CEN TS 14821-4 - **Dopravní a cestovní informace (TTI) – Zprávy předávané celulárními sítěmi – Část 4: Protokoly nezávislé na službě**

Aplikační oblast: Dopravní a cestovní informace

Rok vydání normy a počet stran: Vydána 2005, 42 stran

Zavedení normy do ČSN: vyhlášením

Rok zpracování extraktu: 2008

Úvod

Tato technická specifikace sestává z osmi částí; první část obsahuje architekturu systému, kterou se rozumí klient-server s využitím sítě GSM. Další části, očíslované v řadě 2 až 8, se postupně zabývají jednotlivými detaily této datové komunikace.

Dopravní a cestovní informace jsou šířeny od servisních organizací, které na základě svých vstupních informací sestavují zprávy o dané problematice, nejrůznějšími komunikačními kanály ke koncovým zařízením. Těmi mohou být 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 norma se zabývá jedním ze základních prvků, které musí každá informace obsahovat. Tento prvek je definován v CEN TS 14821-3. K těmto, obrazně řečeno, základním kamenům každé zprávy patří informace o aktuálním čase a údaje, které definují zeměpisnou oblast vztahující se k předávané zprávě.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Užití

Tato norma definuje funkce a rozhraní 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 koncových zařízení od různých výrobců, a to i na mezinárodní úrovni.

1. Termíny a definice

Kapitola 3.1 obsahuje termíny a definice použité v této normě.

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

2. Symboly a zkratky

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, IE, ICV, L_max, MAC, MNA, MF, MO, MT, MV, N_min, OBU, OF, 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 s jinými běžně používanými zkratkami a proto je u všech stručně vysvětlen obsah.

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www. ITSterminology.org).

4 Protokoly nezávislých služeb

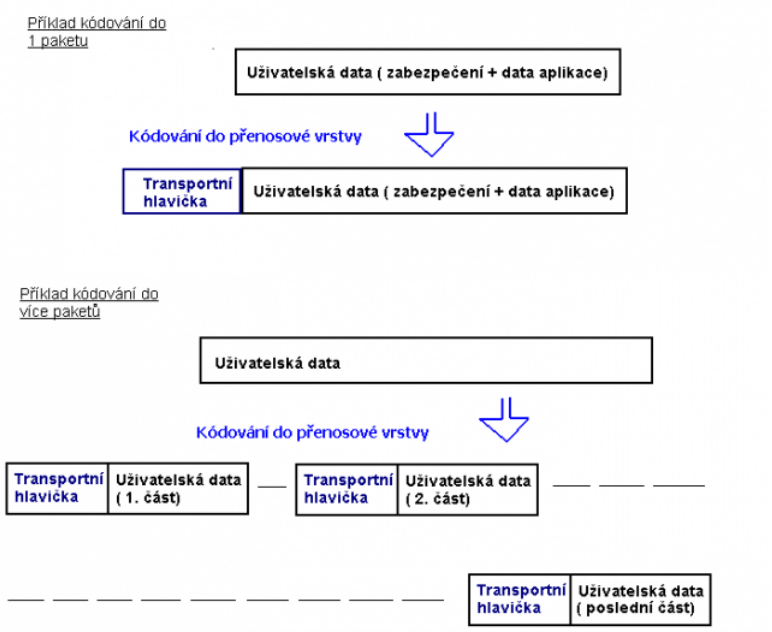
Pojmem protokoly nezávislých služeb jsou míněny takové protokoly, které bez ohledu na specifika aplikace zabezpečují podpůrné služby nutné pro její běh, jakými je třeba přenos dat a kontrola chybovosti přenosu, případně korekce chyby. Aplikační protokol poté od těchto nezávislých protokolů přebírá již ověřená (validní) data a nemusí tak řešit problematiku systému přenosu dat na nižších úrovních.

4.1.1 Přenosový protokol

Tento protokol je paketově orientován a koncipován pro přenosy s nízkou šířkou pásma. Nabízí následující funkce pro zmiňované vyšší vrstvy komunikace:

4.1.1.1 Paketování (Packaging).

Tato funkce je nejlépe patrná z následujícího příkladu:



4.1.1.2 Routování (Routing of Data for Service).

Koncové terminály nebo servisní centra mohou provozovat i více služeb, často na sobě nezávislých. Tehdy se adresování služeb stává obtížnější úlohou. Za účelem jednoznačného rozlišení jednotlivých služeb přenosová vrstva přenáší hodnotu identifikátoru aplikace (Application Identifier value).

Aby služby byly skutečně nezávislé, tak zařízení musí být připraveno obsluhovat současně více uživatelských aplikací, což vyžaduje speciální řízení celé procedury přenosu dat v případě použití výše popsaného balíčkování dat.

4.1.1.1.3 Kontex neboli Závislosti služeb (Service context).

Některé přenosy dat, vyžádané jedinou aplikací, probíhají rovněž souběžně. O této vlastnosti referuje výraz „závislost služby“. Vztah uživatelských dat a k nim příslušnou závislost služby lze vyhodnotit z kombinace položek identifikátoru aplikace (Application Identifier value), původce souvislosti (Contex Originator) a hodnoty pořadí posloupnosti (Contex Sequence Number), které jsou obsaženy ve výrazu hodnota závislosti (Contex Number).

Tato úloha je v kompetenci aplikační vrstvy a z toho důvodu se i výše uvedené výpočty odehrávají na aplikační vrstvě.

Terminál musí být připraven přijímat i nevyžádané zprávy, což platí všeobecně, nikoliv jen pro zprávy typu broadcast. Řízení přijímacích registrů (bufferů) musí být schopno tyto situace řešit.

4.1.1.1.4 Čas od poslední přijaté zprávy typu broadcast (Time since last received Broadcast PDU)

Při použití zpráv typu broadcast je důležité mít informace o použitelnosti tohoto způsobu přenosu. Každý terminál, který má implementován přenosový protokol typu broadcast, si musí pamatovat čas, který uplynul od doby, kdy naposledy přijal zprávu používající tento přenosový protokol, tj. zprávu určenou všem příjemcům (typ broadcast). Přenosová vrstva a procesy na ní probíhající potom mohou zajistit, na požadavek od aplikace, zpětný přenos údaje, který uvádí časový údaj o příchodu zprávy ve vteřinách.

4.1.1.2 Standardní přenos PDU neboli uživatelských dat (Standard Transport PDU)

Ke standardnímu přenosu protokolu náleží tyto položky:

- diskriminátor transportního protokolu - délka 2 hexadecimální čísla,
- ID aplikace,
- aplikační datový protokol (ADP - Application Data Protocol,) verze
- počáteční příznak (závisí na pořadí zprávy) a
- kontextové číslo (Contex Number), které se skládá z následujících částí:
- počátek kontextu (příznak indikuje počátek kontextu služby),
- kontextové pořadové číslo,
- pořadové číslo zprávy,
- další příznak (při současném přenosu více zpráv),
- celkový počet paketů,
- index aktuálního paketu, příznak schránky elektronické pošty (mailboxu),
- indikátor maximální délky.

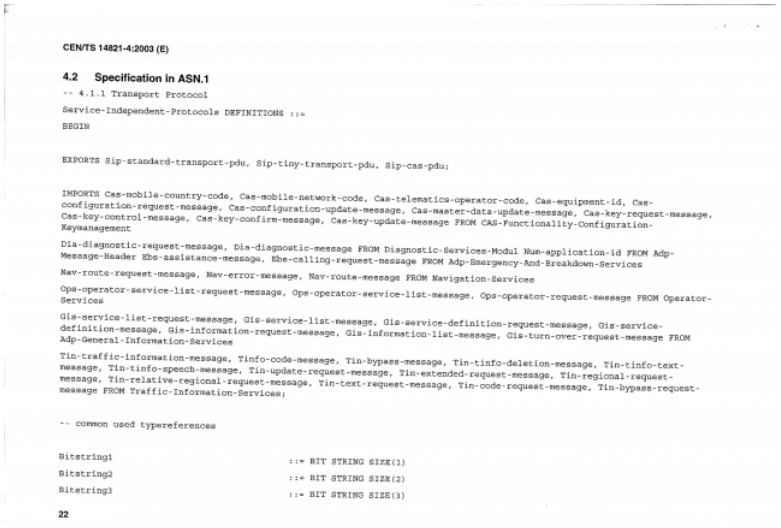
4.1.2 Pro unifikovaný protokol CAS (Conditional Access and Security – podmíněný přístup a bezpečnost) se používají tyto položky:

- diskriminátor CAS protokolu (binárně),
- metody šifrování (tabulky šifrovacích algoritmů a položek protokolu),
- řízení MAC (MAC - Message Authentication Code) – přístupový kód zprávy pomocí metody „triple MAC s dvojnásobnou délkou klíče“ nebo standardní s normální délkou klíče,
- norma šifrování dat (DEC - Data Encryption Standard) – symetricky,
- příznak ID zařízení,
- příznak délky MAC,
- ID zařízení,
- kódy země a operátora,
- generované číslo klíče – pro příjemce,
- klíč parametru,
- vlastní přístupový kód zprávy (MAC - Message Authentication Code),
- délka informace.

Uživatelská data jsou šifrována a délka protokolu CAS PDU závisí na transportní vrstvě a CAS hlavičce. Níže je naznačen způsob šifrování uživatelských dat do bloků. Zbytek dat, který neodpovídá délce šifrovaného bloku, se odesílá jako nešifrovaný poslední blok. Postupy výpočtu počtu bloků jsou také uvedeny.

Příloha A (informativní) Výpis zdrojových programů dle ASN.1

V příloze jsou uvedeny výpisy zdrojových programů popisujících problematiku definovanou v této části. Je uveden výpis z programu zabývající se definicí protokolu nezávislého na servisní službě dle ASN.1.



CEN/TS 14821-4:2003 (E)

4.2 Specification in ASN.1

```
-- 4.1.1 Transport Protocol
Service-Independent-Protocols DEFINITIONS ::=
BEGIN

EXPORTS Sip-standard-transport-pdu, Sip-tiny-transport-pdu, Sip-cas-pdu;

IMPORTS Cas-mobile-country-code, Cas-mobile-network-code, Cas-telematics-operator-code, Cas-equipment-id, Cas-
configuration-request-message, Cas-configuration-update-message, Cas-master-data-update-message, Cas-key-request-message,
Cas-key-control-message, Cas-key-confirm-message, Cas-key-update-message FROM CAS-Functionality-Configuration-
Keymanagement

Dia-diagnostic-request-message, Dia-diagnostic-message FROM Diagnostic-Services-Modul Num-application-id FROM Adp-
Message-Header Ebs-assistance-message, Ebs-calling-request-message FROM Adp-Emergency-And-Breakdown-Services

Nav-route-request-message, Nav-error-message, Nav-route-message FROM Navigation-Services

Ops-operator-service-list-request-message, Ops-operator-service-list-message, Ops-operator-request-message FROM Operator-
Services

Gis-service-list-request-message, Gis-service-list-message, Gis-service-definition-request-message, Gis-service-
definition-message, Gis-information-request-message, Gis-information-list-message, Gis-turn-over-request-message FROM
Adp-General-Information-Services

Tin-traffic-information-message, Tinfo-code-message, Tin-bypass-message, Tin-tinfo-deletion-message, Tin-tinfo-text-
message, Tin-tinfo-speech-message, Tin-update-request-message, Tin-extended-request-message, Tin-regional-request-
message, Tin-relative-regional-request-message, Tin-text-request-message, Tin-code-request-message, Tin-bypass-request-
message FROM Traffic-Information-Services;

-- common used typereferences

Bitstring1                    ::= BIT STRING SIZE(1)
Bitstring2                    ::= BIT STRING SIZE(2)
Bitstring3                    ::= BIT STRING SIZE(3)
```

22

Ve formě počítačových výpisů (viz příklad výše) nebo ve formě vysvětlujících tabulek v této příloze jsou uvedeny typy zpráv (složené z prvků informace (IE) různé délky):

- textové zprávy (IE: hlavička, stav, přítomnost časové značky, přítomnost expirační doby, záloha, časová značka, expirační doba, text);
- potvrzovací (IE: hlavička, potvrzení (Ack/Nack), záloha, časová značka, přídavné informace);
- zrušení zprávy (IE: hlavička, časová značka);
- poruchové hlášení (IE: hlavička, časová značka, kód chyby, popis chyby, akční položka kódu, příznak akční položky, text akční položky, adresa akční položky);
- žádost o spojení (IE: hlavička, automatický volací mód, přítomnost adresy pro zpětné volání (čísla), rezerva, adresa pro zpětné volání, jméno volaného účastníka, přídavné informace).