpečnosti

Procesy správy klíčů a šifrování dat se používají k ochraně dat při přenosech, zajišťování integrity dat a autorizace vysílajícího.

V této kapitole jsou uvedeny různé typy klíčů a jejich aplikace ve zprávách s bližším popisem jejich vytváření a používání. Jsou zde popsány principy a metody šifrování zpráv a způsob jejich používání. Metody a principy využívají standardy DES (Data Encryption Standard).

Norma rozeznává tři základní úrovně pro bezpečnostní operace:

- Úroveň zabezpečení, ve které se pohybuje výrobce zařízení;
- Úroveň zabezpečení, ve které se pohybuje poskytovatel servisních služeb;
- Úroveň zabezpečení pro servisní služby.

6 Aplikační datový protokol pro podmíněný přístup a zajištění bezpečnosti – konfigurace a správa klíčů

Typický konfigurační blok, odesílaný z centra služeb, má strukturu zprávy dle následující tabulky:

Tabulka 1 – Skladba konfiguračního datového bloku

Prvek informace	Délka (bitů)	Poznámka
Příznak aplikace	1	0: celková aktualizace; 1: aktualizace aplikace
Příznak sousedních zemí	1	0: seznam sousedních zemí není připojen; 1: zpráva obsahuje seznam sousedních zemí
Příznak adresy	1	0: není potřeba aktualizace adresového bloku; 1: aktualizace adresového bloku
Příznak přístupu	1	0: není potřeba aktualizace přístupových funkcí; 1: aktualizace přístupových funkcí
Příznak parametru	1	0: není potřeba aktualizace parametrů; 1: aktualizace parametrů je aktivní
Datový blok aplikace	Proměnná délka	Pokud je příznak aplikace =1, obsahuje identifikační číslo aplikace, ke které se tato relace vztahuje. Jedná se o binární číslo v rozsahu 0 ... 255.
Datový blok s informacemi o sousedních zemích	Proměnná délka	Pokud je příznak aplikace =1, obsahuje identifikaci zemí a sítí, ve kterých jsou dostupné telematické služby. Jedná se o binární číslo v rozsahu 0 ... 63.
Datový blok pro adresní údaje	Proměnná délka	Obsahuje následující položky: Typ aktualizace (celková nebo částečná); verzi systému adresace; počet bloků pro aktualizaci (N); blok č. 1; ... ; blok č. N.
Datový blok pro přístupový systém	Proměnná délka	Obsahuje následující položky: Status přístupu; prioritu aktualizace; datum platnosti a kontrolní blok přenosu.
Datový blok pro aktualizované parametry	Proměnná délka	Obsahuje řetězec aktualizovaných parametrů a jejich nových, aktualizovaných hodnot
Volný text	Proměnná délka	

Článek 6.3 věnovaný správě šifrovacích klíčů se zabývá jednotlivými druhy zpráv pro tyto účely, jakými jsou:

- Žádost o klíč (vysílá OBU jednotka);
- Kontrolní zpráva pro správu klíčů;

- Potvrzovací hlášení správy klíčů;
- Aktualizační zpráva pro správu klíčů (vysílaná centrem služeb).

Kapitola je doplněna praktickým příkladem – textovým výpisem aplikačního datového protokolu.

7 Specifikace diagnostické služby

Hlavním úkolem této služby je zajištění bezchybného provozu a případné nápravy (ještě než si zákazník začne stěžovat). Zprávy diagnostických služeb se přenášejí na transportní vrstvě protokolem ADP verze 2 a identifikátor této aplikace je označen v rámci transportní vrstvy „Application ID“ = 83 (hexa).

Předmětem této diagnostiky jsou následující oblasti:

- Status konkrétního zařízení (Identifikátor, výrobní číslo);
- Chybová statistika;
- Statistika funkcí spojených s určováním polohy;
- Volitelné funkce (test hlavních komponent vozidla, vozidlové sběrnice, senzorů i vlastního terminálu).

8 Aplikační datový protokol pro diagnostickou službu – hlavní definice a prvky informace

Diagnostické hlášení od terminálu je inicializováno výzvou k přenosu tohoto hlášení, které má strukturu popsanou v následující tabulce:

Tabulka 2 – Skladba diagnostického hlášení od terminálu

Prvek informace	Komentář
Hlavička hlášení	Popis hlavičky je uveden v CEN/TS 14821-1
Číslo žádosti	Přiděleno centrem služeb,
Návěští identifikace	(0 = je použito číslo zařízení, 1 = je použito sériové číslo)
Maska identifikátoru zařízení	
Identifikátor zařízení	
Maska sériového čísla	
Sériové číslo	
Textový blok	Pro diagnostické účely je tento blok definován v 8.2.7, jeho kódování je v CEN/TS 14821-3 Text a transparentní data

Identifikátor a sériové číslo slouží k verifikaci OBU jednotky. Maska přitom stanoví, jaké oblasti z identifikátoru nebo sériového čísla se dotaz týká. Pouze v případě, že verifikace dotazu je úspěšná, je diagnostické hlášení odesláno na centrum služeb.

Toto diagnostické hlášení má následující skladbu:

Hlavičku hlášení, identifikátor zařízení, statistiku chybných komunikací od posledního nulování tohoto čítače chyb, počet chybových hlášení, chybové hlášení č. 1, chybové hlášení č. 2, ... , dlouhodobě zjišťované statistické odchylky měřených veličin (poloha, rychlost) a volitelné informace (v textovém bloku).

Popis je doplněn výpisem z programu.