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.

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).

© Silmos, s.r.o. 2018 - 2025. *Pomůžeme Vám se zorientovat v oboru Dopravní telematiky a najít správnou normu.*