UNIVERZITA PARDUBICE
DOPRAVNÍ FAKULTA JANA PERNERA

KATEDRA ELEKTROTECHNIKY, ELEKTRONIKY
A ZABEZPEČOVACÍ TECHNIKY V DOPRAVĚ

Analýza vybraných funkčních vlastností mobilní části ETCS L2

Bc. Petr Gregar

DIPLOMOVÁ PRÁCE

2009

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 13. 5. 2009

Bc. Petr Gregar

ANOTACE:

Tato práce se zabývá rozborem protokolu Euroradio+ s ohledem na využití v zabezpečovací technice. Protokol zajišťuje slučitelnost radiových systémů, při výměně zpráv mezi vozidlovým a traťovým vybavením, se zohledněním bezpečnostních aspektů v aplikacích jako ATP systému ETCS Level 2 nebo 3.

Účelem práce je popsat chování (především) mobilní části systému ETCS L2 z hlediska zabezpečení informací. Tento popis by měl sloužit k pozdějšímu návrhu a testování systému před jeho nasazením do provozu.

ANNOTATION:

This thesis is concerned with protocol Euroradio+ considering to use it in signalling technology. The Euroradio+ protocol assures compatibility of radio systems related to message exchanging between vehicles and track equipment in applications as ATP - ETCS Level 2 or 3 with safety-related aspects taking into account.

The point of this thesis is to describe behaviour of onboard part of system ETCS Level 2 from securing of transmitted information point of view. This description should be applicable to a later design and testing of the ETCS system before its implementation to the real operation.

KLÍČOVÁ SLOVA:

ETCS, ERTMS, Euroradio, SFM (Safe Functional Module), CFM (Communication Functional Module), bezpečná komunikace.

KEYWORDS:

ETCS, ERTMS, Euroradio, SFM (Safe Functional Module), CFM (Communication Functional Module), safety communication.

PODĚKOVÁNÍ

Tímto bych rád poděkoval doc. Ing. Kunhartovi CSc. A Ing. Ouředníčkovi za jejich čas a pomoc při ujasňování některých pojmů.

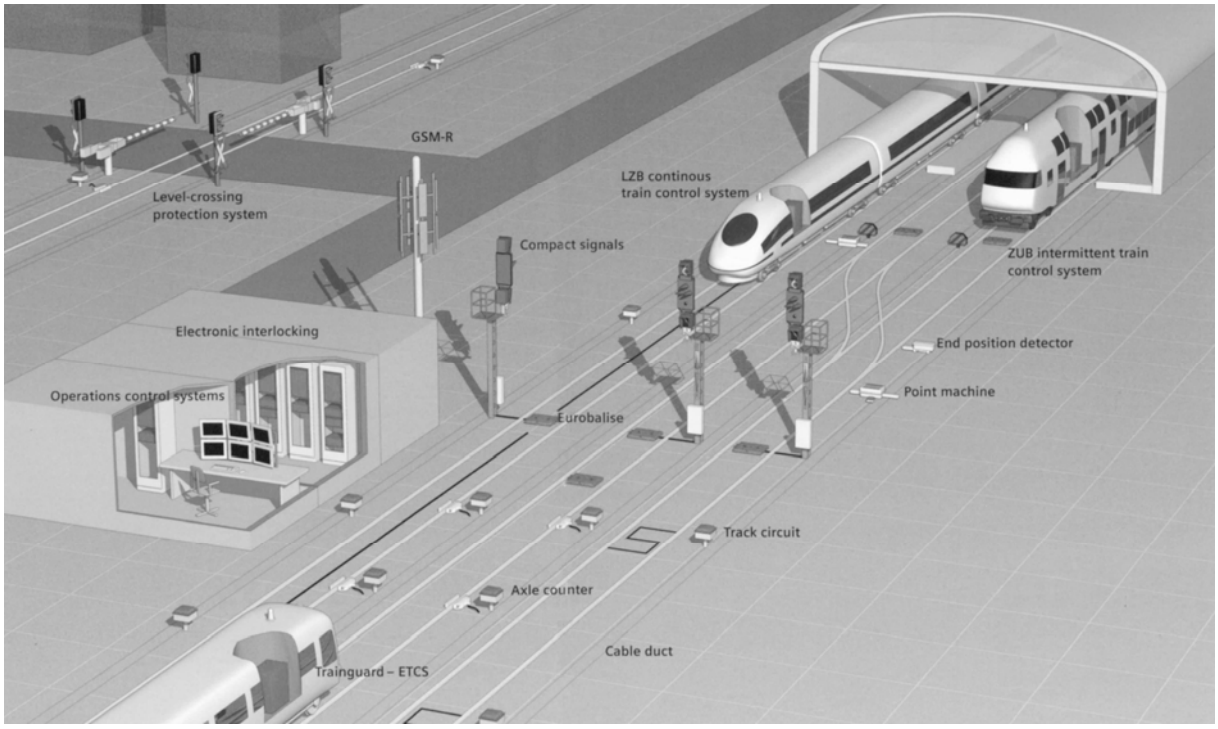
OBSAH

1 ÚVOD

Evropská agentura pro železnice (ERA) byla založena v roce 2004 na základě nařízení EU. ERA sdružuje i přední firmy z oblasti jako Alcatel, Alstom, Ansaldo Signal, Bombardier, Invensys Rail či Siemens. Tato organizace vznikla za účelem vytvořit podklady pro vznik integrovaného evropského železničního prostoru jak po stránce bezpečnostní, technické i právní. Za tímto účelem vydává ERA dokumenty, které mají ošetřit výše zmíněné aspekty železniční dopravy.

Mezi hlavní úkoly patří definice společného evropského systému kontroly vlaků (ETCS). Částí tohoto problému se zabývá i komunikační protokol EURORADIO. Tento protokol se vztahuje na radiokomunikační systémy poskytující své služby bezpečnostně relevantním aplikacím v otevřených sítích. Zajišťují slučitelnost radiových systémů, při výměně zpráv mezi vozidlovým a traťovým vybavením, se zohledněním bezpečnostních aspektů v aplikacích jako automatický vlakový zabezpečovač ETCS Level 2 nebo 3. Dodatečně specifikuje nepovinnou výměnu zpráv mezi vozidlovou částí a RIU pro ETCS Level 1.

Specifikace tohoto protokolu se nezabývají fyzickou architekturou subsystému radiového spojení, použitím otevřených sítí, funkcemi aplikací, ani tokem informací v aplikacích.



Obr.1 Ilustrační obrázek systému ETCS firmy SIEMENS

2 DEFINICE

2.1 Používané výrazy:

Povinné:

Funkce má být poskytnuta vozidlovou a/nebo traťovou částí, je-li požadována interoperabilita.

Volitelné:

Funkce může, ale nemusí být poskytnuta. Je-li poskytnuta musí být poskytnuta dle specifikací. Class1 nepožaduje volitelné funkce. Musí být zaručena slučitelnost mezi systémy EURORADIO poskytujícími a neposkytujícími doplňkové funkce, jinak musí být doplňková služba deaktivována.

2.2 Pojmy:

ATC (AUTOMATIC TRAIN CONTROL) – systém kontroly vlaků, navržený pro práci bez lidského zásahu.

ATP (AUTOMATIC TRAIN PROTECTION) – prostředek zajišťující bezpečnost vlakové dopravy zásahem, je-li překročen některý z určených bezpečných rychlostních či vzdálenostních parametrů.

AUTENTIZACE – (ověření původu zprávy) potvrzení, že zdroj zprávy je ověřený.

AUTENTIZACE – (ověření stejné vrstvy druhé strany (odpovídající vrstvy)) potvrzení, že entita odpovídající vrstvy ve spojení je jediná ověřená.

DES (DATA ENCRYPTION STANDARD) – blokový kód publikovaný roku 1977 NBS jako státní norma. USA 1981 přijatý jako ANSI standard X3.92.

DES KLÍČ – kryptografický klíč délky 64 bitů, každý 8. bit je redundantní paritní bit. Efektivní délka klíče je tedy 56 bitů.

FFFIS – je kompletní definice rozhraní mezi funkčními nebo fyzickými entitami. FFFIS garantuje slučitelnost, nikoli zaměnitelnost fyzických entit.

FIS (FUNCTIONAL INTERFACES SPECIFICAION) – specifikuje spojení mezi funkčními moduly nebo mezi fyzickými entitami: požadovaným tokem vnějších dat, požadovaným charakterem dat, požadovaným rozlišením a rozsahem dat.

FUNKČNÍ MODUL – skupina funkcí přispívající k realizaci samotného komplexního úkolu.

INTEGRITA DAT – vlastnost, udávající, že zpráva nebyla upravena či poškozena neautorizovaným způsobem.

JAZYK ETCS –množina dat a pravidel, která se podílí na naplnění požadavku unifikovaného přenosu informací mezi traťovou a palubní částí systému ERTMS/ETCS. Uplatňuje se na úrovni významových dat, tj. popisuje konkrétní parametry nezbytné pro jízdu vozidla (vzdálenosti, velikost rychlostních omezení, sklony, časové limity a pod.) popř. pro činnost ostatních systémů, zejména RBC (aktuální poloha vlaku, potvrzení příjmu daných informací, odsouhlasení změny parametrů, ...). Jazyk ETCS je definován systémovými požadavky ERTMS/ETCS SUBSET-02, konkrétně SUBSET-026- 7 a 026-8.

KLÍČ – termín pro šifrovací klíč. V této specifikaci se myslí obyčejně zřetězení tří DES kláčů s celkovou délkou 192b (3 x 64b).

MAC (MESSAGE AUTHENTICATION CODE) – kód poslaný se zprávou, sloužící k ověření, zda se zpráva od odeslání nezměnila a zda je zdroj zprávy ověřený a správný. MAC je funkce celé zprávy a klíče.

NÁRODNÍ DOPLŇKY – takto označované části závisí na národních železničních předpisech. Nesmí ohrozit interoperabilitu.

PADDING – informace užitá k vyplnění nepoužité části zprávy kvůli zachování blokové velikosti zprávy.

PEER ENTITA – tímto pojmem je myšlena entita stejné úrovně (na druhé straně spojení). Takže např. peer entita transportní vrstvy je entita transportní vrstvy našeho komunikačního partnera apod..

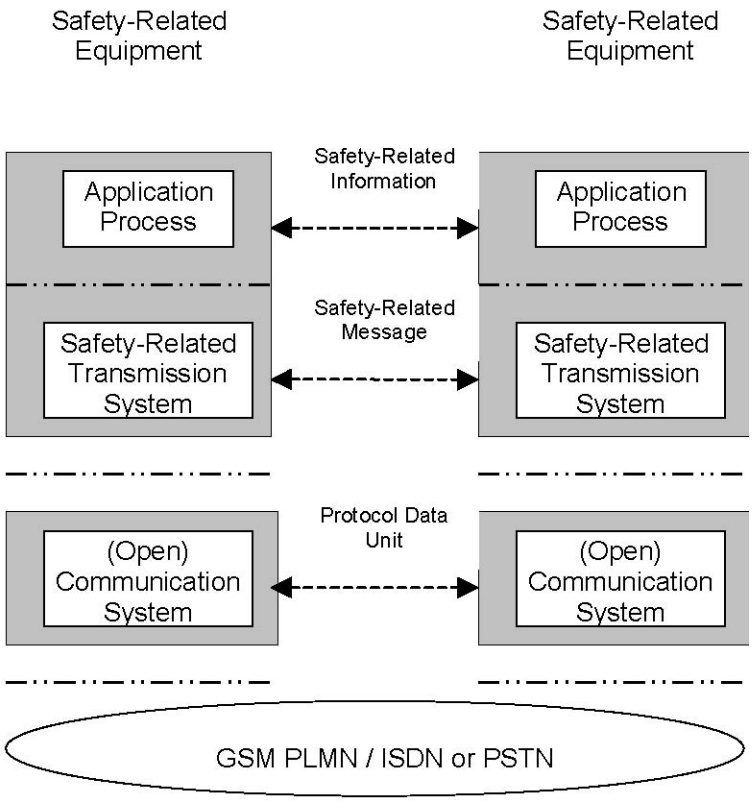
RCS (RADIO COMMUNICATION SYSTEM) – systém poskytující datovou komunikaci v otevřených sítích. Může být vybaven bezpečnými prvky tak, aby zajistil bezpečný přenos dat.

SPRÁVA KLÍČŮ – vytváření, uchování, přidělení, rušení, archivace a použití klíčů v souladu s bezpečnostní strategií.

3 REFERENČNÍ ARCHITEKTUA

EN50159-2 definuje referenční architekturu pro bezpečné systémy používající služby otevřených přenosových sítí. Obecná struktura bezpečnostně relevantních systémů, takových typů jako ETCS, je odvozena z EN50159-2.

Mimo bezpečných informací, si mohou aplikace bezpečnostně relevantního vybavení se vzdálenými aplikacemi vyměňovat také nikoli bezpečné informace.



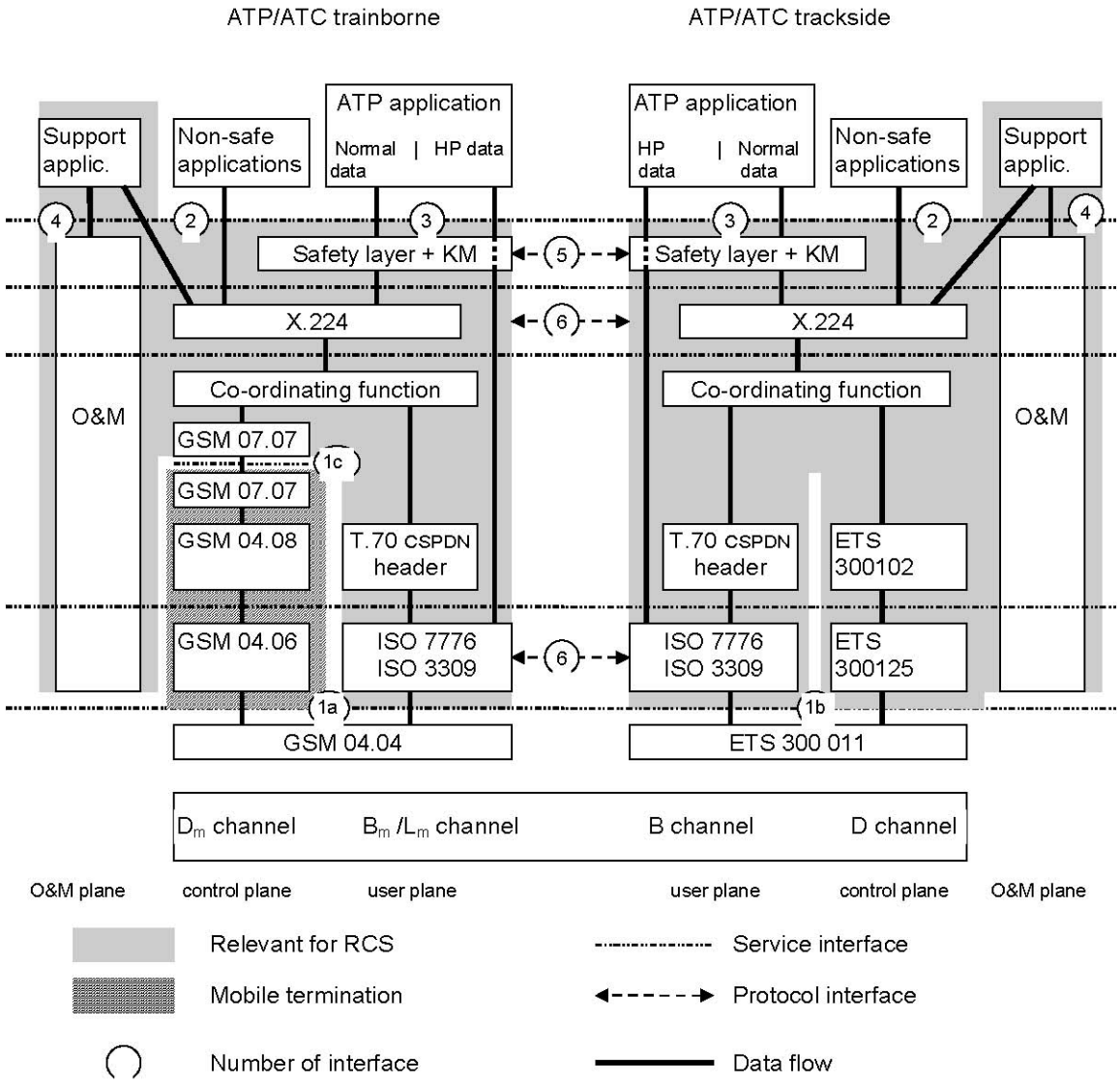
Obr.2 Struktura radio-komunikačního systému

Pro účel tohoto rozboru je otevřený přenosový systém rozdělen do dvou částí: sdělovací systém a otevřená síť.

Síť (v tomto kontextu) je souhrnné označení pro technické prostředky, jimiž je realizováno datové spojení (výměna informací). Otevřená síť je jistý druh sítě, ve které může nastat několik možných nebezpečí (viz EN50159-2). Otevřená síť je mimo rozsah této práce. Zahrnuty jsou pouze služby požadované rozhraním sítě.

Sdělovací (přenosový) systém je (v tomto kontextu) služba, používaná aplikací pro komunikaci mezi účastníky.

SFM (Safe Functional Module) radiokomunikačního systému poskytuje funkce bezpečného přenosového systému. CFM (Communication Functinal Module) radiokomunikačního systému poskytuje funkce komunikačního systému založeného na přenosových službách GSM-R PLMN. Obr.3 detailně zachycuje referenční architekturu RCS, založeného na tomto typu služeb. Definuje rozhraní mezi službami a rozhraní mezi protokoly.



Obr.3 Referenční architektura systému EURORADIO

Rozhraní 1 je rozhraní mezi RCS a příslušným přenosovým médiem. Rozhraní 1a je GSM PLMN rozhraní. Rozhraní 1b je rozhraní k pevným sítím na traťové straně. Rozhraní 1c je doporučené rozhraní mezi RCS a mobilním zakončením MT2 (viz EURORADIO FFFIS).

Rozhraní 2 je volitelné rozhraní mezi nikoli bezpečnými aplikacemi nebo podpůrnými aplikacemi a CFM. Tato možnost není vyžadována pro RIU v ETCS Level 1.

Rozhraní 3 je rozhraní mezi bezpečnými aplikacemi (např. ATP/ATC) a SFM (bezpečnou vrstvou).

Rozhraní 2 a 3 nejsou závazná pro interoperabilitu.

Rozhraní pro logické entity 5 a 6 je pro interoperabilitu povinné. Rozhraní je specifikováno v rámci popisů PDUs (Protocol Data Units) a komunikačně relevantních hledisek funkcí modulu.

Rozhraní 4 je místní rozhraní k Q&M a není v tomto popisu specifikováno.

4 ROZHRANÍ K BEZPEČNÝM SLUŽBÁM

Bezpečné služby poskytnuté SFM jsou přístupné přes bezpečné základní operace služby a jejich odpovídajícími parametry v SaSAP (Safety Service Access Piont).

Je věcí implementace přizpůsobit toto rozhraní k jejím potřebám a omezením, které nepožadují výměnu dat vzdušnou cestou a nemají žádný dopad na chování systému.

4.1 Základní operace služby pro navázání bezpečného spojení

Tab.1 Základní operace služby bezpečné vrstvy pro navázání spojení

SaS-zákl. oper. **Parametr**	**Sa-CONNECT.** **request**	**Sa-CONNECT.** **indication**	**Sa-CONNECT.** **response**	**Sa-CONNECT.** **confirm**
SaCEPID		X	X(=)	X
Volaná adresa • Typ adresy • Síťová adresa • ID mobilní sítě • Typ volaného ETCS ID • Volané ETCS ID	 X X(D) X(U) X X	 X X		
Volající adresa • Volající typ ETCS ID • Volající ETCS ID	 X(D) X(D)	 X(=) X(=)		
Odpovídající adresa • Odpovídající typ ETCS ID • Odpovídající ETCS ID			 X(D) X(D)	 X(=) X(=)
Typ aplikace	X	X(=)		
Třída QoS	X(D)			

X: hlavní parametr.

(=): hodnota parametru je stejná, jako hodnota korespondujícího parametru předchozí SaS základní operace (je-li k dispozici).

X(U): Použití tohoto parametru je volitelné.

X(D): Použití tohoto parametru je volitelné. Není-li poskytnut, bude použita přednastavená hodnota.

SaCEPID (Safe Connection EndPoint Identifier) – parametr identifikující každé bezpečné spojení v SaSAP (Safe Service Access Point) – je poskytnut místně.

Volaná adresa – identifikuje volaného SFM uživatele.

Typ adresy – kvalifikuje použití dílčích parametrů volané adresy.

Síťová adresa – síťová adresa volaného SaS uživatele. Tento parametr je složen z dílčích polí: délka volaného čísla, typ čísla, číslovací plán a vlastní číslo.

ID mobilní sítě – identifikuje mobilní síť. Skládá se z mobilního kódu země a mobilního kódu sítě dle ITU-T E.212

V případě spojení vyvolaného mobilní stranou, by měla žádost o spojení obsahovat dílčí parametr ID mobilní sítě, k vybrání příslušné sítě vztažené k volanému SaS uživateli.

ETCS ID, společně s typem ETCS ID jsou jedinečné v rozsahu ETCS. ETCS ID je užíváno bezpečnou vrstvou během ověřování peer entity. ETCS ID, typ ETCS ID a typ aplikace identifikuje SaS uživatele.

Poznámka: Parametr ETCS ID odpovídá popisu uváděném ve specifikacích, známých jako jazyk ETCS.

ETCS ID volané strany – tento parametr nese ETCS ID přidělené SaS uživateli, se kterým je/má být navázáno bezpečné spojení.

ETCS ID volající strany – tento parametr udává ETCS ID přidělené SaS uživateli, který požaduje bezpečné spojení.

ETSC ID odpovídající strany – parametr obsahuje ETCS ID přidělené SaS uživateli, se kterým bylo spojení navázáno.

Typ aplikace – je identický na obou stranách spojení.

Třída QoS – určí SFM uživatelům metodu specifikace jejich potřeby a dává CFM základy pro výběr protokolu nebo pro požadování služeb nižších vrstev. Parametr není mezi oběma stranami vyjednáván (nemůže být odmítnut). Tento parametr musí být akceptován poskytovatelem služby i peer aplikací, jinak bude požadavek na navázání spojení odmítnut.

Sa-CONNECT.request – zahajuje navazování bezpečného spojení. Bezpečný protokol si vynutí navázání spojení použitím požadavku T-CONNECT.request, přenosového systému nižší vrstvy.

Sa-CONNECT.indication – je užívaný volanou entitou bezpečné vrstvy k tomu, aby informovala volaného SaS uživatele o požadavku na navázání bezpečného spojení.

Sa-CONNECT.response – je použito odpovídajícím SaS uživatelem, k informování o akceptování spojení s entitou bezpečné vrstvy.

Sa-CONNECT.confirm – užito iniciační entitou bezpečné vrstvy k informování volajícího SaS uživatele o úspěšném navázání bezpečného spojení poté, co získala odpověď od volaného SaS uživatele.

Současné žádostí o bezpečné spojení dvou SaSAP jsou řešeny nezávisle bezpečnou vrstvou. Tyto souběžné žádosti mají za následek odpovídající množství bezpečných spojení. Je věcí žádajícího SaS uživatele, aby rozlišil potvrzení odpovídajících Sa-CONNECT.request.

4.2 Základní operace služby pro přenos dat

Jsou definovány dvě základní operace: žádost o odeslání dat
informace o příjmu dat

Tab.2 Základní operace služby bezpečné vrstvy pro přenos dat

Zákl. oper. / **Parametr**	**Sa-DATA.request**	**Sa-DATA.indication**
SaCEPID	X	X
Sa uživatelská data	X [1]	X(=)
Poznámka1: Délka musí být minimálně 1 oktet.		

Vysílaný Sa-DATA.request a přijímaný Sa-DATA.indication uskutečňují bezpečný přenos a bezpečnou proceduru ověření zdroje zprávy. Po provedení bezpečné procedury ověření zdroje zprávy, předá bezpečná entita uživatelská data rozšířená o autentizační kód zprávy (MAC) transportní vrstvě.

Uživatelská data jsou přenášena SFM transparentně (SFM tyto data nijak nevyužívá). Doporučená velikost bezpečných uživatelských dat je $\leq$ 114 oktetů. Maximální délka SaS uživatelských dat k přenesení je omezena na 1023 oktetů.

Při příjmu, po úspěšném provedení procedury ověření zdroje zprávy, jsou uživatelská data doručena SaS uživateli použitím základní služby Sa-DATA.indication. V případě chyby je doručeno Sa-REPORT.indication nebo Sa-DISCONNECT.indication.

Operace bezpečné vrstvy při přenosu SaS uživatelských dat mohou být navrženy jako fronta. Schopnost SaS uživatele vysílat Sa-DATA.request závisí na stavu fronty. Schopnost bezpečné vrstvy vydávat Sa-DATA.indication závisí na přijímajícím SaS uživateli.

4.3 Základní operace služby pro ukončení spojení

Odpojení je zaručeno pomocí těchto dvou operací: žádost o ukončení spojení
indikace ukončení spojení

Tab.3 Základní operace služby bezpečné vrstvy pro ukončení spojení

Zákl. oper. / **Parametr**	**Sa-DISCONNECT.request**	**Sa-DISCONNECT.indication**
SaCEPID	X	X
Disconnect reason	X	X
Disconnect sub-reason	X(U)	X

Sa-DISCONNECT.request je užíván SaS uživatelem k vynucení ukončení bezpečného spojení. Sa-DISCONNECT.indication je určen k informování SaS uživatele o ukončení bezpečného spojení.

Běžná žádost o ukončení od SaS uživatele obsahuje „Reason code“ 0. „Sub-reason code“ může být nastaven SaS uživatelem, dle jeho potřeb, v rozsahu 0 až 255.

Bezpečná vrstva může vydat nevyžádaný Sa-DISCONNECT.indication kdykoli během fáze nastavování spojení, nebo během fáze přenosu dat. Ukončení spojení může být způsobeno neschopností bezpečné vrstvy poskytnout danou službu.

Je možné použít i jiné posloupnosti základních služeb pro provedení ukončení spojení.

4.4 Základní operace služby pro hlášení chyb

Volitelně je hlášení chyb realizováno pomocí Sa-REPORT.indication.

Tab.4 Základní operace služby pro hlášení chyb

Zákl. oper. / **Parametr**	**Sa-REPORT.indication**
SaCEPID	X
Typ zprávy	X
Počet „dvojic“	X
Seznam „dvojic“	X

Bezpečná vrstva používá Sa-REPORT.indication k informování SaS uživatele o chybách, které se vyskytují v bezpečné vrstvě, nebo v nižších vrstvách. Sa-REPORT.indication je vyvolán automaticky (jestli-že je Sa-REPORT specifikovaná chybová reakce). Služba může být také použita k hlášení informací jiných typů než chyb (například diagnostiky). Parametr „typ zprávy“ je použit k rozlišení různých druhů informačních zpráv. Například typ 1 je definovaný pouze pro chybové zprávy.

„Dvojice“ obsahuje 2 parametry – reason (příčina) a sub-reason (detailnější popis příčiny).

4.5 Základní operace služby pro zprávy s vysokou prioritou

Služba pro data s vysokou prioritou je přístupná pomocí následujících dvou operací:

žádost o odeslání HP dat
informace o příjmu HP dat

Tab.5 Základní operace služby pro vysoce prioritní data

Zákl. oper. / **Parametr**	**Sa-HP-DATA.request**	**Sa-HP-DATA.indication**
SaCEPID	X	X
Sa uživatelská data	X	X(=)

Délka uživatelských dat je omezena maximálně na 25 oktetů.

Tyto data jsou přenášena nikoli spolehlivě a nikoli bezpečně. Není zaručeno, že přijímač data přijme. SaS uživatel musí poskytnout řádné potvrzení a opakování, v případě nutnosti.

Tato sekvence se podobá sekvenci pro bezpečný přenos dat.

4.6 Základní operace služby pro registraci do sítě

Pro registraci mobilní stanice do sítě jsou definovány dvě operace:

žádost o registraci do sítě
signalizace stavu registrace do mobilní sítě

Tyto 2 rutiny neposkytují bezpečné služby (takže nejsou bezpečnostně relevantní a nemají dopad na bezpečný protokol).

Tyto základní operace služby jsou předřazeny CFM a interpretovány jako příkaz/odpověď v rozhraní mobilní sítě.

Při implementaci, se mohou místo toho použít základní rutiny uvedené v dodatku B.5 SUBSETu 037.

Tyto rutiny jsou aplikované pouze na palubní část.

Tab.6 Základní operace služby pro přihlášení do sítě

Zákl. oper. **Parametr**	**Sa-REGISTRATION.request**	**Sa-REGISTRATION.indication**
Seznam MNID	X (>= 0 MNIDs)	X (>= 0 MNIDs)

Pomocí Sa-REGISTRATION.request může uživatel žádat o registraci jedné či více mobilních stanic do jedné či více mobilních sítí.

Seznam MNID (Mobile Network ID) je seznam ID mobilních sítí.

ID mobilních sítí identifikuje mobilní síť, ke které se chce přihlásit mobilní stanice. ID mobilní sítě se skládá z mobilního kódu země a mobilního kódu sítě dle ITU-T E.212.

Interpretace seznamu MNID je věcí implementace.

Seznam MNID může například obsahovat:

a) Žádný záznam – seznam MNID je prázdný:

Po všech dostupných mobilních stanicích se požaduje registrace do sítě prostřednictvím automatické síťové registrace (palubní vybavení GSM-R).

b) Jeden záznam:

Po všech dostupných mobilních stanicích se požaduje registrace do sítě používající manuální síťovou registraci z palubního vybavení GSM-R.

c) Dva různé záznamy (MNID#1 a MNID#2):

Mobilní stanice se může rozdělit na dvě části a ty registrovat pomocí obou MNID do obou sítí. V případě, že mobilní stanice, nejsou schopny vykonat registraci do obou sítí, registrace bude poskytnuta dle priority v seznamu – nejprve bude dostupné MNID#1.

Stav registrace do mobilní sítě se signalizuje pomocí Sa-REGISTRATION.indication uživateli služeb. Základní operace služby obsahuje seznam ID mobilních sítí, které jsou k dispozici, protože mobilní stanice v nich byla zaregistrována.

Uživatel není informován o tom kolik mobilních stanic je dostupných, ale přijímá pouze seznam registrovaných sítí, což pro něj znamená, že může, ale nemusí v těchto sítích použít požadavek o spojení.

Je-li vydávaný seznam ID mobilních sítí prázdný, registrace mobilní stanice nebyla provedena nebo byl ztracen signál.

Indikace registrace do sítě může být poskytnuta nezávisle na požadavku. Tato vlastnost dovoluje indikaci po zapnutí či po ztrátě pokrytí. Mohou být indikovány jakékoli změny registrace do sítě.

5 SFM – Safety Functional Module

5.1 Definice služby

Rozhraní mezi uživatelem bezpečné vrstvy a bezpečnou vrstvou není pro interoperabilitu závazné.

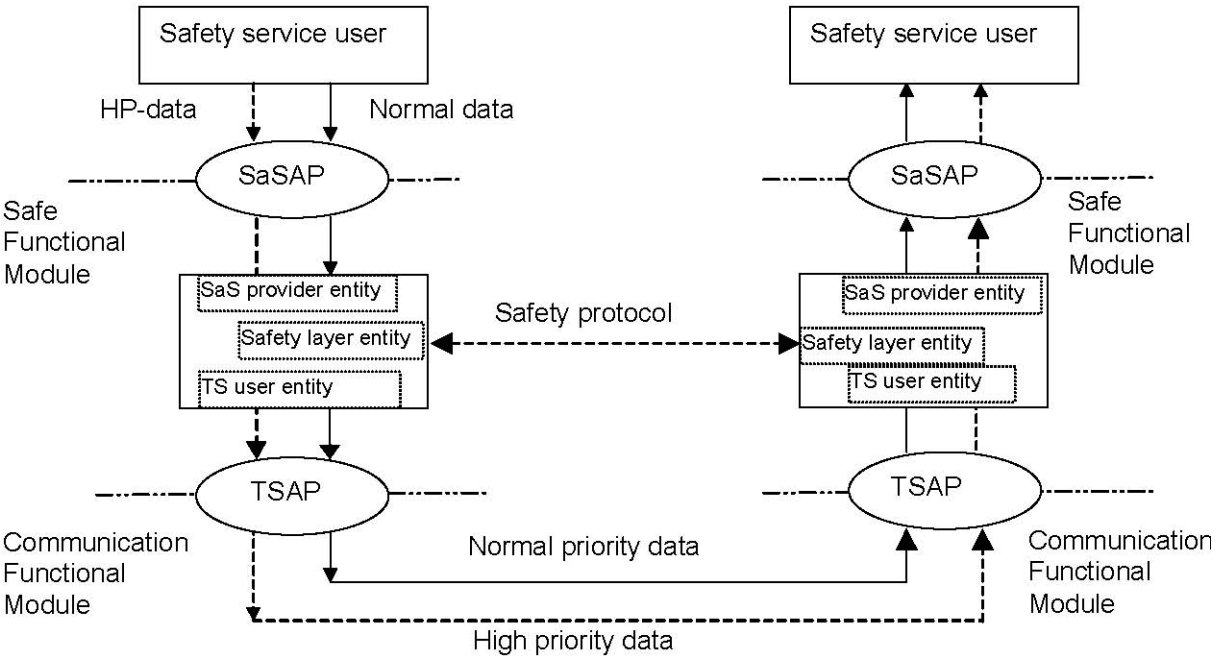
Tato část specifikuje rozhraní mezi SFM a uživatelem SFM. Tj. toky dat do/z SFM, poskytující bezpečné služby. SaS uživatel si vyměňuje data s SaS poskytovatelem.

Bezpečné služby poskytují bezpečné navázání spojení a bezpečný přenos dat během spojení. Bezpečný přenos dat poskytuje integritu a autenticitu dat. SFM ohlašuje chyby, které se vyskytly v bezpečné vrstvě a předává informace o chybách z nižších vrstev.

5.1.1 Model bezpečných služeb

Bezpečná entita komunikuje se svými uživateli pomocí jednoho či několika bezpečných přístupových bodů (SaSAP – Safe Service Access Piont) prostřednictvím bezpečné základní operace. Bezpečné entity podporují výměny dat pomocí bezpečného spojení prostřednictvím „safety protocol data units“ (SaPDU). Tyto přenosy užívají služby transportní vrstvy přes jedno přenosové spojení (TC) skrze jeden přístupový bod přenosové služby (TSAP). Výměna dat pomocí SaPDU je pouze logickým pohledem. Běžné operace přenášejí normální data a HP-operace přenášejí HP-data.

Následující obrázek zachycuje model a nikterak neomezuje implementaci.



Obr.4 Model bezpečných služeb

5.1.2 Navázání bezpečného spojení

Autentizace peer entity je poskytnuta bezpečným protokolem mezi entitami bezpečné vrstvy. Při požadavku na navázání bezpečného spojení bezpečná vrstva aktivuje odpovídající mechanismus na ověření autentizace entity.

Proces zahajující navázání bezpečného spojení je inicializován tehdy, když SaS uživatel požádá bezpečnou vrstvu o spojení. SaS uživatel vyšle informaci o adrese a požadavek QoS, bezpečné vrstvě. Tato QoS hodnota je předána CFM a je interpretována jako požadavek na předdefinovanou množinu QoS (Duality of Service - kvalita poskytovaných služeb).

Služba, poskytující bezpečné spojení je realizována provedením bezpečné procedury „autentizace peer entity“. Navázání transportního (přenosového) spojení mezi traťovou a vozidlovou částí je nutnou podmínkou k navázání bezpečného spojení.

Každá chyba ve vykonání bezpečné procedury „autentizace peer entity“ musí vždy vyústit v odmítnutí navázání spojení a v ukončení transportního spojení.

5.1.3 Bezpečný přenos dat

Bezpečná vrstva zajišťuje výměnu uživatelských dat v obou směrech současně a chrání integritu a rozsah uživatelských dat.

SFM entita garantuje bezpečný přenos dat pro bezpečnostně relevantní zprávy. Služba bezpečného přenosu dat používá bezpečnou proceduru „ověření původu zprávy“.

Tato procedura poskytuje ochranu proti porušení integrity a proti vložení nových zpráv neautorizovanými uživateli přenosového kanálu. Porušením integrity se myslí jakákoliv modifikace zprávy aktivním útokem, či vinou náhodných chyb přenosového kanálu.

Vždy, když SFM entita přijme datovou zprávu, dodanou přenosovým systémem (zprávy od SaS uživatelů jsou považovány za bezpečné), měla by ověřit, zda zpráva byla poslána odpovídající peer entitou, a že zpráva nebyla pozměněna během přenosu. Obě operace (tj. ověření odesílatele a integrity zprávy) jsou zabezpečeny provedením procedury „ověření původu zprávy“.

5.1.4 Ukončení bezpečného spojení

Ukončení bezpečného spojení je vykonáno:
jedním či oběma SaS uživateli ukončením navázaného bezpečného spojení
bezpečnou vrstvou uvolněním navázaného bezpečného spojení
jedním či oběma SaS uživateli přerušením navázaného bezpečného spojení
bezpečnou vrstvou indikující svoji neschopnost založit požadované bezpečné spojení

Ukončení bezpečného spojení je možné kdykoli, bez ohledu na aktuální fázi bezpečného spojení. Požadavek na ukončení nemůže být odmítnut. Bezpečná služba negarantuje doručení Sa uživatelských dat jakmile se zahájí ukončování spojení.

Žádost SaS uživatele o ukončení bezpečného spojení nepotřebuje specifikovanou bezpečnou ochranu na rozdíl od bezpečného navázání spojení, protože ukončení spojení má vliv pouze na dostupnost. Navíc je bezpečné spojení smysluplné, pouze když nejsou ukončena základní spojení mezi nižšími vrstvami, a transportní či síťové spojení může být ukončeno nezávisle na bezpečné vrstvě.

5.1.5 Hlášení chyb

Bezpečná vrstva poskytuje funkci hlášení chyb pro navázané bezpečné spojení SaS uživateli. Nastalé chyby jsou buď indikované pomocí ukončení bezpečného spojení, nebo volitelně pomocí hlášení o chybách. Neschopnost bezpečné vrstvy poskytnout službu bude hlášena SaS uživateli.

5.1.6 Přenos dat s vysokou prioritou

Bezpečná vrstva neposkytuje ochranu pro data s vysokou prioritou. Služba nesmí být použita před úspěšným navázáním bezpečného spojení, tj. může být použita pouze po úspěšném výkonu bezpečné procedury „ověření původu zprávy“.

Velikost HP dat je omezena.

Požadavek Class1: Je povinné být schopný přenést HP data z RBC na vlak.

5.2 Bezpečný protokol

5.2.1 Úvod

Tato část poskytuje detailní specifikace bezpečného protokolu založeném na standardu sdružení CENELEC - EN50159-2. Metoda užitá v SFM odpovídá třídě A1 v EN 50159-2, tj. metoda používající kryptografický bezpečnostní kód s tajným klíčem.

5.2.2 Funkce bezpečné vrstvy

Bezpečná vrstva poskytuje bezpečný přenos uživatelských dat, což zahrnuje i navázání a ukončení bezpečného spojení.

5.2.2.1 Bezpečné procedury

a) Ověření původu zprávy a integrita zprávy

Tyto bezpečné procedury zajišťují integritu a autenticitu během přenosu zpráv. Slouží k ochraně zpráv proti modifikaci a k zajištění, že se nikdo nemůže maskovat jako původce zprávy. Dále je procedura prostě nazývaná „ověření zdroje zprávy“, přestože automaticky poskytuje i ověření integrity.

Procedura1: Message Authentication Origin (MAC) při vysílání (m,Ks)

VSTUP

Zpráva m a kryptografický klíč K_S (Session Key, K_{SMAC}), sdílený mezi odesílatelem (se zdrojovou adresou SA) a příjemcem (s adresou příjemce DA). SA a DA jsou identity ETCS.

PROCEDURA

1) Nastavení příznaku směru zprávy m (hodnota „0“ pro iniciátora, hodnota „1“ pro odpovídajícího).

2) Před zprávu se připojí cílová adresa -> DA | m.

3) Spočte se délka *l* řetězce „DA | m“ v bajtech a přidá se (parametr *l* o velikosti 2B) před řetězec pro výpočet MAC -> *l* | DA | m.

4) Není-li délka řetězce „*l* | DA | m“ celočíselný násobek 64b provede se tzv. vycpání (vyplnění - padding) vložením doplňkových dat na konec zprávy -> *l* | DA | m | p.

5) Vypočte se MAC pro řetězec "*l* | DA | m | p" použitím CBC-MAC funkce a kryptografického klíče K_S: MAC(m) = CBC-MAC(K_S, *l* |DA|m|p).

VÝSTUP

Nenastane-li chyba vygeneruje se MAC(m), nastane-li chyba informuje se Error management.

Ověření původu zprávy je provedeno následujícím způsobem:

Při vysílání dat (DT) SaPDU (Safe Protocol Data Unit), řízení (MA – Management) SaPDU, druhé autentizační zprávy (AU2) SaPDU, třetí autentizační zprávy (AU3) SaPDU, nebo autentizační odpověď (AR) Sa PDU, je spočtena MAC délky 64b (použitím zprávy m a kryptografického klíče Ks jako vstupu).

Výpočet MAC odpovídá ve všech případech ISO 9797-1. Použitá bloková šifra je jednoduchý DES s upraveným MAC algoritmem 3, kde je poslední blok dat při výpočtu MAC (postup výpočtu viz. dále) počítán zašifrováním pomocí K_1, dešifrováním pomocí K_2, pak zašifrováním pomocí K_3 (modifikace IEC 9797-1 jež používá pouze 2 klíče K a K´). Je použita metoda vycpávání (padding) IEC 9797-1.

Pro tyto SaPDUs je kryptografický klíč K_S, použitý pro výpočet MAC, session klíč, odvozený během navazování spojení. Délka klíče $K_S = (K_1, K_2, K_3)$ musí být 192 bitů (včetně paritních bitů). Každý osmý bit ze 192bitů by měl být nastaven na hodnotu odpovídající sudé paritě, jak je definováno ve standardu ANSI X.92.

Data s vysokou prioritou jsou posílána bez MAC ochrany.

ETCS identita přijímače (DA) je připojena před zprávu m, pro výpočet MAC. Identita je 24 bitový kód. Když je adresa kratší, před adresu jsou vřazeny nulové bity tak, aby parametr DA získal délku 24 bitů.

Délka *l* řetězce „DA | m" je spočtena a připojena před řetězec „DA | m" pro výpočet MAC. Délka řetězce *l* je 16ti bitový binární kód a není přenášena, protože přijímač si ji může spočítat.

Je-li to nezbytné, tj. když délka řetězce „DA | m" není celočíselný násobek 64 bitů, musí proběhnout vycpání před výpočtem MAC. Je přidáno tolik nulových bitů kolik je potřeba. Vycpávací data nejsou posílána, protože přijímač je může spočítat, když zná vycpávací algoritmus, který byl použit. Vycpání je tedy použito z důvodu výpočtu MAC.

CBC-MAC(K,X) funkce používá tajný kód K a libovolný datový řetězec X, pro který má být spočítaná. Výpočet je definován následujícím způsobem:

Nechť K = (K1,K2,K3), nechť X je představováno 64bitovými bloky dat X1,X2,…,Xq. Nechť E(Kn,Y) je bloková šifra, jednoduchý DES, kódující datový řetězec Y užitím klíče Kn (n=1,2,3), E-1(Kn,Y) je bloková šifra v dešifrovacím významu. Pak Hq je odvozeno tímto způsobem (iterací):

$H_0 = 0$

$H_i = E\ (K_1, H_{i-1}\ (XOR)\ X_i)$

$H_q = E\ (K_3, E^{-1}\ (K_2, E\ (K_1, H_{q-1}\ (XOR)\ X_q)))$

MAC datového řetězce X je roven H_q.

V případě DT SaPDU zpráva m = ´000´|MTI|DF|SaDU sestává z identifikátoru typu zprávy (MTI) určující typ DT SaPDU, příznak směru (DF) a bezpečná uživatelská data (SaDU).

Co se týče AU2 SaPDU, zpráva m = ETY|MTI|DF|SA|SaF|auth2 sestává z typu ETCS ID, MTI indikujícím AU2 SaPDU, DF, zdrojové adresy (SA), bezpečnostních rysů (SaF – Safe Features) a odpovídající autentizační zprávy auth2 = Ra|Rb|B (viz dále).

Zpráva AU3 SaPDU obsahuje zprávu m = ´000´|MTI|DF|auth3. Tato zpráva se skládá z MTI indikujícím AU3 SaPDU, DF a odpovídající autentizační zprávy auth3 = Rb|Ra (viz dále).

V případě AR SaPDU, zpráva m = ´000´|MTI|DF se skládá z MTI, jež identifikuje AR SaPDU a DF.

Příznak směru je použit jako ochrana proti útokům odrazem (zrcadlení). Je inicializován během navazování spojení. Jeho hodnota je 0, když iniciátor spojení vysílá zprávu a 1, když volaná strana spojení odesílá zprávu.

Nastane-li během výpočtu MAC chyba, je informován error management a přebírá další kroky. Nenastanou-li chyby, výstup výpočtu je MAC zprávy m.

Procedura2 : Ověření autentičnosti zprávy (MAC) na příjmu (m,K_S,MAC´(m´))

VSTUP

Zpráva m zahrnující příznak směru (DF), šifrovací klíč (K_S), který je sdílený mezi odesílatelem a příjemcem, MAC´(m´), což je MAC spočtený pro m´ odesílatelem.

PROCEDURA

1) Před zprávu m se připojí cílová adresa (DA) -> DA | m

2) Spočte se délka *l* řetězce „DA | m“ v bajtech a přidá se (parametr *l* o velikosti 2B) před řetězec pro výpočet MAC -> *l* | DA | m.

3) Není-li délka řetězce „*l* | DA | m“ celočíselný násobek 64b provede se tzv. vycpání (vyplnění - padding) vložením doplňkových dat na konec zprávy -> *l* | DA | m | p.

4) Výpočte se MAC pro řetězec „*l*|DA|m|p“ použitím CBC-MAC funkce a kryptografického klíče: CBC-MAC(K_S, *l*|DA|m|p)

5) Porovnání MAC a MAC´

6) Ověření hodnoty DF.

VÝSTUP

Zpráva m je předaná SaS uživateli v případě, že MAC = MAC´ a zároveň hodnota DF je správná. Jinak se dalších akcí ujímá Error management.

Při příjmu DT SaPDU, MA SaPDU, AU2 SaPDU, AU3 SaPDU, nebo AR SaPDU je vypočteno MAC podobným způsobem jako v případě vysílání. Vstupními parametry jsou zpráva m, kryptografický klíč K_S a MAC vysílané jako část přijatého SaPDU. Příjemce zprávy používá stejné parametry jako vysílač zprávy, odvozené od odesílatelovy a příjemcovy identity a typu zprávy. Zpráva m sestává ze stejných částí jaké jsou popsány výše. Přijímač přidává svoji ETCS identitu (DA) a vypočte délku řetězce „DA|m“, která musí být přidaná před zprávu kvůli výpočtu MAC a provede vycpání, je-li to nutné.

Je-li takto vypočtený MAC stejný s MAC přeneseným jako část SaPDU a jestliže hodnota DF je správná, uživatelská data jsou předána SaS uživateli. Vyskytne-li se chyba, například nesprávná

hodnota DF, MAC se neshoduje, nebo neexistuje kryptografický klíč pro základní spojení, je informován chybový management a přebírá další akce. Běžně začíná vyhodnocování kontrolou MAC a pouze když je korektní je užita informace v PDU. AU2 je výjimka, protože jsou třeba některé informace z PDU pro výpočet MAC.

b) Autentizace peer entity

Autentizace peer entity je bezpečná procedura, jež je použita během navazování spojení k výpočtu session klíče.

Prodedura3: Peer Entity Authentication (ETCS ID A, ETCS ID B, Kab)

VSTUP

ETCS ID účastníka A i účastníka B a sdílený autentizační klíč Kab.

PROCEDURA

Protokol autentizace peer entity bude definován později.

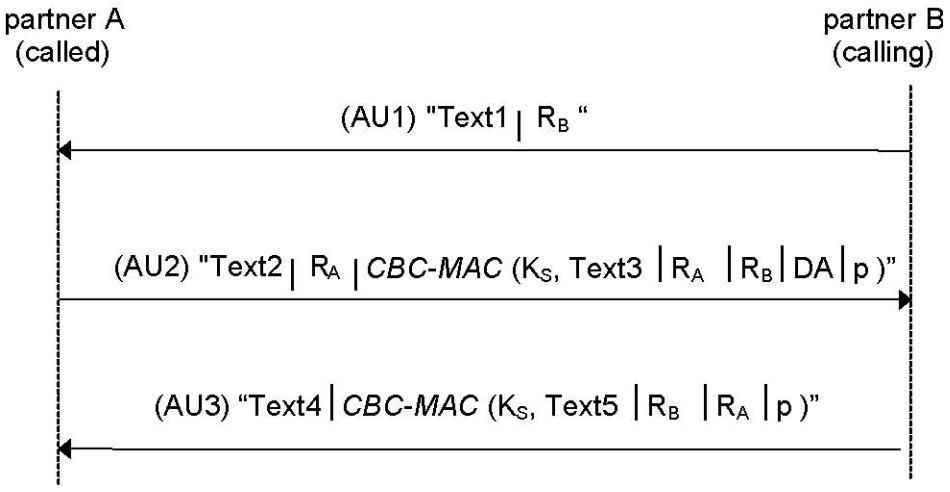
VÝSTUP

Nevyskytne-li se chyba, jsou úspěšně autentizováni oba uživatelé navzájem a je autentizován také session klíč jež sdílejí obě strany.

PŘÍPAD CHYBY

Nikoli bezpečné spojení mezi A a B. Je informován error management.

Autentizace peer entity je vykonávaná během navazování spojení. Její vstupní parametry jsou ETCS ID A i B, což jsou unikátní identifikátory. Autentizační kód byl předtím stranami A a B stanovený použitím logického či fyzického mechanismu určení klíčů.



Obr.5 Sa-Protokol použitý pro autentizaci peer entity a generování klíčů

Iniciátor navazování spojení (partner B) startuje bezpečnostně relevantní protokol, když požaduje spojení na úrovni transportní vrstvy. Pro výpočet MAC se užívá procedura „ověření zdroje zprávy“.

Iniciátor navazování spojení přenáší náhodné číslo Rb, délky 64 bitů, které je vygenerováno stranou B jako část první autentizační zprávy AU1SaPDU, směřující ke komunikačnímu partnerovi A. Náhodné číslo Rb musí být uloženo před odesláním AU1SaPDU. Po přijetí této zprávy, generuje A jako část druhé zprávy AU2SaPDU náhodné číslo Ra, délky 64 bitů a MAC vypočtený přes textové pole TEXT3, náhodná čísla Rb a Ra, identifikátor cíle DA (v tomto kontextu ETCS ID) a vycpávací bity. Pro výpočet MAC je generován klíč Ks užitím funkce generování session klíčů, použity parametry Ra, Rb a autentizační kód Kab. Po přijetí AU2SaPDU a odvození klíče Ks, část B kontroluje korektnost druhé autentizační zprávy přijaté od A. Poté B vypočte MAC přes pole TEXT5 a dvě náhodná čísla Ra, Rb a pošle jej jako část zprávy AU3SaPDU a uživateli A. Nakonec A zkontroluje AU3SaPDU použitím Ks.

Textová pole:

text1 = "ETY | MTI | DF | SA | SaF", kde SA = volající ETCS ID

text2 = "ETY | MTI | DF | SA | SaF", kde SA = volané ETCS ID

text3 = " | DA | ETY | MTI | DF | SA | SaF"

zde DA = volající ETCS ID, SA = volané ETCS

text4 = " ‘000’ | MTI | DF"

text5 = " | DA | ‘000’ | MTI | DF"

zde DA = volané ETCS ID

Textová pole se skládají z typu ETCS ID (ETY – ETCS ID Type), identifikátoru typu zprávy (MTI) indikující DF, SA (24bitů), DA (24bitů) a bezpečnostních rysů (SaF).

Nenastanou li chyby výstup procedury autentizace peer entity je provedena úspěšná autentizace účastníků A a B navzájem a session klíče K_S, sdíleným mezi učastníky A a B. Nastane-li chyba, je informován Error management a přebírá další akce. V tomto případě není mezi A a B navázáno bezpečné spojení.

c) Informace o HP datech

Bezpečná vrstva nechrání HP-data. Tato data jsou poskytnuta stejným spojením na úrovni transportní vrstvy jako běžná data. HP data se tedy přenášejí nikoli bezpečně a nikoli spolehlivě.

d) Šifrovací klíče

Funkce key managementu jsou popsány v Unisig SUBSET 038.

Následující tabulka popisuje úrovně hierarchie klíčů:

Tab.7 Hierarchie klíčů

Úroveň	Účel
3) Transportní klíče (K_{TRANS})	Chrání management komunikace mezi KMC a RBC nebo vlakem pro určení či obnovu autentizačních klíčů.
2) Autentizační klíče (K_{MAC})	Slouží k odvození session klíčů odvozených při navazování spojení.
1) Session klíče (K_{SMAC})	Chrání přenos dat mezi bezpečnými entitami.

K_{TRANS} klíče jsou použity KMC (Key Management Centrum) k distribuci klíčů úrovně 2, nebo k změnám přiřazení klíčů, včetně rušení klíčů a zavádění nových entit. KMC sdílí tyto klíče s každou entitou.

K_{MAC} klíče (také označované K_{ab}) jsou použity pro odvození session klíčů. Tyto klíče jsou přiřazeny jednotlivým entitám. Sdílejí-li dvě entity klíč úrovně 2, může být mezi nimi navázáno bezpečné spojení. Velikost takového klíče musí být 192 bitů (včetně bitů paritních), sestávající z tří 64bitových DES klíčů pro jednotlivé DES s upraveným MAC algoritmem.

K_{SMAC} (také označované jako K_S) jsou odvozeny během procedury autentizace peer entity, použitím klíče úrovně 2. Jsou užity pro ochranu během navázání spojení a přenosu dat, tj. výpočet MAC pouze v jednom spojení. Jsou pro každé spojení různé a mohou být sdíleny jen entitami jež sdílejí K_{MAC} klíč. Délka takovéhoto klíče je rovna 192 bitům a zahrnuje tři 64 bitové DES klíče.

Session klíče jsou generovány použitím procedury odvození klíčů, která je popsána níže. Oba komunikační partneři přispívají jejich 64 bitovými pseudonáhodnými čísly k session klíči.

Během procedury autentizace peer entity je odvozen session klíč dvěma komunikujícími entitami pomocí autentizačního klíče KMAC = (K1, K2, K3) těchto entit. Jeden 192 bitový KSMAC klíč se vygeneruje pomocí procedury odvození klíče. Odvození korespondujících DES session klíčů mezi entitami A a B je specifikováno dále.

Náhodné číslo Rx, kde x $\in$ {a,b} je rozděleno na dva (RxL a RxF) 32bitové bloky.

Ra = RaL|RaR a Rb = RbL|RbR.

Tři 64-bitové klíče Ks1, Ks2 a Ks3 jsou počítány dle následujícího předpisu:

$K_{S1} = MAC\ (RaL|RbL,K_{ab}) = DES\ (K_3,DES^{-1}(K_2,DES(K_1,RaL|RbL)))$

$K_{S2} = MAC\ (RaR|RbR,K_{ab}) = DES\ (K_3,DES^{-1}(K_2,DES(K_1,RaR|RbR)))$

$K_{S3} = MAC\ (RaL|RbL,K'_{ab}) = DES\ (K_1,DES^{-1}(K_2,DES(K_3,RaL|RbL)))$

Délka klíče úrovně 1 je 192 bitů včetně paritních bitů.

5.2.2.2 Komunikační procedury

a) Navázání spojení

Následující procedury jsou použity během navazování spojení: bezpečná informace o adrese je předána CFM a je aplikována procedura autentizace peer entity.

b) Přenos dat

Účelem fáze přenosu dat je umožnit přenos běžných uživatelských dat mezi dvěma SaS uživateli propojených bezpečným spojením.

Během fáze přenosu dat jsou použity následující procedury: ověření původu zprávy pro normální data, základní operace služby poskytované transportní vrstvou.

c) Ukončení spojení

Bezpečné spojení je ukončeno na požadavek SaS uživatele, zásahem poskytovatele transportní služby, nebo akcí ošetřující chybu v bezpečné vrstvě (Error management).

Autentizace fáze ukončení spojení není požadována.

d) Ošetření chyb

Chyba se může vyskytnout během navázání spojení, při autentizaci peer entity, během přenosu dat a při řízení bezpečného protokolu.

Všechny chyby musí být hlášeny místnímu SaS uživateli prostřednictvím Sa-REPORT.indication nebo pomocí Sa-DISCONNECT.indication.

Různé druhy chyb jsou ošetřeny různými strategiemi: ignorováním bezpečnostně relevantní události, ignorováním bezpečnostně relevantní události a signalizací chyby SaS uživateli pomocí Sa-REPORT.indication (volitelně), nebo ukončením bezpečného spojení, ukončením přenosového spojení a signalizace chyby SaS uživateli pomocí Sa-DISCONNECT.indication.

Je věcí SaS uživatele reagovat na indikovanou událost patřičným způsobem.

5.2.3 Časové posloupnosti

V této kapitole je popsán tok kontrolních informací a uživatelských dat.

5.2.3.1 Navázání spojení

Když Sa-CONNECT.request požaduje bezpečné spojení, bezpečná vrstva žádá navázání transportního spojení prostřednictvím T-CONNECT.request. Tato základní operace služby zahrnuje první zprávu procedury autentizace peer entity (AU1 SaPDU) jako uživatelská data.

Poznámka: AU1 a AU2 SaPDU jsou vyměněny prostřednictvím operace T-CONNECT.

Volaná peer entita transportní vrstvy indikuje požadavek navázání spojení na úrovni transportní vrstvy jeho bezpečné vrstvě pomocí základní operace služby T-CONNECT.indication. AU1 SaPDU je předána do bezpečné vrstvy v této základní operaci služby jako uživatelská data. Na konci prvního kroku volaná entita bezpečné vrstvy zkontroluje AU1 SaPDU.

Je-li akceptována, bezpečná entita reaguje na požadavek navázání transportního spojení základní operace T-CONNECT.response. To zahrnuje druhou zprávu protokolu autentizace peer entity AU2 SaPDU jako uživatelská data.

Při příjmu informuje volající transportní entita bezpečnou vrstvu o úspěšném navázání přenosového spojení použitím T-CONNECT.confirmation. AU2 SaPDU je předána bezpečné vrstvě jako uživatelská data v této základní operaci služby.

Bezpečná entita poté generuje zprávou AU3 SaPDU, která obsahuje třetí zprávu autentizačního protokolu (auth3), jako uživatelská data. Používá T-DATA.request k předání této zprávy transportní vrstvě.

Na příjmu, transportní entita užije T-DATA.indication k předání AU2 SaPDU bezpečné vrstvě jako uživatelská data. Bezpečná entita vyhodnotí AU2SaPDU.

V případě úspěšného vyhodnocení AU3 SaPDU, bezpečná entita předá Sa-CONNECT.indication bezpečnému uživateli (např. ATP aplikaci).

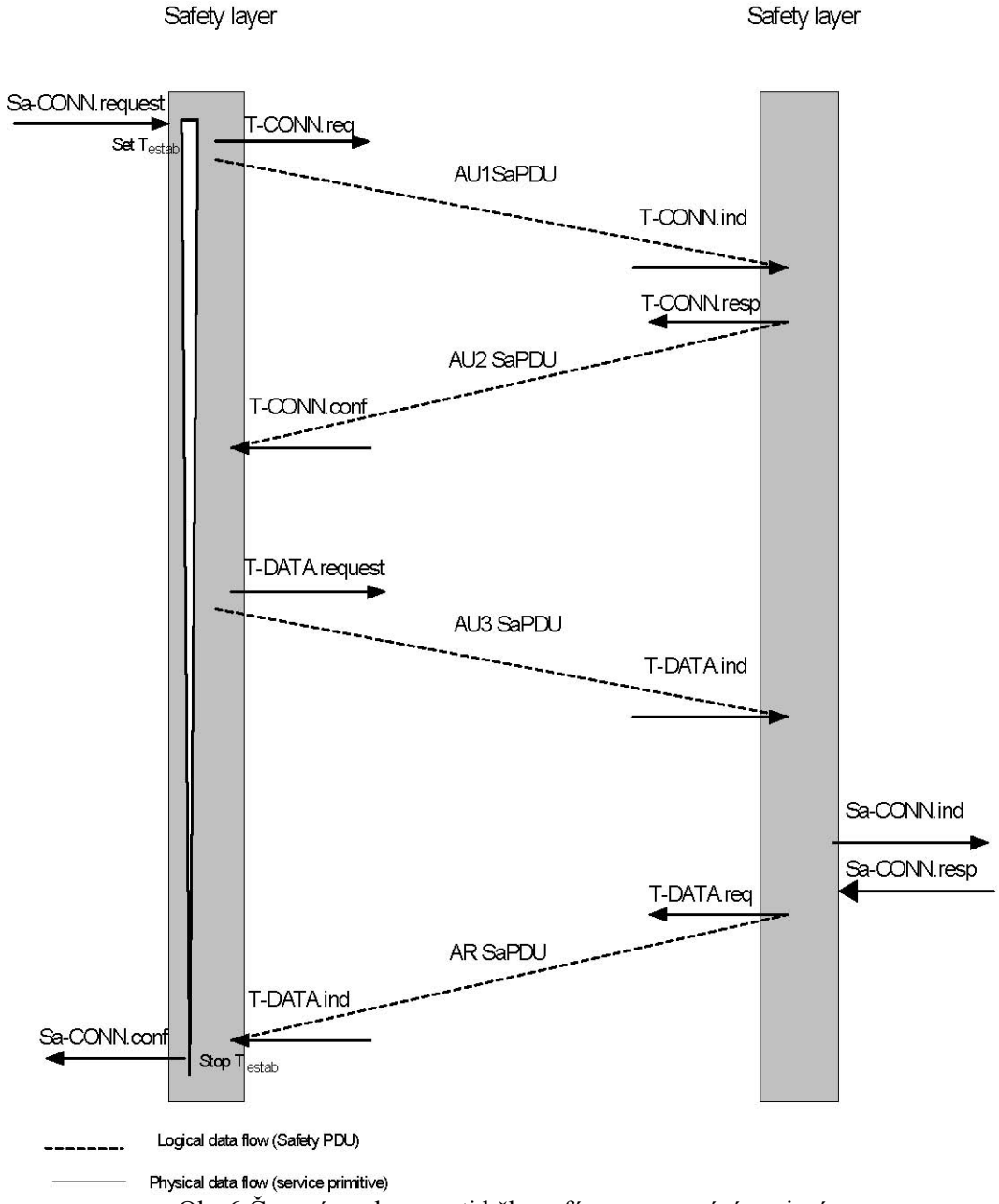
Akceptuje-li Sa uživatel požadavek na vytvoření bezpečného spojení, reaguje užitím základní operace služby Sa-CONNECT.response.

Bezpečná entita na volané straně předá zprávu AR SaPDU prostřednictvím T-DATA.request a T-DATA.indication základních operací služby jeho bezpečné peer entitě.

Poznámka: Zpráva AR SaPDU není vyžadována procedurou ověření peer entity. Přidáno kvůli poskytování potvrzení dle požadavků standardu OSI.

Po úspěšné vyhodnocení tohoto SaPDU obsahující autentizační data, bezpečná entita informuje SaS uživatele, že je úspěšně navázáno bezpečné spojení prostřednictvím základní operace služby Sa-CONNECT.confirmation.

Po přijetí Sa-CONNECT.confirmation, je volající SaS uživatel schopen posílat data peer uživateli bezpečným spojením. Volaný SaS uživatel je schopen žádat přenos dat okamžitě po Sa-CONNECT.response.



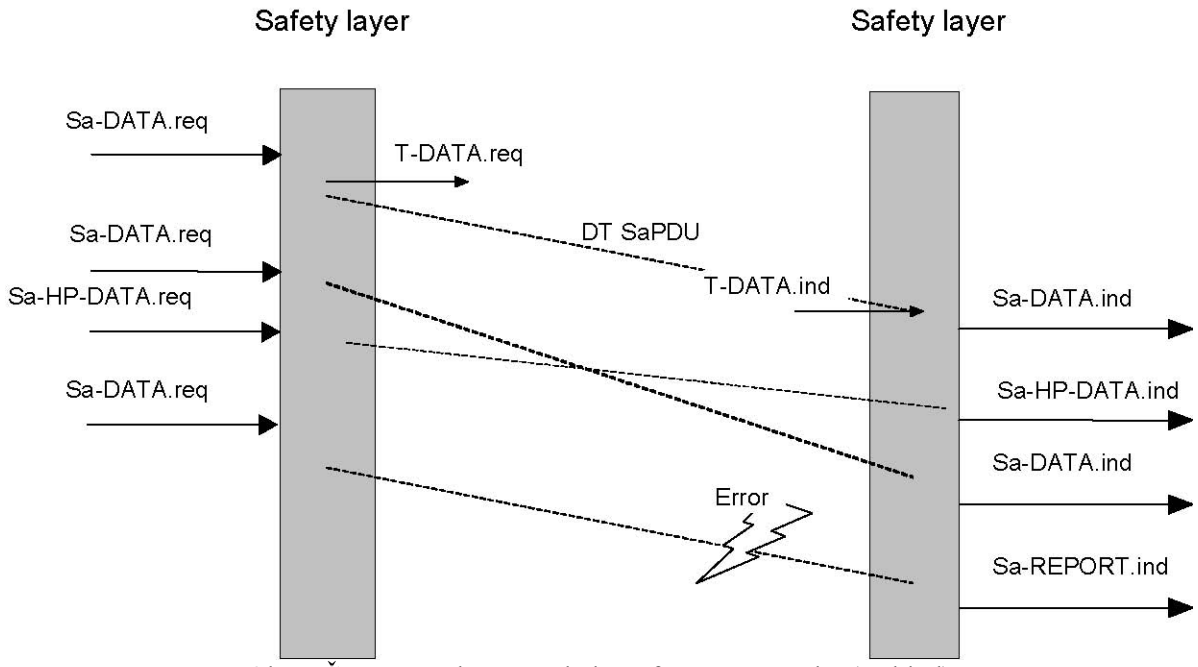
Obr.6 Časové posloupnosti během fáze navazování spojení

Časovač maximální prodlevy při navazování spojení je užívaný pro detekci nepřijatelného zpoždění během navazování spojení. Časovač T_{estab} je nastaven po přijetí Sa-CONNECT.request a je zastaven před generováním Sa-CONNECT.confirmation. V případě překročení času, je generováno Sa-DISCONNECT.indication zahrnující tuto příčinu. Všechny SaPDU budou ignorována, budou-li přijata po uplynutí tohoto času.

Entita bezpečné vrstvy RBC musí být schopna zacházet s více než jedním bezpečným spojením zároveň (dle konzultací je to 30 spojení zároveň). Palubní systém musí být schopen kontaktu s dvěma bezpečnými entitami zároveň kvůli hladkému přechodu mezi pokrytím sousedních RBC. Tuto vlastnost mohou také vyžadovat další situace.

5.2.3.2 Přenos dat

Na obr. 7 je ukázka, přenosu dat SFM. Uživatelská data z SaDATA.request jsou zahrnuta v uživatelských datech – části DT SaPDU. Pro přenos DT SaPDU se používá T-DATA.request a T-DATA.indication.



Obr.7 Časová posloupnost během fáze přenosu dat (příklad)

Přijímající entita bezpečné vrstvy zkontroluje formát SaPDU, řídící informace protokolu a zkontroluje MAC i integritu.

Uživatelská data bezpečného přenosu DT SaPDU jsou zahrnuta v Sa-DATA.indication.

Přenos dat s vysokou prioritou je podobný přenosu normálních dat.

V případě bezpečnostního problému s DT SaPDU, Sa-REPORT.indication, nebo Sa-DISCONNECT.indication tento problém signalizuje Sa uživateli.

5.2.3.3 Ukončení spojení

Ukončení spojení je vyžadováno prostřednictvím Sa-DISCONNECT.request. Bezpečná vrstva tak žádá transportní vrstvu o odpojení prostřednictvím T-DISCONNECT.request. DI SaPDU je zahrnuto v uživatelských datech T-DISCONNECT.request.

Peer entity jsou informovány o odpojení prostřednictvím T-DISCONNECT.indication a Sa-DISCONNECT.indication.

Autentizace fáze ukončení spojení není požadována.

V případě, že poskytovatel služeb nebo bezpečná vrstva začala fázi ukončení spojení, toto ukončení bude indikováno oběma SaS uživatelům prostřednictvím Sa-DISCONNECT.indication obsahující příslušný důvod.

Poznámka: V případě, že poskytovatel služeb způsobil ukončení spojení, SaPDU může být ztracený kvůli poškození či ztrátě TPDU.

5.2.4 Struktura a kódování SaPDU

5.2.4.1 Hlavní struktura SaPDU

Všechny SaPDU budou obsahovat celý počet oktetů. Oktety SaPDU jsou číslovány od 1 dále v pořadí ve kterém jsou vkládány do SaPDU. Bity v oktetu jsou číslovány od 8 do 1, kde 1. bit je nejnižšího řádu. Když SaPDU obsahuje více než jeden bajt, bit 8 prvního bajtu představuje nejvíce signifikantní bit pole SaPDU.

Jsou-li po sobě jdoucí bajty použity pro reprezentaci binárního čísla, bajt s nejnižším číslem má nejvýznamnější hodnotu.

Význam „RESERVED“: Vysílací strana musí vložit hodnotu 0.
Přijímací strana jej nebere v potaz.

SaPDU bude obsahovat elementy v následujícím pořadí:
Hlavičku sestávající z identifikátoru typu zprávy a příznaku směru.
Datové pole (je-li přítomno).
MAC pole (je li použité).

Struktura je ukázána v tab.8.

Tab.8 Struktura SaPDU

Typ hlavičky + Směr	**Data**	**MAC -** není použito pro AU1 a DI SaPDU
1 oktet	Proměnná délka	8 oktetů

Pole identifikátor typu zprávy:

Message type identifier (MTI) specifikuje typ SaPDU.

Tab.9 MTI SaPDU

Typ	Kód typu	Jméno
AU1 SaPDU	0001	První autentizační SaPDU (AU1)
AU2 SaPDU	0010	Druhá autentizační SaPDU (AU2)
AU3 SaPDU	0011	Třetí autentizační SaPDU (AU3)
AR SaPDU	1001	Odpověď na třetí autentizační SaPDU (AR)
DT SaPDU	0101	Datová SaPDU (DT)
DI SaPDU	1000	SaPDU ukončení spojení (DI)
Poznámka1: HP SaPDU neobsahují hlavičku. Poznámka2: Další SaPDU jsou definovány pro key management (viz: Key Management FIS).		

Pole příznaku směru – direction flag:

DF se používá k ochraně proti napadení odrazem (zrcadlením). Je inicializován během navazování spojení. Jeho hodnota je 0, když iniciátor spojení odesílá zprávu a 1, když odpovídající odesílá zprávu.

MTI a DF společně tvoří hlavičku.

Pole MAC jeho struktura i výpočet je rozebírán v odpovídající části.

5.2.4.2 PDU pro navázání spojení

AU1 a AU2 SaPDU jsou vyměněny prostřednictvím T-CONNECT.

První autentizační SaPDU sestává z polí specifikovaných tabulkou 10.

Tab.10 Struktura AU1 SaPDU

Oktet	Bit 8765 4321	Jméno pole	Pole
1	xxx. .... 001. .... 010. .... 011. .... 101. .... 110.	”ETY”	ETCS ID typ pole ”SA” RBC Pohon Reservováno pro balízu – není vyžadováno pro Class 1 Entita key managementu Entita zabezpečovacího systému (stavědla)
1	...0 001.	”MTI”	Identifikátor typu zprávy: AU1
1	0	”DF”	Příznak směru: ’0’ indikuje směr od volajícího k volanému
2 3 4	xxxx xxxx xxxx xxxx xxxx xxxx	”SA”	Volající ETCS ID
5	xxxx xxxx 0000 0001	”SaF”	Požadovaná bezpečná vlastnost Single DES s modifikovaným MAC algoritmem 3. Všechny ostatní hodnoty jsou rezervovány.
6 ... 13	xxxx xxxx ... xxxx xxxx	"R_B"	Náhodné číslo R_B

Druhá autentizační SaPDU sestává z polí specifikovaných tabulkou 11.

Tab.11 Struktura AU2 SaPDU

Oktet	Bit 8765 4321	Jméno pole	Pole
1	xxx.	”ETY”	ETCS ID typ pole ”SA”
	000. .... 001. .... 010. .... 011. .... 101. .... 110.		RIU RBC Pohon Reservováno pro balízu – není vyžadováno pro Class 1 Entita key managementu Entita zabezpečovacího systému (stavědla)
1	...0 010.	”MTI”	Identifikátor typu zprávy: AU2
1	1	”DF”	Příznak směru: ’1’ indikuje směr od volaného k volajícímu
2 3 4	xxxx xxxx xxxx xxxx xxxx xxxx	”SA”	Odpovídající ETCS ID.
5	xxxx xxxx 0000 0001	”SaF”	Požadovaná bezpečná vlastnost Single DES s modifikovaným MAC algoritmem 3. Všechny ostatní hodnoty jsou rezervovány.
6 ... 13	xxxx xxxx ... xxxx xxxx	"R_A"	Náhodné číslo R_A druhé autentizační zprávy
14 ... 21	xxxx xxxx ... xxxx xxxx		Pole MAC. MAC je spočítána dle pravidel daných peer entitou a procedurou ověření původu zprávy.

Třetí autentizační SaPDU sestává z polí specifikovaných tabulkou 12.

Tab.12 Struktura AU3 SaPDU

Oktet	Bit 8765 4321	Jméno pole	Pole
1	000.	”ETY”	Rezervováno
1	...0 011.	”MTI”	Identifikátor typu zprávy: AU3
1	0	”DF”	Příznak směru: ’0’ indikuje směr od volajícího k volanému
2 ... 9	xxxx xxxx ... xxxx xxxx		Pole MAC. MAC je spočítána dle pravidel daných peer entitou a procedurou ověření původu zprávy.

Autentizační odpověď AR SaPDU sestává z polí specifikovaných tabulkou 13.

Tab.13 Struktura AR SaPDU

Oktet	Bit 8765 4321	Jméno pole	Pole
1	000.	”ETY”	Rezervováno
1	...1 001.	”MTI”	Identifikátor typu zprávy: AR
1	1	”DF”	Příznak směru: ’1’ indikuje směr od volaného k volajícímu
2 ... 9	xxxx xxxx ... xxxx xxxx		Pole MAC. MAC je spočítána dle pravidel daných peer entitou a procedurou ověření původu zprávy.

5.2.4.3 SaPDU pro přenos dat

DATA SaPDU sestává z polí specifikovaných tabulkou 14.

Tab.14 Struktura DT SaPDU

Oktet	**Bit** 8765 4321	**Jméno pole**	**Pole**
1	000.		
1	...0 101.	”MTI”	Identifikátor typu zprávy: DT
1	x	”DF”	Příznak směru
2 ... 2+n-1	xxxx xxxx ... xxxx xxxx		Uživatelská data (délka n>=1 oktet): uživatelská data odpovídajícího SaPDU
2+n ... 2+n+7	xxxx xxxx ... xxxx xxxx		Pole MAC

5.2.4.4 SaPDU pro ukončení spojení

Disconnect SaPDU sestává z polí specifikovaných tabulkou 15.

Tab.15 Struktura DI SaPDU

Oktet	**Bit** 8765 4321	**Jméno pole**	**Pole**
1	000.		
1	...1 000.	”MTI”	Identifikátor typu zprávy: DI
1	x	”DF”	Příznak směru
2	xxxx xxxx		Reason: příčina ukončení spojení
3	xxxx xxxx		SUB-reason: detailnější specifikace příčiny

5.2.4.5 SaPDU pro vysoce prioritní data

HP SaPDU sestává z polí specifikovaných tabulkou 16.

Tab.16 Struktura HP SaPDU

Oktet	**Bit** 8765 4321	**Pole**
1 ... n	xxxx xxxx ... xxxx xxxx	Uživatelská data (délka n>=1 oktet): uživatelská data odpovídajícího SaPDU

5.2.5 Stavová tabulka:

Diagram přechodu stavů a stavová tabulka jsou shodné pro mobilní i stacionární část SFM.

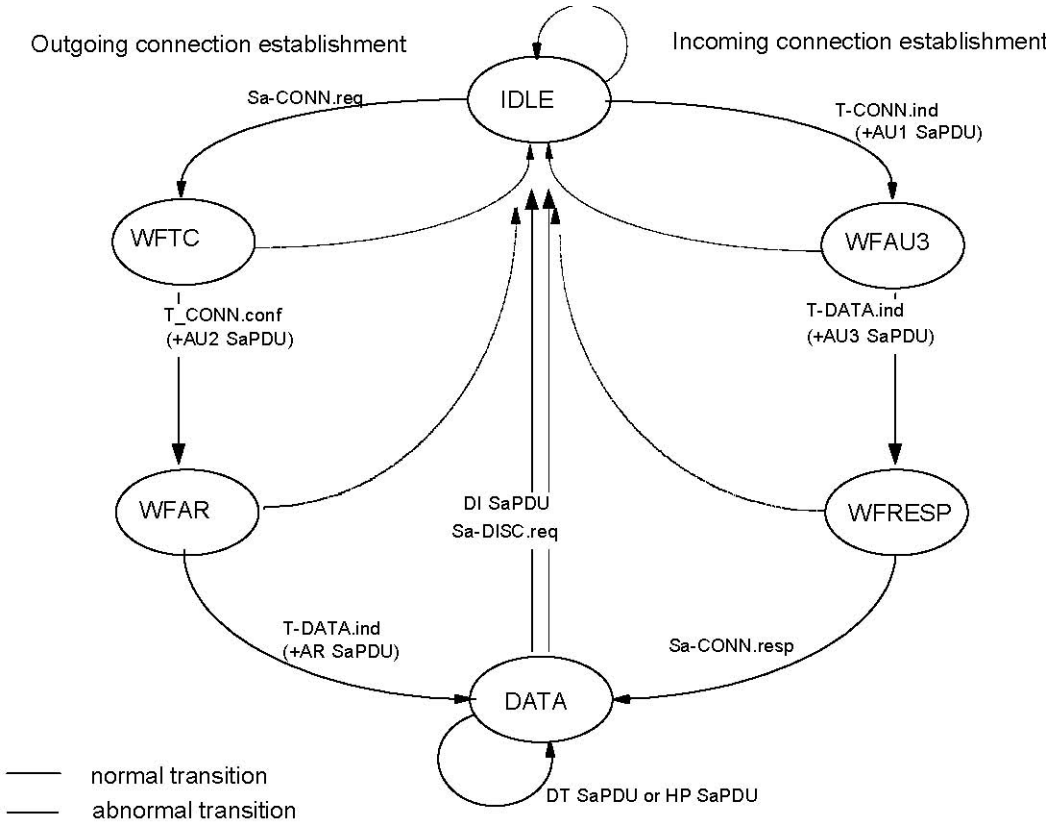
Tato sekce popisuje bezpečnostní protokol v rámci stavových tabulek. Stavové tabulky ukazují stav entity bezpečné vrstvy, události jež se vyskytují v protokolu, prováděné akce a následné stavy. Stavové tabulky jsou pouze koncepční a neukládají žádné omezení implementaci.

Stavové tabulky také definují mapování mezi bezpečnými základními operacemi služby a protokolovými událostmi, které může SaS uživatel očekávat.

Stavy jsou reprezentovány v tabulce jejich zkratkou. Tyto zkratky jsou definovány v tabulce 17.

Tab.17 Stavy

Zkratka stavu	Jméno stavu
WFTC	Čeká na spojení na úrovni transportní vrstvy
WFAR	Čeká na AR SaPDU
DATA	Bezpečné spojení je ustaveno a připraveno na přenos dat
WFAU3	Čeká na AU3 SaPDU
WFRESP	Čeká na Sa-CONNECT.response
IDLE	Bezpečné spojení je uzavřeno, nebo neexistuje



Obr.8 Přechodový diagram stavů entity bezpečné vrstvy

Průsečnice každého stavu a přicházející události, jež je neplatná, je zanechána ve stavové tabulce (tab.23) prázdná. Akce jež nastane v těchto případech bude jedna z následujících:

1) Pro případ související s bezpečnou službou (tj. přicházející od SaS uživatele), nepodnikne akci.

2) Pro případ související s přijetím SaPDU, následuje procedura pro ošetření chyb protokolu jestliže to umožňuje stav podporující spojení na úrovni transportní vrstvy.

3) Pro případ pádu do jiné než výše uvedené kategorie (včetně těch, jež jsou vyloučeny definicí chování bezpečné entity nebo SaS uživatele), nepodnikne akci.

V každém průsečíku stavu a události, která je platná, specifikuje akci která může zahrnovat jednu z následujících:

Jedna akce ze seznamu množství ochozích událostí (žádná, jedna, více) danou jejich zkratkou definovanou v tab. 19 následovanou určitými speciálními akcemi (tab. 21) a zkratkou výsledných stavů (tab. 17).

Podmíněné akce oddělené středníkem. Každá podmíněná akce obsahuje výrok následovaný dvojtečkou a akci jak je definováno v předchozím odstavci. Výroky jsou booleovské výrazy dané jejich zkratkou a definované tab. 20. Nastane jen akce odpovídající platnému výroku.

Existuje unikátní spojení mezi bezpečným spojením a spojením na úrovni transportní vrstvy. Mapování místních referencí (SaCEPID a TCEPID) je věcí implementace.

Tab. 18 specifikuje jména a zkratky příchozích událostí pocházející od TS poskytovatele, SaS uživatele, nebo entity bezpečné vrstvy.

Tab.18 Příchozí události

Zkratka	Původce události	Jméno
Sa-CONN.req	SaS-uživatel	Sa-CONNECT.request
Sa-CONN.resp	SaS-uživatel	Sa-CONNECT.response
Sa-DATA.req	SaS-uživatel	Sa-DATA.request
Sa-HP-Data.req	SaS-uživatel	Sa-HP-DATA.request
Sa-DISC.req	SaS-uživatel	Sa-DISCONNECT.request
T-DISC.ind	Poskytovatel TS	T-DISCONNECT.indication
T-CONN.ind (+AU1SaPDU)	Poskytovatel TS	T-CONNECT.indication
T-CONN.conf (+AU2SaPDU)	Poskytovatel TS	T-CONNECT.confirmation
AU3 SaPDU	Entita bezpečné vrstvy	Authentication 3 SaPDU
AR SaPDU	Entita bezpečné vrstvy	Authentication response SaPDU
DI SaPDU	Entita bezpečné vrstvy	Disconnect Request SaPDU
DT SaPDU	Entita bezpečné vrstvy	Data SaPDU
HP SaPDU	Entita bezpečné vrstvy	High priority data SaPDU
Časovač Testab	Entita bezpečné vrstvy	Časovač navázání spojení

Tab. 19 specifikuje jména a zkratky ochozích událostí pocházející od SaS poskytovatele, TS uživatele, či entity bezpečné vrstvy.

Tab.19 Odchozí události

Zkratka	Původce události	Jméno
Sa-CONN.ind	Poskytovatel SaS	Sa-CONNECT.indication
Sa-CONN.conf	Poskytovatel SaS	Sa-CONNECT.confirmation
Sa-DATA.ind	Poskytovatel SaS	Sa-DATA.indication
Sa-HP-DATA.ind	Poskytovatel SaS	Sa-HP-DATA.indication
Sa-DISC.ind	Poskytovatel SaS	Sa-DISCONNECT.indication
Sa-REPORT.ind	Poskytovatel SaS	Sa-REPORT.indication
T-CONN.req (+AU1SaPDU)	TS-uživatel	T-CONNECT.request
T-CONN.resp (+AU2SaPDU)	TS-uživatel	T-CONNECT.response
T-DISC.req	TS-uživatel	T-DISCONNECT.request
AU3 SaPDU	Entita bezpečné vrstvy	Authentication 3 SaPDU
AR SaPDU	Entita bezpečné vrstvy	Authentication response SaPDU
DI SaPDU	Entita bezpečné vrstvy	Disconnect Request SaPDU
DT SaPDU	Entita bezpečné vrstvy	Data SaPDU
HP SaPDU	Entita bezpečné vrstvy	High Priority data SaPDU

Tab. 20 obsahuje výše zmíněné výroky.

Tab.20 Výroky

Jméno	Popis
Pre0	Sa-CONNECT. request neakceptovatelný • je vyžadován nejméně jeden následující parametr: typ aplikace • chyba typu aplikace
Pre1	Neakceptovatelný T-CONNECT.indication, • je vyžadován nejméně jeden následující parametr: typ aplikace, uživatelská data • chyba typu aplikace Neakceptovatelný AU1 SaPDU • chyba formátu AU1 SaPDU • chyba ETY,MTI,DF či SaF • není k dispozici KMAC
Pre2	Neakceptovatelný T-CONNECT.confirmation, • je vyžadován nejméně jeden následující parametr: uživatelská data Neakceptovatelný AU2 SaPDU • chyba formátu AU2 SaPDU • chyba ETY,MTI,DF či SaF • není k dispozici KMAC • chyba MAC

Jméno	Popis
Pre3	Neakceptovatelný AU3 SaPDU • chyba formátu AU3 SaPDU • Chyba ETY, MTI nebo DF • chyba MAC
Pre4	Neakceptovatelný AR SaPDU • chyba formátu AR SaPDU • chyba ETY, MTI či DF • chyba MAC
Pre 5	Chybný SaPDU • chyba MAC v DT SaPDU
Pre6	Neakceptovatelný DT SaPDU • chyba délky DT SaPDU • chyba MTI • chyba DF (ne chyba MAC)

Tab.21 Definice časovače

Symbol	Jméno	Definice
T_{estab}	Čas navázání spojení	Horní hranice času po kterém místní bezpečná entita inicializuje proceduru řízení chyb. Když nepřijme odpověď na autentizační zprávu.

Tab.22 Akce integrity

Zkratka	Akce
a5	Spuštění časovače T_{estab}
a6	Zastavení časovače T_{estab}
a19	Zastavení všech časovačů; reset všech počítadel.

Tab.23 Tabulka stavů

Stav / Událost	IDLE	WFTC	WFAR	DATA	WFAU3	WFRESP
Sa-CONN.req	Pre0: Sa-DISC.ind, IDLE; not Pre0: T-CONN.req (AU1 SaPDU), a5, WFTC					
Sa-CONN.resp						AR SaPDU, DATA
Sa-DATA.req				DT SaPDU, DATA		
Sa-HP-DATA.req				HP SaPDU, DATA		

Stav / Událost	IDLE	WFTC	WFAR	DATA	WFAU3	WFRESP
Sa-DISC.req		T-DISC.req a19, IDLE Pozn.1	T-DISC.req (+DI SaPDU),a19, IDLE	T-DISC.req (+DI SaPDU), a19, IDLE		T-DISC.req (+DI SaPDU) a19, IDLE
T-CONN.ind (+AU1SaPDU)	Pre1:T-DISC.req (+DI SaPDU), IDLE; not Pre1: T-CONN.resp (+AU2 SaPDU) WFAU3					
T-CONN.conf (+AU2SaPDU)		Pre2: Sa-DISC.ind, T-DISC.req, a19, IDLE Pozn.1 not Pre2: AU3 SaPDU, WFAR				
T-DISC.ind nebo T-DISC.ind (+DI SaPDU)		Sa-DISC.ind, a19, IDLE	Sa-DISC.ind, a19, IDLE	Sa-DISC.ind a19, IDLE	a19, IDLE	Sa-DISC.inda19, IDLE
AU3 SaPDU					Pre3: T-DISC.req (+DI SaPDU), a19, IDLE not Pre3: Sa-CONN.ind, WFRESP	
AR SaPDU			not Pre4: Sa-CONN.conf, a6, DATA; Pre4: Sa-DISC.ind, T-DISC.req (+DI SaPDU), a19, IDLE			
DT SaPDU				not Pre5 and not Pre6: Sa-DATA.ind, DATA; Pre5: Sa-REPORT.ind, DATA Pozn.3 Pre6: Sa-DISC.ind, T-DISC.req (+DI SaPDU), a19, IDLE		

Stav / Událost	IDLE	WFTC	WFAR	DATA	WFAU3	WFRESP
HP SaPDU				Sa-HP-DATA.ind, DATA Pozn.2		
Překročení času Testab		Sa-DISC.ind, T-DISC.req, a19, IDLE Pozn.1	Sa-DISC.ind, T-DISC.req (+DI SaPDU), a19, IDLE			
Poznámky: 1. Není zahrnuto DI SaPDU 2. HP SaPDU obcházejí bezpečné procedury 3. Volitelně je Sa-REPORT.indication doručeno SaS uživateli (jestliže je podporováno)						

5.3 Management bezpečného protokolu

5.3.1 Funkce managementu bezpečného protokolu

Management bezpečného protokolu definuje konfigurační management potřebný k práci s parametry bezpečného protokolu, a jeho dohled i diagnostiku. Hlavní důraz je kladen na dosažení technické interoperability mezi mobilní a stacionární jednotkou s ohledem na management bezpečného protokolu.

Všechny detaily, které jsou závislé na implementaci (jako: generování, uchovávání a rušení klíčů, nebo záznam chyb), nejsou popsány v SUBSETu 037.

Aktualizace klíčů radiovou (online key management) cestou apod. jsou možné použitím managementu SaPDU. Použití řízení SaPDU je volitelné.

Řízení vrstvy bezpečného protokolu je zahrnuto v podsystému SFM. Část je zřejmě bezpečnostně relevantní a musí být ošetřena bezpečným způsobem, zatímco některé části nejsou. Tyto detaily jsou závislé na implementaci a nejsou v SUBSETu 037 uvedeny.

5.3.2 Management konfigurace

Management konfigurace definuje parametry potřebné pro funkci bezpečného protokolu a jeho řízení, a funkce k jeho řízení.

5.3.2.1 Parametry adres

Pro adresování používá bezpečný protokol ETCS Identity. ETCS Identity jsou unikátní v rozsahu příslušného ETCS typu. ETCS ID společně s typem aplikace identifikuje uživatele bezpečné služby.

Tab.24 ETCS Identity (viz Unisig SRS – SUBSET 026 kapitola 7)

ETCS ID	Rozsah hodnot **Oktet1 Oktet2 Oktet3** **8765 4321 8765 4321 8765 4321**	Popis
ETCS ID palubní jednotky	tttt tttt tttt tttt tttt tttt	
ETCS ID RBC	cccc cccc ccrr rrrr rrrr rrrr 11 1111 1111 1111	c…c ID regionu či země r…r ID RBC neznámé ETCS ID

ETCS ID	Rozsah hodnot **Oktet1 Oktet2 Oktet3** **8765 4321 8765 4321 8765 4321**	Popis
ETCS ID RIU (ETCS level1)	cccc cccc ccrr rrrr rrrr rrrr 11 1111 1111 1111	c…c ID regionu či země r…r ID RIU neznámé ETCS ID
ETCS ID entity KM	cccc cccc cckk kkkk kkkk kkkk	c…c ID regionu či země k…k ID entity Key manag.

Poznámka: Definice struktury a hodnot ETCS ID je mimo rozsah této práce.

Identity jsou použity během navazování spojení pro výpočet odpovídajících bezpečných vazeb, tzn. ETCS ID jsou relevantní pro výkon bezpečné procedury „autentizace peer entity“.

Bezpečné spojení mezi dvěma ETCS identitami je možné, jakmile sdílejí autentizační klíč (K_{ab}) k navázání spojení. Mimo autentizačního klíče, musejí být pro každé bezpečné spojení definovány také další parametry.

Volitelně jsou přístupové body přenosové služby (TSAP) použity bezpečnou vrstvou ke zpřístupnění přenosové (transportní) vrstvy.

5.3.2.2 Parametr časovač

Parametr maximálního zpoždění při navazování spojení je použit pro detekci nepřijatelného zpoždění během navazování spojení.

Tab.25 Parametr časovač bezpečné vrstvy

Parametr	Symbol	Použitá hodnota	Komentář
Maximální zpoždění při navazování spojení	T_{estab}	40 s	Závisí na komunikační síti

5.3.3 Dohled a diagnostika

Dohled a diagnostika popisuje řízení chyb bezpečné vrstvy, monitorování a kontrolu bezpečnostně relevantních událostí.

Chybový management definuje řízení chyb a hlášení o chybách aplikační vrstvě, je-li to potřebné z důvodu interoperability.

Poznámka: Záznam chyb SFM jednotkou není pro Class 1 vyžadován. Je-li potřebný, musí být ošetřen aplikací.

5.3.3.1 Hlášení chyb

Všechny bezpečnostně relevantní chyby, jež se vyskytnou v bezpečné vrstvě musí být neprodleně hlášeny aplikaci, okamžitě po jejich výskytu. Chyby ošetřeny vnitřně, managementem bezpečné vrstvy, mohou být hlášeny aplikaci, ale nemusí. Existují dvě možnosti informování o chybách (směrem k aplikaci):

1) Vede-li chyba k povinnému ukončení spojení, může být hlášena aplikaci použitím Sa-DISCONNECT.indication. Aplikace je informována o druhu chyby prostřednictvím parametru disconnect reason.

2) Je-li chyba ošetřena pouze vnitřně managementem bezpečné vrstvy, nebo nevede-li k povinnému ukončení spojení, může být volitelně hlášeno aplikaci použitím Sa-REPORT.indication. Aplikace je informována o typu chyby parametry reason code a sub-reason code.

5.3.3.2 Ošetření chyb

Vyskytne-li se chyba v bezpečné vrstvě, chybový management musí, v závislosti na parametrech reason a sub-reason, podniknout následující kroky. Reason code a sub-reason code jsou použity v Sa-DISCONNECT.indication a Sa-REPORT.indication k signalizování typu chyby uživateli služby.

Akce ošetření chyby vyvolá odeslání T-DISCONNECT.request (+DI SaPDU), je-li vyžadován dle stavové tabulky.

Požadavek Class1: Když je chybová informace přenesena k aplikaci parametrem Sa-DISCONNECT.indication, jsou další akce zodpovědností aplikace.

Indikace chyby poskytnutá T-CONNECT.indication bude zpracována bezpečnou vrstvou:

Když: reason = přijata chyba sítě, tato chyba je předána aplikaci
reason = volaný TS uživatel není dostupný, nemůže být přijatý komunikační vrstvou, jako ATP aplikace předpokládá na základě podpory peer entity. Nicméně, když je přijat bezpečnou vrstvou tento reason, bude informována aplikace.

Tab.26 Normální ukončení bezpečného spojení

Reason Code	Sub-reason Code	Popis	Akce zacházení s chybami
0		Normální ukončení požadované SFM uživatelem	Sa-DISCONNECT.indication

Tab.27 Sub-reason-y náležící k: 'žádné přenosové služby k dispozici'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
1	1	Síťová chyba	Sa-DISCONNECT.indication Aplikace se může pokusit opětovně navázat spojení
1	2	Síťové zdroje nejsou dostupné	Sa-DISCONNECT.indication Aplikace se může pokusit opětovně navázat spojení a nižším parametrem QoS
1	3	Služba nebo volba není momentálně k dispozici	Sa-DISCONNECT.indication Aplikace se může pokusit opětovně navázat spojení s modifikovaným parametrem
1	5	Důvod neznámý	Sa-DISCONNECT.indication

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
1	6	Volaný TS uživatel není k dispozici	Sa-DISCONNECT.indication Aplikace se může pokusit opětovně navázat spojení krátkým volacím kódem
1	8	Neregistrována žádná mobilní stanice	Sa-DISCONNECT.indication Aplikace se může pokusit o opětovnou registraci do sítě
Poznámka: 1.Sub-reason je stejný s reason T-DISCONNECT.indication. 2. Sub-reason-y jsou věcí implementace. Chybové kódy nejsou přenášena vzdušnou cestou.			

Tab.28 Sub-reason-y náležící k: 'chybějící parametr či neplatná hodnota parametru'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
3	2	Chybějící autentizační klíč	Sa-DISCONNECT.indication
3	3	Jiný problém key managementu (např. ztráta session klíče)	Sa-DISCONNECT.indication. SFM uživatel může navázat nové spojení.
3	29	Požadovaná bezpečná vlastnost není podporována	Sa-DISCONNECT.indication

Tab.29 Sub-reason-y náležící k: 'neplatný MAC'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
4	1	Chyba MAC	Sa-REPORT.indication
4	2	Chyba MAC v AU2 SaPDU.	Sa-DISCONNECT.indication
4	3	Chyba MAC v AU3 SaPDU	T-DISCONNECT.request.
4	4	Chyba MAC v AR SaPDU	Sa-DISCONNECT.indication

Tab.30 Sub-reason-y náležící k: 'selhání sekvence integrity'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
5	1	Opakování autentizační zprávy (AU1 SaPDU, AU2 SaPDU, AU3 SaPDU, AR SaPDU) po navázání spojení. Tento kód chyby je použit v případě, že chyba není pokryta reason kódem 9.	Sa-DISCONNECT.indication

Typ chyby: Selhání v DF – příznaku směru

Tato kontrola je vyvolána po prověření MAC (ne v případě AU1 či DI SaPDU). Vyskytne-li se chyba jež ovlivní DF, MAC to jistí a reakce bude odpovídat tab. 29. Je-li MAC korektní, ale DF je nekorektní, uplatní se Sa-DISCONNECT.indication.

Tab.31 Sub-reasons náležící k: 'chyba DF'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
6	1	Hodnota direction flagu '0' namísto '1'	Sa-DISCONNECT.indication Aplikace předpokládá požadavek na navázání nového spojení.
6	2	Hodnota direction flagu '1' namísto '0'	Sa-DISCONNECT.indication (po předchozím Sa-CONNECT.indication) Aplikace předpokládá požadavek na navázání nového spojení.

Tab.32 Sub-reasons náležící k: ‘vyčerpán čas pro navázání spojení’

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
7	3	Vypršel čas T_{estab} aniž by byl přijat AR SaPDU	Sa-DISCONNECT.indication Aplikace se může pokusit opětovně navázat spojení

Tab.33 Sub-reasons náležící k: 'neplatné pole SaPDU'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
8	1	Neplatné pole informací	Odmítnutí SaPDU
8	4	Neplatné odpovídající ETCS ID v AU2, tj. ETCS-Identita neodpovídá přijatelnému ETCS ID.[4]	Sa-DISCONNECT.indication
8	5	Neplatné AU1 SaPDU: hlavička indikuje AU1 SaPDU, ale zbytek SaPDU neodpovídá struktuře AU1 SaPDU.	Odmítnutí SaPDU

[4] existuje-li požadavek na připojení k neznámé RBC, každá možná RBC může být očekávána

Tab.34 Sub-reasons náležící k: 'chyba v sekvenci SaPDU během navazování spojení'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
9	1	Odeslání AU1 SaPDU, ale obdržena jiná zpráva než AU2 SaPDU.	Sa-DISCONNECT.indication
9	2	Odeslání AU2 SaPDU, ale obdržena jiná zpráva než AU3 SaPDU.	T-DISCONNECT.request
9	3	Odeslání AU3 SaPDU, ale obdržena jiná zpráva než AR SAPDU.	Sa-DISCONNECT.indication

Tab.35 Sub-reasons náležící k: 'chybná délka SaPDU'

Reason Code	Sub-reason Code	Popis	Akce ošetřující chybu
10	1	Chybná délka AU1 SaPDU	Odmítnutí AU1 SaPDU
10	2	Chybná délka AU2 SaPDU	Sa-DISCONNECT.indication
10	3	Chybná délka AU3 SaPDU	T-DISCONNECT.request
10	5	Chybná délka DT SaPDU	Sa-DISCONNECT.indication
10	8	Chybná délka AR SaPDU	Sa-DISCONNECT.indication

Kód 127 (neznámý) může být použit, když:

nemůže být vybrán žádný reason ani sub-reason kód
reason či sub-reason kód není definován

Kódy 11-126 jsou vyhrazeny pro budoucí využití. Kódy 128-255 jsou rezervovány pro národní/individuální použití. Pro tyto reason kódy jsou sub-reason kódy (0…126,128…255) také rezervovány pro národní/individuální použití.

6 OMEZENÍ, JEŽ BUDOU POSKYTNUTA ATP APLIKACI

Tato část definuje podmínky a omezení, která budou pokryta ATP aplikací, při použití služeb poskytovaných SFM.

Je-li požadována ochrana proti zpoždění zprávy, špatné posloupnosti zpráv, vymazání zprávy a opakování zprávy, bude poskytnuta aplikací.

Musí být definována a poskytována procedura pro potvrzení příjmu a opakované zaslání HP dat. Délka uživatelských dat je omezena na maximálně 25 bajtů.

Jestliže je požadováno, mělo by být poskytnuto bezpečné sledování spojení.

Základní operace služby mají být vydané podle definovaných sekvencí.

V případě změny oblasti RBC, nebo vstup do prostoru RBC, musí být požadován požadavek na navázání spojení co nejdříve jak je možné. Běžně je doba navazování bezpečného spojení menší než hodnota T_{estab} = 40s.

V případě přihlašování do mobilní sítě (roaming do další GSM-R PLMN), musí být akceptováno dodatečné zpoždění (viz. SUBSET 093 sekce 6.3.7).

Maximální délka aplikační zprávy, určené k přenosu, je omezena na 1023 bajtů.

Je-li na jednom fyzickém spojení multiplexována více než jedna ATP aplikace (volitelně), přijímaná HP data jsou přenesena všem ATP aplikacím.

Je-li požadováno, musí být dokončen přenos aplikačních dat (pro oba směry) před ukončením spojení.

V případě ukončení bezpečného spojení způsobeným sítí, nebo odmítnutí požadavku na navázání spojení, aplikace musí žádat opětovné navázání bezpečného spojení. Palubní ATP iniciuje opětovné navázání bezpečného spojení. Kvůli možné ztrátě uživatelských dat může být požadována opětovná synchronizace aplikačních dat.

V případě potřeby musí aplikace “vycpat” uživatelská data na potřebnou velikost (celé bajt(y)).

Aplikace by měla kontrolovat, jestli je volaný ETCS ID základní operace Sa-CONNECT.indication shodný jako jeho vlastní ETCS ID.

Aplikace OBU musí poskytovat ID mobilní sítě pro žádost o bezpečné spojení.

7 POROVNÁNÍ PROTOKOLU EURORADIO S NORMOU EN50159-2

7.1 Popis normy EN50159-2

Norma EN50159-2 se zabývá sdělovacími a zabezpečovacími systémy, a systémy pro zpracován dat, které využívají služby otevřených přenosových sítí. Tato norma se zaměřuje na popis požadavků, které je nutno uvažovat při bezpečném přenosu informací otevřeným přenosovým systémem. EN50159-2 byla 1. 1. 2000 přijata skupinou CENELEC (Evropský výbor pro normalizaci v elektronice), takže ji každý člen tohoto sdružení musí považovat za svoji národní normu.

Tato norma říká, že používá-li bezpečnostně relevantní elektronický systém výměnu dat mezi dvěma, či více místy, je sdělovací systém, zajišťující tuto výměnu dat, nedílnou součástí systému a je bezpodmínečně nutné prokázat jeho bezpečnost v souladu s ENV 50129 (tehdy předběžná verze normy „Drážní zařízení - Zabezpečovací elektronické systémy“).

Otevřený přenosový systém je z hlediska bezpečnosti považovaný za černou skříňku, to znamená že jeho vlastnosti jsou neznámé (potencionálně jakékoli). Otevřený přenosový systém může obsahovat jakékoli z následujících součástí:

prvky zacházející s daty (pracující pro uživatele neznámým způsobem)
neznámý počet uživatelů
zařízení, jež mohou být připojena k jakýmkoli jiným přenosovým systémům
přenosová média s neznámými vlastnostmi
směrovací prvky (pracující pro uživatele neznámým způsobem)

Otevřený přenosový systém může být vystaven vlivům:

jiných (neznámých) uživatelů vyměňujících si neznámá data
uživatele, který se pokouší chovat se nestandardním způsobem
jakémukoli jinému vlivu majícímu vliv na integritu bezpečnosti

Z těchto vlastností vyplývá, že na takovýto systém nemůže být kladen žádný bezpečnostní požadavek. Bezpečnost se zajistí pomocí dodržování bezpečných postupů při práci s daty.

Norma EN50159-2 nespecifikuje otevřený přenosový systém, zařízení k němu připojená, rušení (EMC …) ani jaký typ dat se vztahuje k bezpečnosti a který nikoli.

7.2 Možná (uvažovaná) ohrožení přenosového systému

Norma ENV 169-2 definuje nejpodstatnější příčinu nebezpečí, jako přijetí neautentické zprávy (v nejhorším případě ještě považování ji za autentickou).

Základní druhy možných ohrožení v otevřených přenosových systémech:

opakování zprávy
vymazání zprávy
přeřazení zprávy
vložení zprávy
poškození zprávy
zpoždění zprávy
maskování uživatele.

Tyto potenciální možnosti vzniku nebezpečí lze eliminovat zajištěním následujících služeb: integrita, autenticita, včasnost a správnost řazení zpráv.

7.3 Možné druhy obran

Byly vyvinuty metody, které zajišťují ochranu proti výše zmíněným ohrožením. Seznam těchto metod není definitivní a mohou být vyvinuty a použity nové metody (s prokázanou bezpečností).

Metody možných obran proti potenciálním nebezpečím:
- pořadové číslo
- časový údaj
- časová prodleva
- ID zdroje a místa určení
- zpětné zprávy
- postup identifikace
- bezpečnostní kód
- kryptografické metody

7.3.1 Pořadové číslo:

Tato obrana spočívá v přiřazení pořadového čísla ke každé zprávě. Toto opatření umožní kontrolovat správný sled zpráv. Tento typ ochrany sebou nese i několik komplikací, které je nutno ošetřit: rozsah čísla, inicializace čísla (při spuštění i po přerušení sledu zpráv). Tato ochrana není použita v popisech zabezpečení komunikace Euroradio.

7.3.2 Časový údaj:

Tato ochrana se používá, je-li informace doručovaná cílové entitě vztažena k času. V určitých případech je tato souvislost přímo spjata s bezpečností, protože zpráva doručená se zpožděním může způsobit nebezpečný stav

Existuje několik variant provedení této ochrany, jako časová prodleva. V tomto případě přijímač kontroluje časové zpoždění mezi určitými událostmi vázanými na příchod či odesílání zpráv. Je-li tento čas překročen je toto považováno za chybu a musí být provedeny potřebné kroky. Tuto volbu lze kombinovat se zpětnou zprávou a měřit čas pouze ve vysílači. Tento typ odměřování času je použit při navazování bezpečného spojení (parametr Testab.).

7.3.3 Identifikátory zdroje a místa určení zprávy:

Takovýto identifikátor je nutný v případě skupinového připojení (připojení více komunikačních jednotek k přenosovému systému) kvůli rozlišení jednotlivých uživatelů. Je možno připojit jako přídavná data ID zdroje, ID cíle, nebo oba parametry.

S tímto opatřením je také spojeno několik úskalí, které je nutno vzít v potaz. Je nutno zaručit jednoznačnost takového identifikátoru v rozsahu celého komunikačního systému (s tím souvisí také potřebná velikost takovéhoto identifikátoru respektive počet možných různých identifikátorů). Tento problém je v ETCS řešen kombinací tří parametrů: typ ETCS ID, ETCS ID a typu aplikace.

Tato obrana je použita při navazování bezpečného spojení i při přenosu dat.(MAC + transport selektor).

7.3.4 Zpětná zpráva:

Je-li přenosový systém schopen přenosu dat oběma směry lze realizovat takovouto obranu v jednom z následujících provedení:

- zaslat zpět zprávu obsahující data odvozená z předchozí zprávy (nebo přímo nezměněná data)
- zaslat zpět zprávu obsahující data odvozená z vlastního procesu
- zaslat zpět zprávu obsahující data pro účely bezpečnosti

Potvrzení může být jak kladné (potvrzení včasnosti doručení) tak záporné (nedoručení zprávy v daném čase, nebo doručení chybné zprávy. Takovéto provedení obrany může přispět k synchronizaci hodin obou komunikujících partnerů, usnadnění dynamických kontrolních procesů atd.. Na zpětný kanál je nutno, z bezpečnostního hlediska, pohlížet stejným způsobem jako na přímý kanál. To znamená, že zpětná zpráva musí být zabezpečena jako jakákoli jiná bezpečnostně relevantní zpráva.

Tento typ ochrany je použit při navazování bezpečného spojení (sled několika zpráv oběma směry tzv. postup identifikace). V případě přenosu HP dat je nutno zajistit potvrzení příjmu aplikací. V případě přenosu běžných uživatelských dat je možnost nedoručení ošetřena časovým a/nebo místním omezením oprávnění k provádění kritických úkonů (např. MA). Norma Euroradio neuvažuje zpětné zprávy při přenosu dat (nechává je jako možnost implementace).

7.3.5 Postup identifikace:

Tato ochrana slouží k zabránění možnosti přijímat data z neautorizovaného zdroje, která se tváří jako autorizovaná (druh maskování). Postup identifikace je možné rozdělit na dvě skupiny: obousměrná identifikace, nebo dynamický postup identifikace.

Při navazování bezpečného spojení je požit dynamický postup identifikace prostřednictvím sledu několika zpráv (AU1, AU2, AU3 a AR SaPDU) během nichž se ustanoví klíč pro dané spojení.

7.3.6 Bezpečnostní kód:

Bezpečnostní kódy se používají v přenosových systémech pro poskytnutí ochrany při výskytu chyb (náhodných i shlukových). Bezpečnostní kódy mohou chybu detekovat, nebo dokonce opravit. Tyto kódy aplikuje většinou i přenosový systém, ale na jeho kroky nelze, s ohledem na bezpečnost, spoléhat. Z toho plyne že bezpečnostní kód je nutno použít i v bezpečnostně relevantní části. V zabezpečovací technice se používá kódů pro detekci chyb, nikoli pro opravu.

U takovýchto kódů je nutno ověřit jejich schopnost odhalit chyby různých očekávaných typů a pravděpodobnost detekce chyby.

Tento typ zabezpečení norma EURORADIO využívá prostřednictvím MAC.

7.3.7 Kryptografické techniky:

Takovéto techniky mohou přispět bezpečnosti v sítích, jde je možno očekávat škodlivé útoky (veřejná síť, rádiové spojení, nebo přenosový systém připojený k veřejné síti). Kryptografické metody používají jako vstup klíč a data a prostřednictvím algoritmu vypočtou kód. Míra ochrany závisí na utajení klíčů a na síle algoritmu. Zacházení s klíči obstarává tzv. key management, který není náplní této práce.

Takovýto mechanismus nemůže nikdy chránit data takovým způsobem, aby jej nebylo možno prolomit neoprávněným uživatelem. Je proto nutné zvážit úroveň nebezpečí takovéhoto útoku, tj. motivaci či finanční a technické prostředky, které může mít k dispozici potencionální neoprávněný uživatel. Je také nutno brát v úvahu rychlý vývoj IT odvětví a uvažovat možnosti takového napadení v budoucnu. Proto jsou tyto techniky nastaveny tak, aby je nebylo možno se současným vybavením v potřebné době odhalit (odhalit jak klíč tak algoritmus).

8 POPIS FUNKČNÍHO CHOVÁNÍ

8.1 Rozsah systému

Následující případy užití se zabývají částí EVC, která provádí bezpečnostní funkce. Tyto funkce mají za účel zajistit navázání a udržení bezpečného spojení, zabezpečit příslušnými atributy zprávy při odesílání a kontrolovat bezpečnostní prvky zprávy při příjmu. Tato část EVC se podle normy (ERTMS/ETCS – Class 1 – subset 037) nazývá SFM (Safe Functional Module). SFM radiokomunikačního systému poskytuje funkce bezpečného přenosového systému. Z důvodů přehlednosti bude nadále tato část nazývána jako systém. Bezpečná aplikace (bezpečné aplikace), Error management a CFM (Communication Functinal Module) jsou pro náš případ primárními aktéry. Bezpečná aplikace iniciuje případy užití při odesílání zpráv či při navazování/ukončování spojení. Error management iniciuje volané případy užití týkající se indikace chyby či ukončení spojení z bezpečnostních důvodů. CFM iniciuje případy užití při příjmu zpráv.

8.2 Rozhraní

Bezpečná aplikace – Systém (SaSAP)

Systém – Error management

Systém – Key management

Systém – CFM (TSAP)

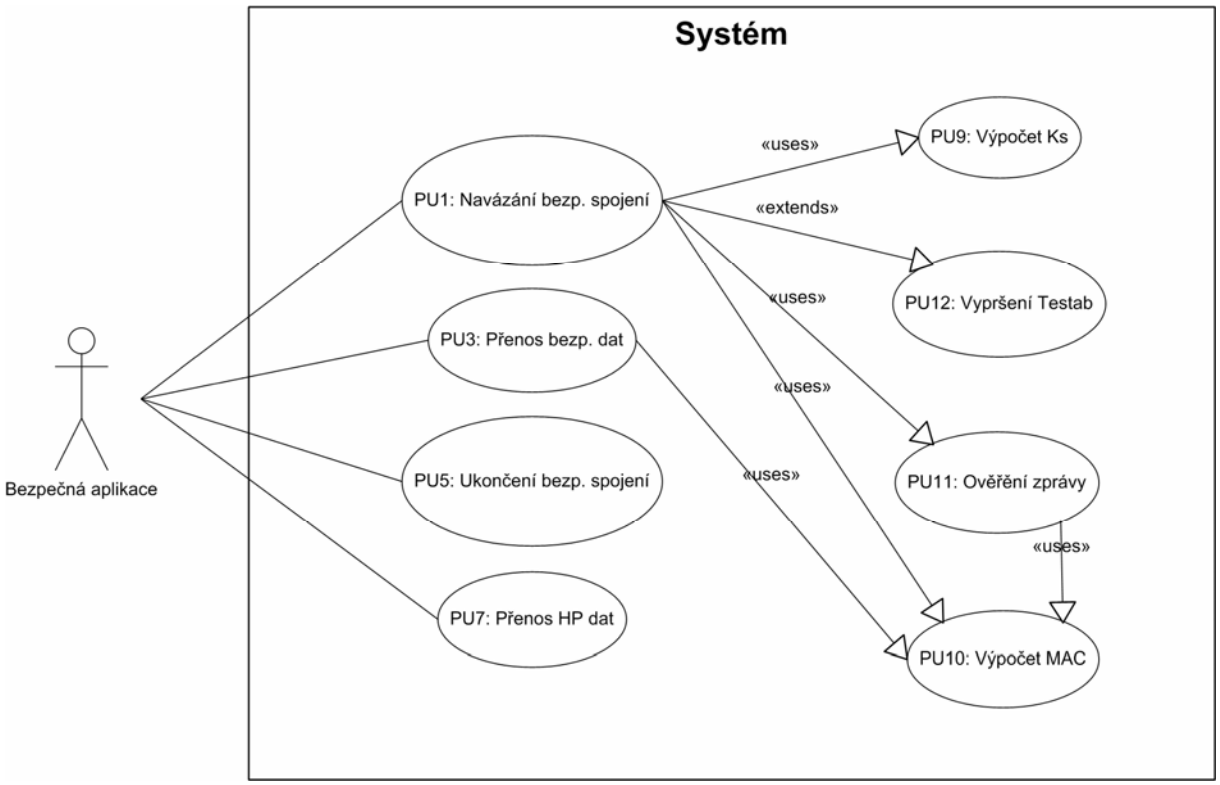
Rozhraní k bezpečným službám je popsáno v kapitole 4.

Rozhraní ke komunikačním službám jsou detailně popsány v příloze B.

8.3 Seznam aktérů

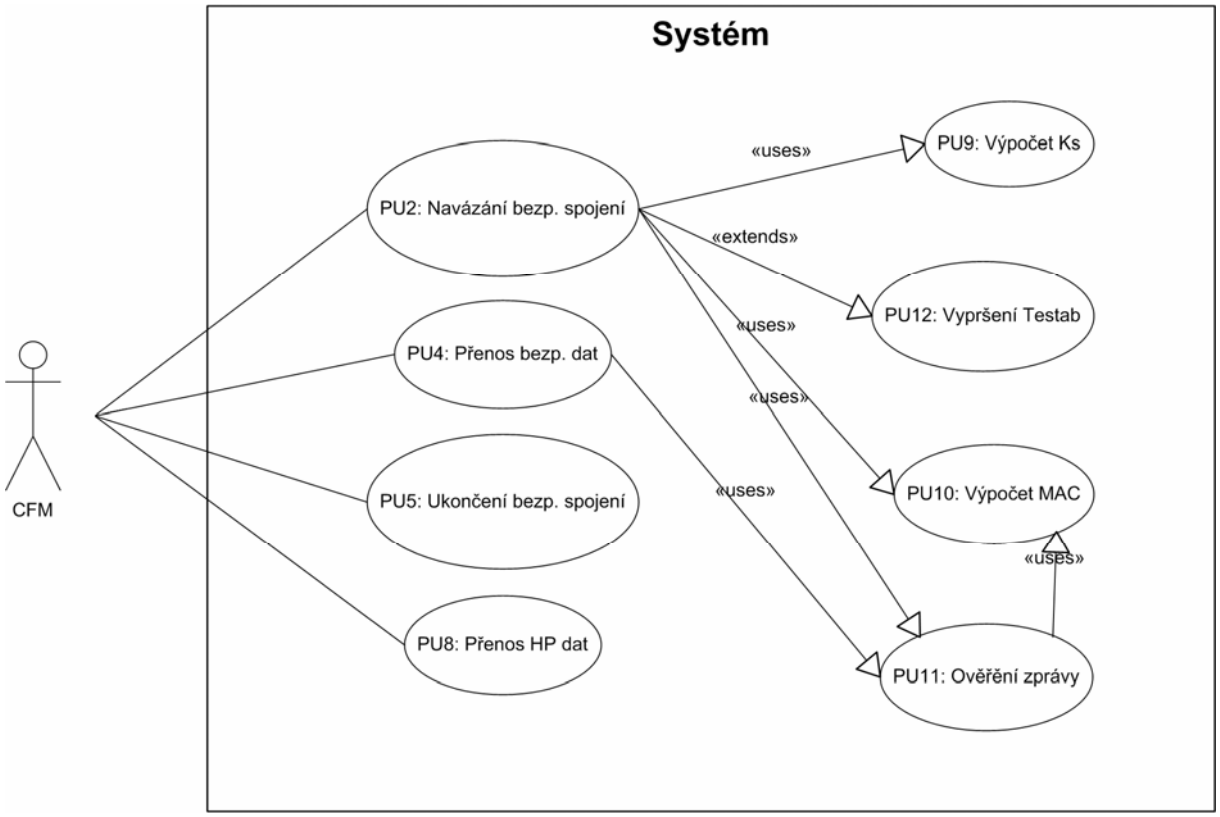
Primární aktéři:

Bezpečná aplikace: pravděpodobně program typu ATP běžící na EVC.



Obr.9: Diagram případů užití aktéra Bezpečná aplikace

CFM: komunikační jednotka na vozidle, jež se stará o odesílání a příjem zpráv vzdušnou cestou (zahrnuje nižší síťové vrstvy dle referenčního modelu OSI).

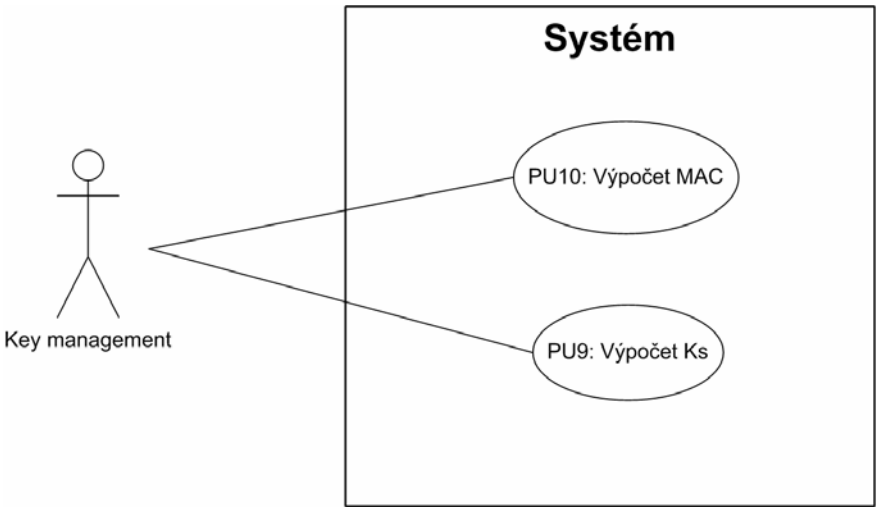


Obr.10: Diagram případů užití aktéra CFM

Pomocní aktéři:

Error management: ošetřuje chyby, jež mohou nastat v systému.
Tento aktér zasahuje do všech případů užití.

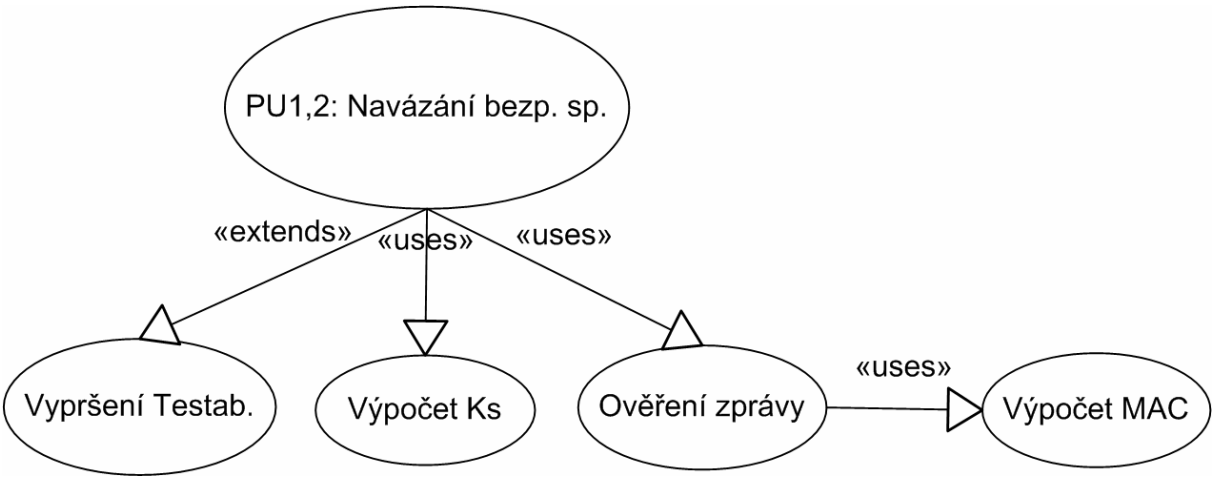
Key management: spravuje všechny druhy klíčů a poskytuje je systému. Popis není součástí této práce.



Obr.11: Diagram případů užití aktéra Key management

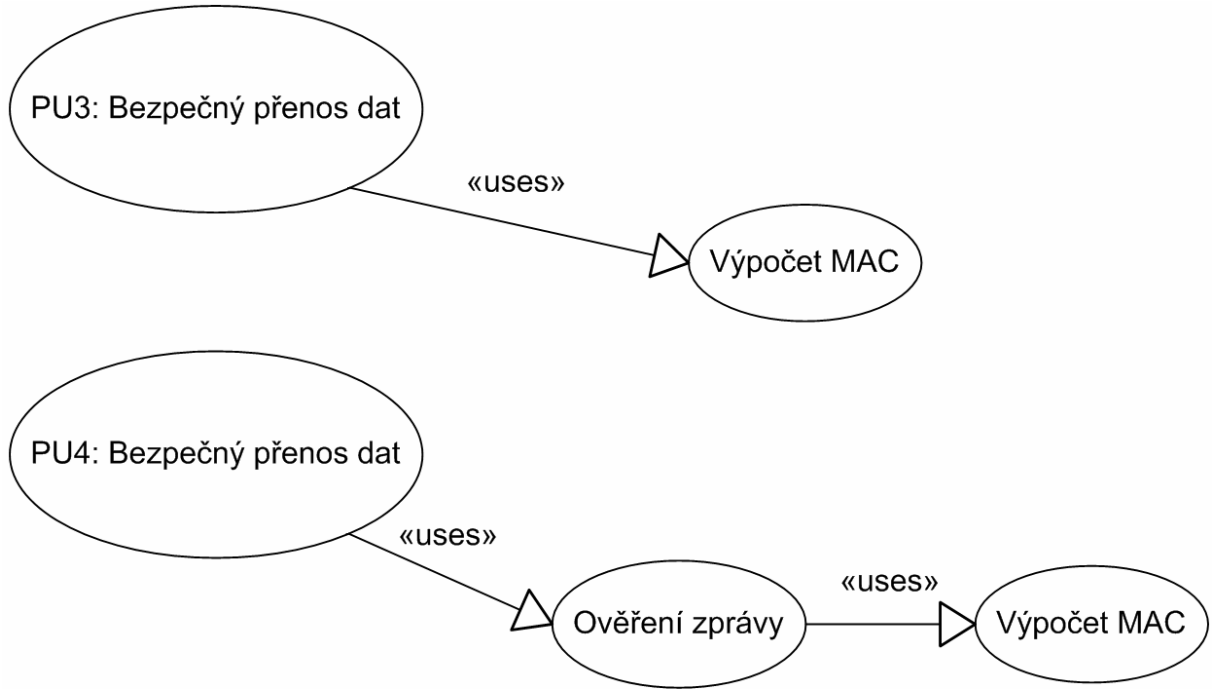
8.4 Seznam aktérů a jejich uživatelských cílů

Navázání bezpečného spojení – Bezpečná aplikace, CFM, Error management, Key management



Obr.12: Diagram vztahů případů užití Navázání bezpečného spojení

Přenos dat – Bezpečná aplikace, CFM, Error management, Key management



Obr.13: Diagram vztahů případů užití Bezpečný přenos dat

Ukončení spojení – Bezpečná aplikace, CFM, Error management
Tento případ užití není provázán s jiným.

Hlášení chyb – Bezpečná aplikace, CFM, Systém, Error management
Tento případ užití není provázán s jiným.

Zprávy s vysokou prioritou – Bezpečná aplikace, CFM, Error management
Tento případ užití není provázán s jiným.

8.5 Seznam příchozích událostí

Sa-CONN.req

Sa-CONN.resp

Sa-DATA.req

Sa-HP-Data.req

Sa-DISC.req

T-DISC.ind

T-CONN.ind (+AU1SaPDU)

T-CONN.conf (+AU2SaPDU)

AU3 SaPDU

AR SaPDU

DI SaPDU

DT SaPDU

HP SaPDU

Časovač Testab

8.6 Seznam odchozích událostí

Sa-CONN.ind

Sa-CONN.conf

Sa-DATA.ind

Sa-HP-DATA.ind

Sa-DISC.ind

Sa-REPORT.ind

T-CONN.req (+AU1SaPDU)

T-CONN.resp (+AU2SaPDU)

T-DISC.req

AU3 SaPDU

AR SaPDU

DI SaPDU

DT SaPDU

HP SaPDU

8.7 Navázání bezpečného spojení:

Služba, poskytující bezpečné spojení je realizována provedením bezpečné procedury „autentizace peer entity“.

Autentizace peer entity je poskytnuta systémem mezi entitami bezpečné vrstvy. Při požadavku na navázání bezpečného spojení systém aktivuje odpovídající mechanismus na ověření autentizace entity.

Každá chyba ve vykonání bezpečné procedury „autentizace peer entity“ musí vždy vyústit v odmítnutí navázání spojení a v ukončení transportního spojení.

Příklad užití 1:

Název:	Navázání bezpečného spojení ze strany mobilní části (autentizace peer entity).
Rozsah:	Systém.
Úroveň:	Uživatelský cíl.
Primární aktér:	Iniciátor spojení - bezpečná aplikace.
Spouštěč:	Systém obdržel od bezpečné aplikace požadavek na navázání bezpečného spojení.
Aktér2:	CFM.

Vstupní podmínky: Mobilní část je přihlášena do sítě.

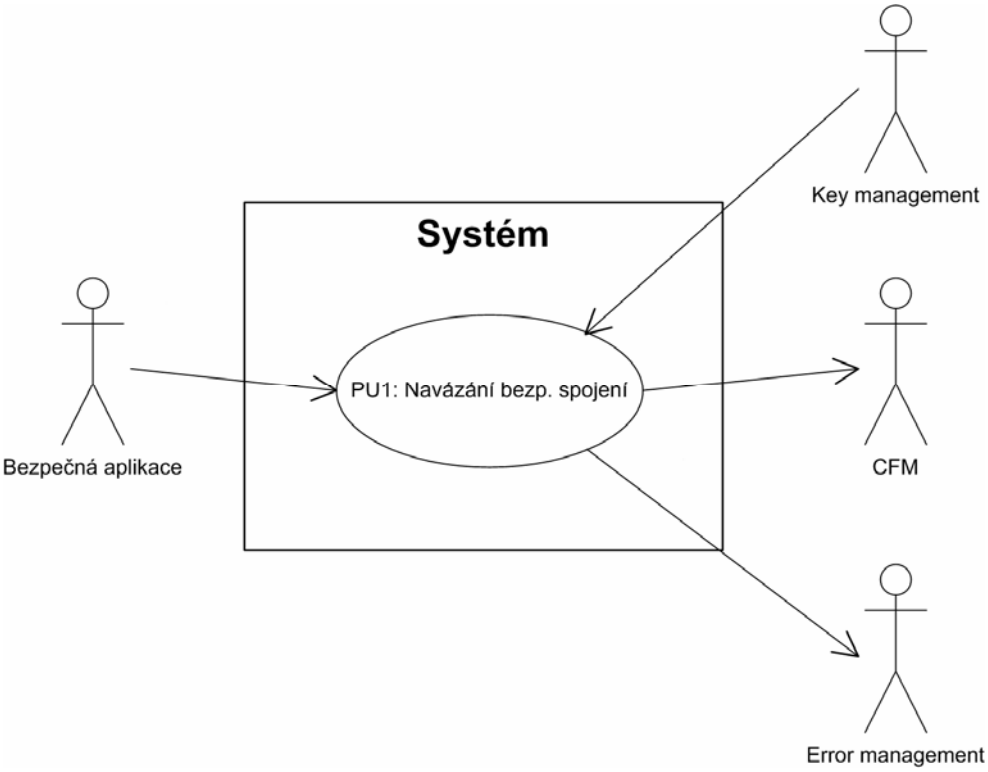
Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Primární aktér požaduje bezpečné spojení.
2) Systém přijme požadavek na bezpečné spojení (SaCONN.req).
3) Systém spustí časovač Testab. (běžně 40s).
4) Systém vygeneruje zprávu AU1.
5) Systém předá tuto zprávu k odeslání aktérovi 2 (T-CONN.req).
6) Systém čeká na příjem zprávy AU2 od aktéra 2.
7) Aktér2 přijme a předá zprávu AU2 systému (T-CONN.conf).
8) Systém odvodí session klíč z dat zprávy AU2 dle procedury výpočet session klíče.
9) Systém ověří zprávu AU2 dle procedury ověření zprávy.
10) Systém vygeneruje zprávu AU3.
11) Systém předá tuto zprávu k odeslání aktérovi 2.
12) Systém čeká na příjem zprávy AR od aktéra 2.
13) Aktér 2 přijme zprávu AR.
14) Systém ověří zprávu AR dle procedury ověření zprávy.
15) Systém zastaví časovač Testab.
16) Primární aktér obdrží od systému informaci o úspěšném navázání bezpečného spojení (SaCONN.conf).

Pozn.: Jestliže vyprší čas Testab., přebírá další akce error management.

V případě jakékoli chyby je ukončeno spojení a další akce přebírá error management.



Obr.14: Diagram vztahů případu užití Navázání bezpečného spojení

Příklad užití 2:

Název: Navázání bezpečného spojení ze strany RBC (autentizace peer entity).

Rozsah: Systém.

Úroveň: Uživatelský cíl.

Primární aktér: Iniciátor spojení – CFM

Spouštěč: Systém obdržel od CFM požadavek na navázání bezpečného spojení.

Aktér2: Bezpečná aplikace

Vstupní podmínky: Mobilní část je přihlášena do sítě

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Primární aktér požaduje bezpečné spojení.
2) Systém přijme zprávu AU1 (T-CONN.ind).
3) Systém spustí časovač Testab. (běžně 40s).
4) Systém odvodí session klíč z dat zprávy AU1 dle procedury výpočet session klíče.
5) Systém ověří zprávu AU1 dle procedury ověření zprávy.
6) Systém vygeneruje zprávu AU2.
7) Systém předá tuto zprávu k odeslání primárnímu aktérovi (T-CONN.resp).

8) Systém čeká na příjem zprávy AU3 od primárního aktéra.

9) Primární aktér přijme zprávu AU3.

10) Systém ověří zprávu AU3 dle procedury ověření zprávy.

11) Systém předá informaci o navázání bezpečného spojení aktérovi 2 (SaCONN.ind).

12) Aktér 2 potvrdí přijetí bezpečného spojení systému (SaCONN.resp).

13) Systém vygeneruje zprávu AR.

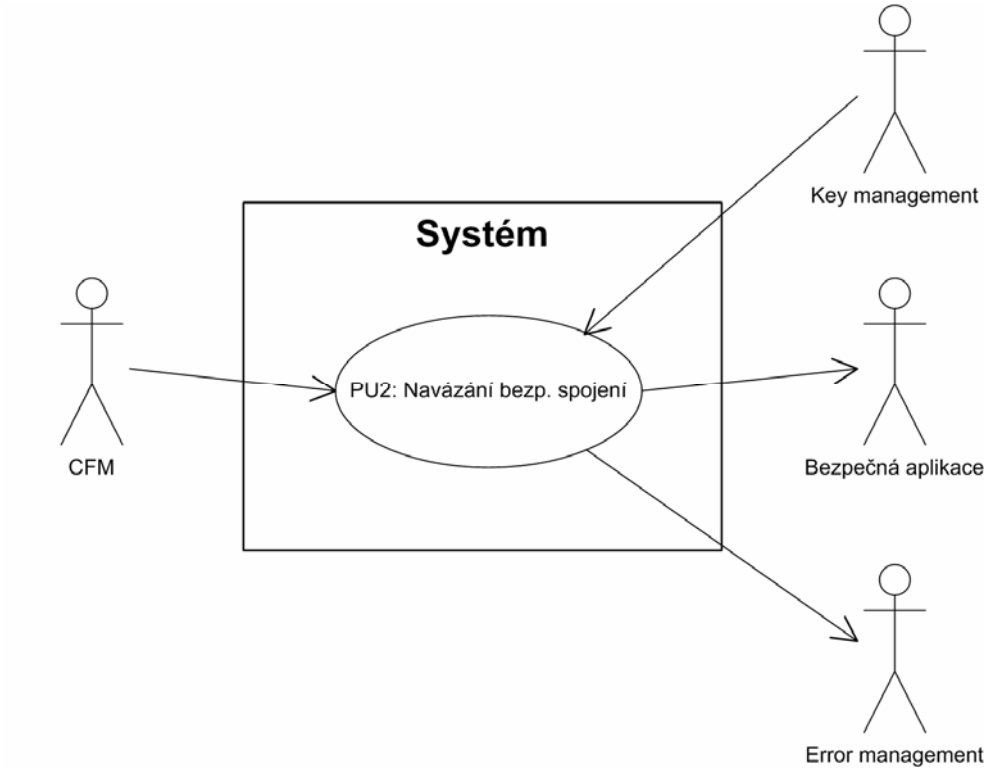
14) Systém předá tuto zprávu k odeslání primárnímu aktérovi.

15) Primární aktér odešle zprávu „druhé straně“ komunikace.

Pozn.: Jestliže vyprší čas Testab., přebírá další akce error management.

V případě jakékoli chyby je ukončeno spojení a další akce přebírá error management.

Podrobný popis procedury navázání bezpečného spojení je uveden v kapitole 5.2.3.1.



Obr.15: Diagram vztahů případu užití Navázání bezpečného spojení

8.8 Bezpečný přenos dat:

Účelem fáze přenosu dat je umožnit přenos běžných uživatelských dat mezi dvěma SaS uživateli propojených bezpečným spojením.

Systém zajišťuje výměnu uživatelských dat v obou směrech současně a chrání integritu a rozsah uživatelských dat.

Systém garantuje bezpečný přenos dat pro bezpečnostně relevantní zprávy. Služba bezpečného přenosu dat používá bezpečnou proceduru „ověření původu zprávy“.

Tato procedura poskytuje ochranu proti porušení integrity a proti vložení nových zpráv neautorizovanými uživateli přenosového kanálu. Porušením integrity se myslí jakákoliv modifikace zprávy aktivním útokem, či vinou náhodných chyb přenosového kanálu.

Vždy, když systém přijme datovou zprávu, dodanou přenosovým systémem (zprávy od SaS uživatelů jsou považovány za bezpečné), měla by ověřit, zda zpráva byla poslána odpovídající peer entitou, a že nebyla pozměněna během přenosu. Obě operace (tj. ověření odesílatele a integrity zprávy).

Velikost dat je omezena na 1023B.

Příklad užití 3:

Název:	Bezpečný přenos dat ze strany bezpečné aplikace.
Rozsah:	Systém.
Úroveň:	Uživatelský cíl.
Primární aktér:	Iniciátor spojení – bezpečná aplikace.
Spouštěč:	Systém obdržel od bezpečné aplikace požadavek na navázání bezpečného spojení.
Aktér2:	CFM

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Primární aktér žádá po systému odeslání uživatelských dat (SaDATA.req).

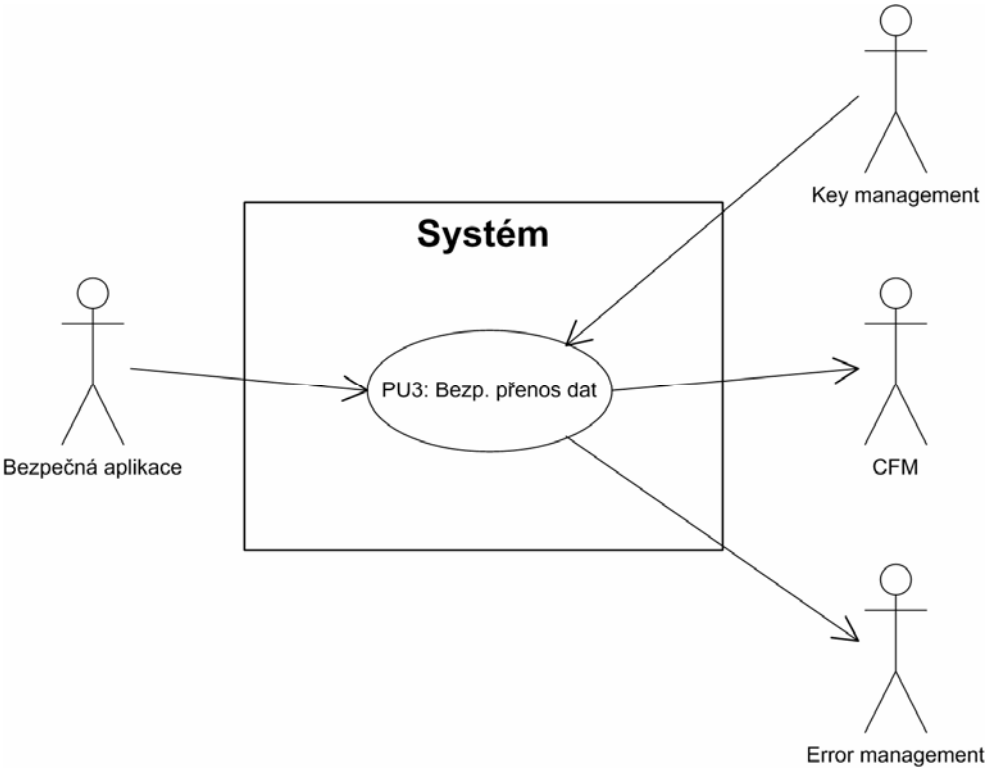
2) Systém spočte MAC zprávy dle procedury výpočet MAC zprávy.

3) Systém systém vybaví zprávu bezpečnostními atributy

4) Systém předá tuto zprávu k odeslání aktérovi 2.

5) Aktér2 odešle zprávu „druhé straně“ komunikace.

Podrobný popis jednotlivých druhů zpráv je popsán v kapitole 5.2.4.



Obr.16: Diagram vztahů případu užití Bezpečný přenos dat

Příklad užití 4:

Název: Bezpečný přenos dat ze strany CFM.

Rozsah: Systém.

Úroveň: Uživatelský cíl.

Primární aktér: Iniciátor spojení – CFM.

Spouštěč: Systém obdržel od CFM přijatou zprávu.

Aktér2: Bezpečná aplikace.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

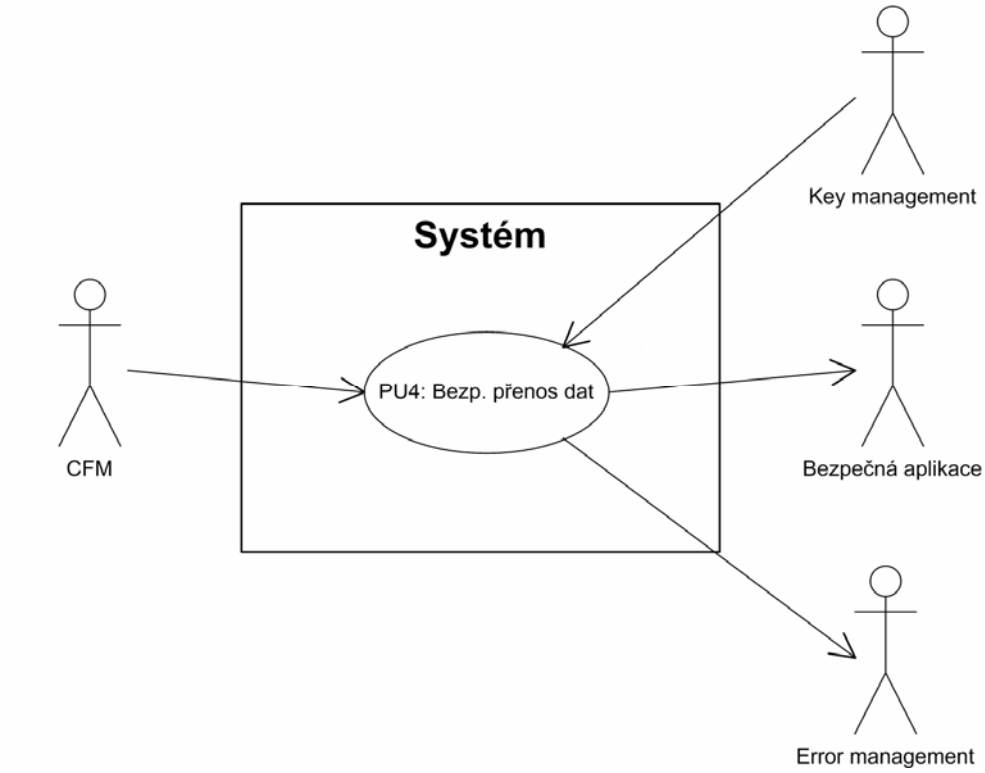
1) Primární aktér přijme a předá zprávu systému (SaDATA.ind).

2) Systém spočte svojí variantu MAC zprávy dle procedury výpočet MAC zprávy.

3) Systém ověří zprávu dle procedury ověření zprávy.

4) Systém předá příslušnému aktérovi uživatelská data (Sa-DATA.ind).

Podrobný popis procedury navázání bezpečného spojení je uveden v kapitole 5.2.3.2.



Obr.17: Diagram vztahů případu užití Bezpečný přenos dat

8.9 Ukončení bezpečného spojení:

Ukončení bezpečného spojení je možné kdykoli, bez ohledu na aktuální fázi bezpečného spojení. Požadavek na ukončení nemůže být odmítnut. Bezpečná služba negarantuje doručení Sa uživatelských dat jakmile se zahájí ukončování spojení.

Žádost SaS uživatele o ukončení bezpečného spojení nepotřebuje specifikovanou bezpečnou ochranu na rozdíl od bezpečného navázání spojení, protože ukončení spojení má vliv pouze na dostupnost. Navíc je bezpečné spojení smysluplné, pouze když nejsou ukončena základní spojení mezi nižšími vrstvami, a transportní či síťové spojení může být ukončeno nezávisle na bezpečné vrstvě.

Bezpečné spojení je ukončeno na požadavek SaS uživatele, zásahem poskytovatele transportní služby, nebo akcí ošetřující chybu v bezpečné vrstvě (Error management).

Příklad užití 5:

Název:	Ukončení bezpečného spojení.
Rozsah:	Systém.
Úroveň:	Uživatelský cíl.
Primární aktér:	Bezpečná aplikace, error management, CFM.
Spouštěč:	Systém obdržel požadavek na ukončení bezpečného spojení.
Aktér2:	Bezpečná aplikace, CFM.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení.

Minimální záruky: V každém případě je ukončeno bezpečné spojení

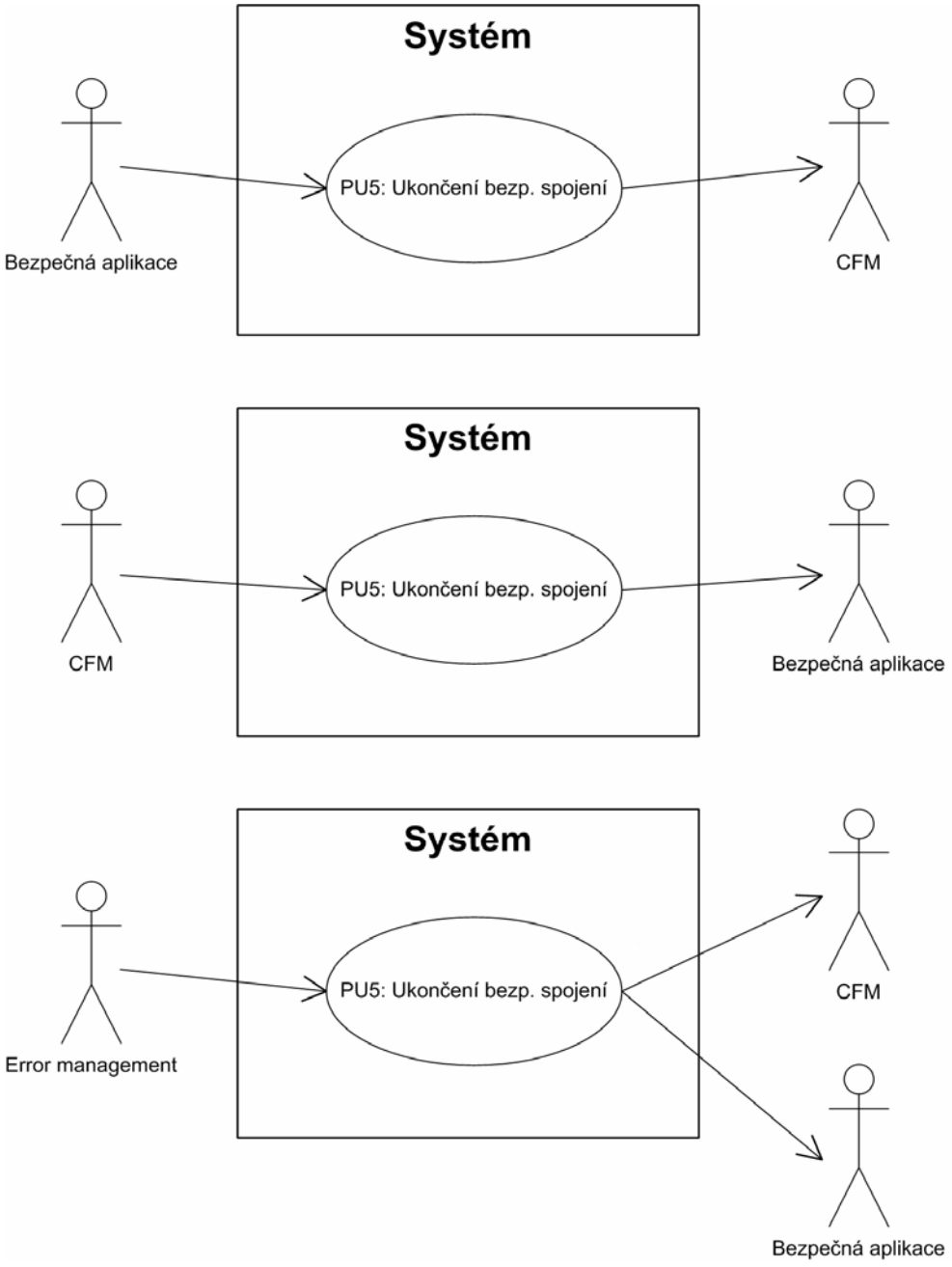
Hlavní úspěšný scénář:

1) Primární aktér žádá o ukončení bezpečného spojení (SaDISCONN.req).

2) Systém ukončí bezpečné spojení (T-DISCONN.req).

3) Systém informuje aktéra 2 o ukončení bezpečného spojení – včetně příslušného důvodu ukončení (SaDISCONN.ind).

V případě ukončení bezpečného spojení způsobeným sítí, nebo odmítnutí požadavku na navázání spojení, aplikace musí žádat opětovné navázání bezpečného spojení. Palubní ATP iniciuje opětovné navázání bezpečného spojení. Kvůli možné ztrátě uživatelských dat může být požadována opětovná synchronizace aplikačních dat.



Obr.18: Diagram vztahů případu užití Ukončení bezpečného spojení

8.10 Hlášení chyb:

Chyba se může vyskytnout během navázání spojení, při autentizaci peer entity, během přenosu dat a při řízení bezpečného protokolu.

Systém poskytuje funkci hlášení chyb pro navázané bezpečné spojení SaS uživateli. Nastalé chyby jsou buď indikované pomocí ukončení bezpečného spojení, nebo volitelně pomocí hlášení o chybách. Neschopnost bezpečné vrstvy poskytnout službu bude hlášena SaS uživateli.

Všechny bezpečnostně relevantní chyby, jež se vyskytnou v bezpečné vrstvě musí být neprodleně hlášeny aplikaci, okamžitě po jejich výskytu. Chyby ošetřeny vnitřně, managementem bezpečné vrstvy, mohou být hlášeny aplikaci, ale nemusí. Existují dvě možnosti informování o chybách (směrem k aplikaci):

1) Vede-li chyba k povinnému ukončení spojení, může být hlášena aplikaci použitím Sa-DISCONNECT.indication. Aplikace je informována o druhu chyby prostřednictvím parametru disconnect reason.

2) Je-li chyba ošetřena pouze vnitřně managementem bezpečné vrstvy, nebo nevede-li k povinnému ukončení spojení, může být volitelně hlášeno aplikaci použitím Sa-REPORT.indication. Aplikace je informována o typu chyby parametry reason code a sub-reason code.

Příklad užití 6:

Název:	Hlášení chyb.
Rozsah:	Error management.
Úroveň:	Uživatelský cíl.
Primární aktér:	Systém.
Spouštěč:	Systém informuje error management o nastalé chybě.
Aktér2:	Bezpečná aplikace, CFM.

Hlavní úspěšný scénář:

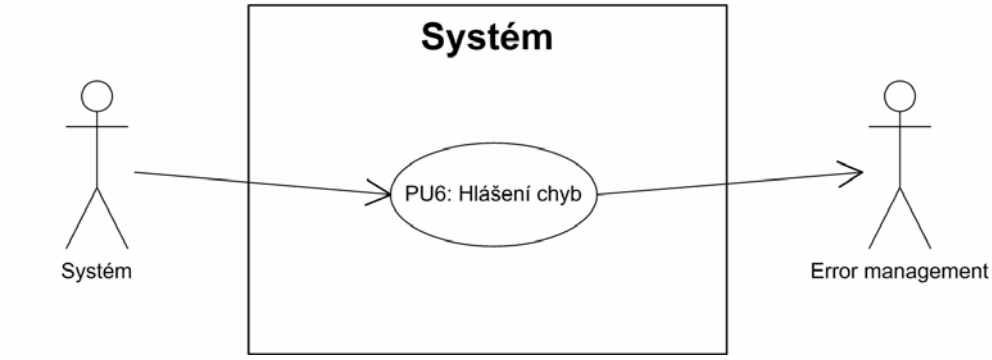
1) Systém informuje error management o nastalé chybě.

2) Error management předá aktérům informaci o příslušné chybě (SaDISCONN.ind či SaREPORT.ind).

3) Error management provede příslušné kroky.

Pod pojmem příslušné kroky je myšleno: požadování ukončení spojení (je-li toto vyžadováno) atp.. Podrobněji v kapitole 5.3.3.2.

Podrobný popis jednotlivých chyb i jejich ošetření je zachycen v kapitolách 5.3.3.1 a 5.3.3.2.



Obr.19: Diagram vztahů případu užití Hlášení chyb

8.11 Přenos dat s vysokou prioritou:

Systém neposkytuje ochranu pro data s vysokou prioritou. Služba nesmí být použita před úspěšným navázáním bezpečného spojení, tj. může být použita pouze po úspěšném výkonu bezpečné procedury „ověření původu zprávy“.

Velikost HP dat je omezena na maximálně 25B.

Požadavek Class1: Je povinné být schopný přenést HP data z RBC na vlak.

Příklad užití 7:

Název:	Přenos dat s vysokou prioritou ze strany bezpečné aplikace.
Rozsah:	Systém.
Úroveň:	Uživatelský cíl.
Primární aktér:	Iniciátor spojení – bezpečná aplikace.
Spouštěč:	Systém obdržel od bezpečné aplikace požadavek na odeslání HP dat.
Aktér2:	CFM.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení.

Minimální záruky: Vyskytneli se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

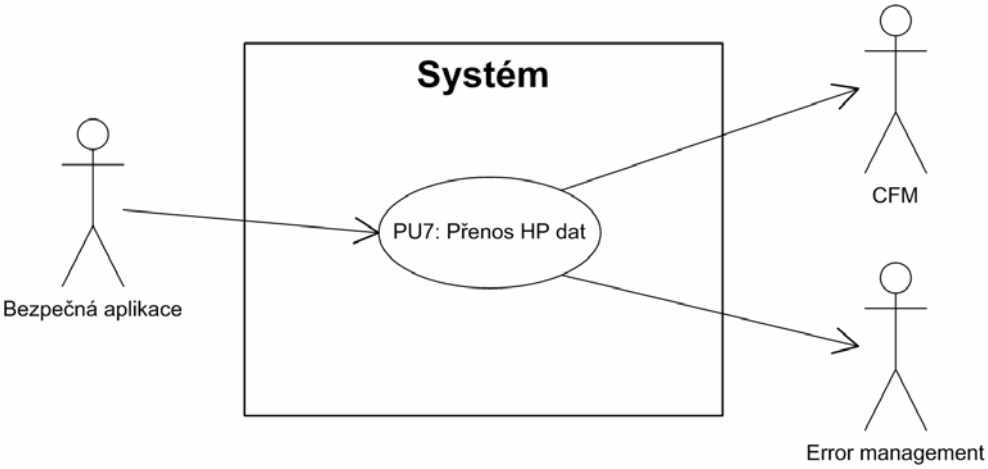
1) Primární aktér žádá po systému odeslání HP dat (Sa-HP-DATA.req).

2) Systém přednostně předá zprávu k odeslání aktérovi 2.

3) Aktér 2 odešle zprávu „druhé straně“ komunikace.

4) Systém čeká na potvrzení o doručení zprávy.

5) Aktér 2 potvrdí příjem zprávy.



Obr.20: Diagram vztahů případu užití Přenos HP dat

Příklad užití 8:

Název: Přenos dat s vysokou prioritou ze strany CFM.

Rozsah: Systém.

Úroveň: Uživatelský cíl.

Primární aktér: Iniciátor spojení – CFM.

Spouštěč: Systém obdržel od CFM zprávu s vysokou prioritou.

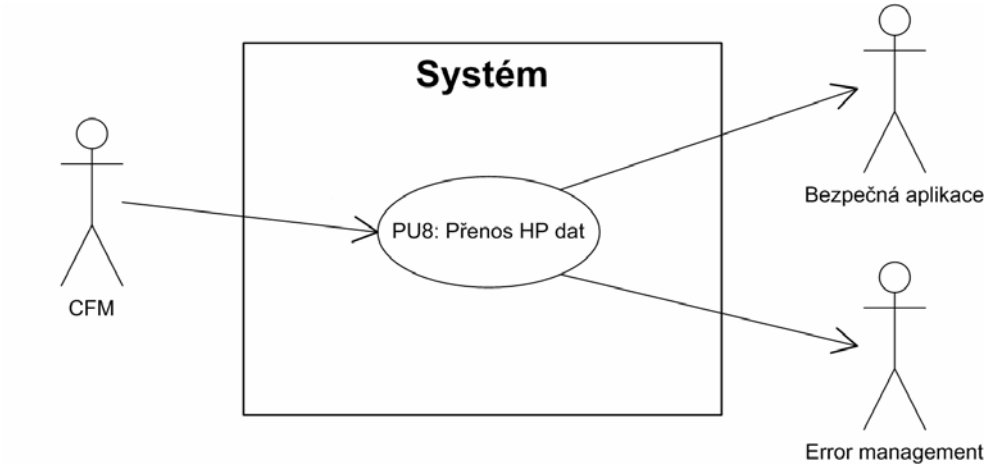
Aktér2: Bezpečná aplikace.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení.

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Primární aktér předá systému HP data.
2) Systém předá zprávu bezpečné aplikaci (Sa-HP-DATA.ind).
3) Systém předá potvrzení o příjmu zprávy primárnímu aktérovi.
4) Primární aktér odešle potvrzení o příjmu „druhé straně“ komunikace.



Obr.21: Diagram vztahů případu užití Přenos HP dat

Specifikace nařizují potvrzovat doručení zprávy, případně její opětovné odeslání. Tuto funkci musí zařídit aplikace. Dle mého názoru je nutno zavést další časovač. Ten bude nastaven na hodnotu o něco vyšší, než je předpokládané zpoždění přenosem (tam a zpět). V případě že tento časovač vyprší bude nutné odeslat HP zprávu znovu a to až do doby, kdy bude potvrzeno její přijetí.

Sdílí-li jedno fyzické spojení více ATP aplikací jsou HP data doručena všem aplikacím tohoto typu multiplexovaných na tomto fyzickém spojení.

8.12 Případy užití nižší úrovně:

8.12.1 Výpočet session klíče

Příklad užití 9:

Název:	Výpočet session klíče.
Rozsah:	Systém.
Úroveň:	Subfunkce.
Primární aktér:	Případ užití vyšší úrovně.
Spouštěč:	Případ užití vyšší úrovně žádá výpočet session klíče.
Aktér2:	Error management.

Vstupní podmínky: Jsou k dispozici náhodná čísla Ra a Rb a klíče vyšších úrovní.

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Výpočet session klíče je detailně popsán v kapitole 5.2.2.1, proto zde uvedu pouze předpis pro jeho výpočet. V tomto případě nemá význam rozepisovat případ užití.

KS1 = MAC (RaL|RbL,Kab) = DES (K3,DES-1(K2,DES(K1,RaL|RbL)))

KS2 = MAC (RaR|RbR,Kab) = DES (K3,DES-1(K2,DES(K1,RaR|RbR)))

KS3 = MAC (RaL|RbL,K´ab) = DES (K1,DES-1(K2,DES(K3,RaL|RbL)))

Key management není v rozsahu této práce. Je popsán v Subset-038.

8.12.2 Výpočet MAC zprávy

Příklad užití 10:

Název: Výpočet MAC zprávy.

Rozsah: Systém.

Úroveň: Subfunkce.

Primární aktér: Případ užití vyšší úrovně.

Spouštěč: Případ užití vyšší úrovně žádá výpočet MAC zprávy.

Aktér2: Error management.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení – existuje session klíč.

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Systém nastaví příznak směru zprávy m.

2) Systém připojí cílovou adresu před zprávu – DA|m.

3) Systém vypočte délku řetězce DA|m (v bajtech).

4) Systém ověří, že délka řetězce DA|m je celočíselný násobek 64b.

5) Systém připojí délku řetězce (16b) před řetězec – l|DA|m (|p).

6) Vypočteme MAC řetězce l|DA|m (|p) použitím CBC-MAC funkce a kryptografického klíče Ks: MAC(m) = CBC-MAC(KS, l |DA|m|p).

Rozšíření případu užití:

4a1) Délka řetězce není celočíselný násobek 64b.

4a2) Systém provede „vycpání“ a tím zvětší velikost dat na nejbližší vyšší celočíselný násobek 64b.

CBC-MAC(K,X) funkce používá tajný kód K a libovolný datový řetězec X, pro který má být spočítaná. Výpočet je definován následujícím způsobem:

Nechť K = (K1,K2,K3), nechť X je představováno 64bitovými bloky dat X1,X2, …, Xq. Nechť E (Kn, Y) je bloková šifra, jednoduchý DES, kódující datový řetězec Y užitím klíče Kn (n=1, 2, 3), E^{-1} (Kn, Y) je bloková šifra v dešifrovacím významu. Pak H_q je odvozeno tímto způsobem (iterací):

$H_0 = 0$

$H_i = E\ (K1, H_{i-1}\ (XOR)\ X_i)$

$H_q = E\ (K3, E^{-1}\ (K2, E\ (K1, H_{q-1}\ (XOR)\ X_q)))$

MAC datového řetězce X je roven H_q.

Vycpávací data (nulové bity) nejsou posílána, protože přijímač je může spočítat, zná-li vycpávací algoritmus, který byl použit. Vycpání je použito z důvodu výpočtu MAC.

8.12.3 Ověření původu zprávy a integrita zprávy

Tyto bezpečné procedury zajišťují integritu a autenticitu během přenosu zpráv. Slouží k ochraně zpráv proti modifikaci a k zajištění, že se nikdo nemůže maskovat jako původce zprávy. Dále je procedura prostě nazývaná „ověření zprávy“.

Příklad užití 11:

Název: Ověření zprávy.

Rozsah: Systém.

Úroveň: Subfunkce.

Primární aktér: Případ užití vyšší úrovně.

Spouštěč: Případ užití vyšší úrovně žádá ověření původu zprávy.

Aktér2: Error management.

Vstupní podmínky: Mezi účastníky je navázáno bezpečné spojení – existuje session klíč.

Minimální záruky: Vyskytne-li se chyba je informován error management a přebírá další akce.

Hlavní úspěšný scénář:

1) Systém připojí cílovou adresu před zprávu – DA|m.

2) Systém vypočte délku řetězce DA|m (v bajtech).

3) Systém ověří, že délka řetězce DA|m je celočíselný násobek 64b.

4) Systém připojí délku řetězce (16b) před řetězec – l|DA|m (|p).

5) Vypočteme MAC řetězce l|DA|m (|p) použitím CBC-MAC funkce a kryptografického klíče Ks: MAC(m) = CBC-MAC(KS, l |DA|m|p).

6) Porovná se přijatý a vypočtený MAC.

7) Ověří se hodnota DF.

Postup výpočtu je podrobněji popsán výše (kap. 5.2.2.1), z důvodů přehlednosti textu jej nebudu uvádět opakovaně i zde.

Výjimkou je zpráva AU2, která obsahuje data nutná k jejímu ověření – náhodné číslo Rb.

8.12.4 Vypršení času Testab:

Tento časovač omezuje maximální prodlevu při navazování spojení.

Je-li dosaženo času Testab. dojde k ukončení fáze navazování bezpečného spojení.

Příklad užití 12:

Název: Vypršení času Testab.

Rozsah: Systém.

Úroveň: Subfunkce.

Primární aktér: Systém.

Spouštěč: Případ užití vyšší úrovně žádá ověření původu zprávy.

Aktér2: Error management.

Minimální záruky: V každém případě je ukončena fáze navazování bezpečného spojení.

Hlavní úspěšný scénář:

1) Vypršel nastavený čas Testab.
2) Systém ukončí fázi navazování bezpečného spojení.
3) Systém informuje aktéra 2 o ukončení fáze navazování bezpečného spojení.

9 ZHODNOCENÍ

Protokol Euroradio zabezpečuje komunikaci na koncích otevřeného přenosového systému. K tomu používá kombinace několika druhů ochran. I přes to, že neobsahuje všechna výše uvedená zabezpečení, je tento systém velice dobře zabezpečen proti všem druhům možných rizik mimo nebezpečí, že zpráva nebude z jakéhokoli důvodu doručena (vinou ukončení spojení, nenadálého rušení, ztráty pokrytí …). Tento problém je ale vyřešen pomocí omezení kritických aktivit vlaku místně, nebo časově, takže aplikace s vysokou pravděpodobností zaručí, že nedoručením běžné zprávy vznikne nebezpečná situace (vždy bude platit více omezující podmínka).

Nebezpečí zpoždění se nedá u sítí typu GSM eliminovat a je nutno s ním počítat a přizpůsobit aplikace tomuto nedostatku. Zpoždění může nabývat až desítek sekund což představuje ve vysokých rychlostech velice velké vzdálenosti. Proto je, jako v předešlé situaci, využito omezení kritických aktivit časem a/nebo polohou.

Při navazování takového bezpečného spojení si iniciátor spojení s druhou stranou vymění několik zpráv a tím provede vytvoření bezpečného spojení a obě strany si ověří autenticitu a způsobilost druhé strany. V této fázi se také ustanoví session klíč, který se následně používá pro výpočet MAC. Tento klíč (192b včetně paritních bitů) je složen ze 3 částí (po 64b, z nichž je 56b aktivních, ostatní jsou redundantní paritní bity). Každá tato část je postupně použita při iteračním výpočtu MAC. Tato metoda podstatně potlačuje riziko úniku session klíče k neoprávněnému uživateli – maskování je reálně nemožné.

MAC velmi dobře detekuje různé druhy chyb a tím téměř eliminují nerozpoznání poškozené zprávy.

Obdrží-li příjemce zprávu, která není určena pro něj (což by nemělo nastat protože mezi takovýmito uživateli pravděpodobně není navázáno bezpečné spojení), okamžitě to odhalí pomocí MAC. MAC tedy zaručuje integritu a autenticitu zprávy. Tímto je zabráněno nebezpečí vložení a přeřazení.

V normě EN50159-2 není uvedeno nebezpečí zrcadlení, tento problém je v protokolu Euroradio ošetřen tzv. příznakem směru (DF).

Celkové riziko možnosti chyby zprávy či napadení komunikace je navíc velice omezeno tím, že komunikace probíhá skrze bezpečné spojení, které bylo vytvořeno při zahájení komunikace.

HP data, kvůli potřebě rychlého předání protější straně, obcházejí (dle protokolu Euroradio) zabezpečovací funkce. Je tedy nutné kontrolovat jejich korektní doručení aplikací. Tuto kontrolu je nutno ošetřit (nejspíše na vyšší úrovni). Zpráva HP dat je zabezpečena pouze tím, že prochází bezpečným spojením ustaveným mezi uživateli během navazování komunikace.

9.1 Možná vylepšení protokolu

Protokol Euroradio je již dlouhou dobu upravován a vylepšován renomovanými odborníky. Proto mě (studenta bez praxe a detailního přehledu v zabezpečovací technice a sítích takovéhoto typu – což je podle mého názoru otázka mnohaletého intenzivního studia tohoto konkrétního problému) nenapadá mnoho vylepšení.

Jako první věc, kterou bych si dovedl představit, je kódování uživatelských dat ve zprávě tak,aby nebyly čitelné pro ostatní uživatele. Otázkou však je, zda má toto opatření reálný význam. Neoprávnění uživatelé mohou data získat (velkým úsilím), ale bez možnosti vyslat je zpět nemají možnost ovlivnit jakékoli bezpečnostně relevantní pochody.

Bylo by také jistě možné zavést číslování zpráv. Tento „nedostatek“ lze snadno ošetřit přímo aplikací (je-li to potřebné). V sítí tohoto druhu je ale možné, že zprávy budou doručeny v různém pořadí (vinou jiného směrování atd.). Proto je nutné, aby aplikace takovéto data dovedly opětovně seřadit v případě, že tyto data nají návaznost. Číslování zpráv by také omezilo možnost rizika, které by mohlo vyplynout ze ztráty zprávy během přenosu, nebo z opakování zprávy.

Jako poslední možnost vylepšení vidím větší zabezpečení HP dat. Tyto data nejsou dle specifikací Euroradio nikterak zabezpečena. Vzhledem k možnému zpoždění, které může nastat při přenosu i takovýchto zpráv (v sítích tohoto typu), je podle mého názoru zpoždění vyvolané výpočtem a následným zpracováním MAC (nebo jiným zabezpečením jako CRC apod.) naprosto zanedbatelné. Tento druh zabezpečení zprávy by přitom velice zlepšil důvěryhodnost tohoto typu zpráv.

V současné době používá jazyk ETCS pouze 2 druhy HP-zpráv, což snižuje možnost jejich chybné interpretace.

Jako dobré vodítko pro pochopení návazností a podrobností může sloužit stavový diagram, který je uveden v kapitole 5.2.5. V téže kapitole následuje podrobný popis reakcí systému na jednotlivé příchozí události.

Podle mého názoru je nutno, zabývat se také uchováváním datové komunikace (z určité poslední doby, jízdy, …). Tato vlastnost systému by byla vhodná nejen pro potřebu testování, ale především při prošetřování možných nehod či provozních problémů. Schopnost systému zaznamenat komunikaci by jistě byla také velice užitečná při diagnostice a údržbě.

Specifikace Euroradio nepopisují konkrétní aplikace a použití, takže nic nebrání doplnění potřebných ochran aplikací na vyšší úrovni.

Závěrem bych rád podotkl, že daný problém (komunikace dle všech závazných nařízení) je velice rozsáhlý. Pokud by měl být řešen jako kompletní výrobek (součást hnacího vozidla) je nutný dlouhodobý intenzivní vývoj. Nejedná se však pouze o problém zkoumání toků dat a chování systému, ale i samotného návrhu hardwarových komponent, které jsou samozřejmě také bezpečnostně relevantní. Další nutnou součástí výstroje by byly také prvky komunikace. Ať už jde o komunikaci mezi jednotlivými částmi hnacího vozidla (řízení pohonu, EVC, řízení sběrače, brzdový systém …), rádiovou komunikaci s RBC (RIU) či komunikaci s balízami umístěnými v kolejišti. Je také nutno umístit na hnací vozidlo prostředky pro bezpečné měření rychlosti či ujeté vzdálenosti, bez nichž by byl celý navrhovaný systém (ETCS L2) zcela zbytečný.

Z výše uvedených argumentů vyplývá, že celkový návrh systému je otázkou dlouhodobého vývoje skupiny odborníků z mnoha oborů.

SEZNAM OBRÁZKŮ

Přílohy:

SEZNAM TABULEK

Přílohy:

SEZNAM ZKRATEK

AR	Authentication Response	Autentizační odpověď
ATC	Automatic Train Control	Automatická kontrola vlaku
ATP	Automatic Train Protection	Automatická ochrana vlaku
AU1	First Authentication message	První autentizační zpráva
AU2	Second Authentication message	Druhá autentizační zpráva
AU3	Third Authentication message	Třetí autentizační zpráva
BAC	Balanced Asynchronous Class	Symetrická asynchronní třída přenosu dat
B_m	Full-rate traffic channel	
BS	Bearer Service	Nosná služba
CEPID	Connection EndPoint IDentifier	ID koncového bodu spojení
CELENEC	Comité Européen de Normalisation ELECtrotechnique	Evropské komise pro normalizaci v elektrotechnice
CFM	Communication Functional Module	Komunikační funkční modul
CRC	Cyclic Redundancy Check	Kontrola chyb cyklickým kódem
CSPDN	Circuit Switched Public Data Network	Veřejná síť založená na přepojování okruhů
DA	Destination Address	Adresa cíle
DCE	Data Communication Equipment	Komunikační datové zařízení
DES	Data Encryption Standard	Standard kódování dat
DF	Direction Flag	Příznak směru
DI	Disconnect	Odpojení
D_m	Control Channel	Řídící kanál
DST	Destination	Cíl (místo určení)
DT	Data	Data
DTE	Data Terminal Equipment	Uživatelské rozhraní sítě
eMLPP	Enhanced Multi-Level Precedence and Pre-emption	Rozšířená mnohaúrovňová priorita a přednostní právo
ERA	European Railway Association	Evropská drážní asociace
EIRENE	European Integrated Railway radio Enhanced NEtwork	Evropská integrovaná pokročilá rádiová síť pro železnice
EN	EuropeaN standard	Evropská norma
ENV	EuropeaN experiental standard	Předběžná evropská norma
ERTMS	European Rail Train Management System	Evropský systém pro řízení vlaků
ETCS	European Train Control System	Evropský vlakový zabezpečovací systém

ETS	European Telecommunication Standard	Evropský telekomunikační standard
ETY	ETCS ID type field in a SaPDU	Typ ETCS ID
EU	European Union	Evropská unie
FEC	Forward Error Correction	Metoda pro korekci chyb
FFFIS	Form Fit Functional Interface Specification	Specifikace rozhraní (obšírnější než FIS)
FIS	Functional Interface Specification	Specifikace rozhraní
FRMR	FRaMe Reject	Odmítnutí rámce
GSM-R	Global System for Mobile Communication - Railway	Globální systém pro mobilní komunikaci –drážní
HDLC	High level Data Link Layer Control	Vysokoúrovňové řízení linkové vrstvy
HP	High Priority	Vysoká priorita
ID	Identity	Identifikátor (identita)
IEC	International Electrotechnical Commission	Mezinárodní elektrotechnická komise
ISDN	Integrated Services Digital Network	Digitální síť integrovaných služeb
ISO	International Organisation for Standardisation	Mezinárodní organizace pro standardizaci
IT	Information Technology	Informační technologie
ITU	International Telecommunication Union	Mezinárodní telekomunikační unie
K_{AB}	Authentication Key (same as K_{MAC})	Autentizační klíč (stejný jako K_{MAC})
KM	Key Management	Správa klíčů
K_{MAC}	Authentication Key	Autentizační klíč
KMC	Key Management Centre	Centrum správy klíčů
K_{S}	Session Key (same as K_{SMAC})	Session klíč (stejný jako K_{SMAC})
K_{SMAC}	Session Key	Session klíč
K_{TRANS}	Transport Key	Transportní klíč
LAPB	Link Access Protocol Balanced	Symetrický linkový přístupový protokol
LSB	Least Significant Bit	Bit s nejnižší váhou
m	message	Zpráva
MA	Management	Řízení (správa)
MAC	Message Authentication Code	Autentizační kód zprávy
MS	Mobile Station	Mobilní stanice
MSB	Most Significant Bit	Bit s nejvyšší váhou

MSISDN	Mobile Station International Subscriber Directory Number	Mezinárodní volací číslo mobilní stanice
MT2	Mobile Termination type 2	Mobilní zakončení typu 2
MTI	Message Type Identifier	ID typu zprávy
NPDU	Network Protocol Data Unit	Datová jednotka síťového protokolu
NSAP	Network Service Access Point	Přístupový bod síťové služby
NSAP	Network layer Service Access Point	Přístupový bod služby síťové vrstvy
NSDU	Network Service Data Unit	Datová jednotka síťové služby
NT	Network Termination	Mobilní zakončení
O&M	Operation and Maintenance	Činnost a údržba
OBU	OnBoard Unit	Palubní jednotka
OSI	Open System Interconnection	Propojení otevřených systémů
PDU	Protocol Data Unit	Datová jednotka protokolu
PLMN	Public Land Mobile Network	Veřejná pozemní mobilní síť
PSTN	Public Switched Telephone Network	Veřejná spojovaná telefonní síť
QoS	Quality of Service	Kvalita služeb
RBC	Radio Block Centre	Centrum radiové komunikace
RCS	Radio Communication System also used as synonym for EURORADIO system	Radiokomunikační systém také použito jako synonymum pro systém EURORADIO
RIU	Radio In-fill Unit	
RP	Response	Odpověď
RQ	Request	Požadavek
SA	Source Address	Adresa zdroje
SABME	Set Asynchronous Balanced Mode Extended	Set Asynchronous Balanced Mode Extended
SaCEPID	Safe Connection EndPoint Identifier	Identifikátor koncového bodu bezpečného spojení
SaF	Safety Features	Bezpečné vlastnost
SAP	Service Access Point	Přístupový bod služby
SaPDU	Safety Protocol Data Unit	Datová jednotka bezpečného protokolu
SaS	Safety Service	Bezpečná služba
SaSAP	Safety Service Access Point	Přístupový bod bezpečné služby
SaSDU	Safety Service Data Unit	Datová jednotka bezpečné služby
SaUD	Safety User Data	Bezpečná uživatelská data
SFM	Safe Functional Module	Bezpečný funkční modul
SRC	Source	Zdroj

SREJ	Selective REJect	Selective REJect
SRS	System Requirements Specification	Specifikace požadavků na systém
TC	Transport Connection	Transportní (přenosové) spojení
TCEPID	Transport Connection EndPoint Identifier	Identifikátor koncového bodu transportního (přenosového) spojení
TCH	Traffic Channel	Dopravní kanál
TP	Transport Protocol	Transportní (přenosový) protokol
TP2	Transport Protocol Class 2	Transportní (přenosový) protokol třídy 2
TPDU	Transport Protocol Data Unit	Datová jednotka transportního (přenosového) protokolu
TS	Transport Service	Transportní (přenosová) služba
TSAP	Transport Service Access Point	Přístupový bod transportní (přenosové) služby
TSDU	Transport Service Data Unit	Datová jednotka transportní (přenosové) služby
UA	Unnumbered Acknowledge	Neočíslované potvrzení
UI	Unnumbered Information (HDLC frame)	Neočíslovaná informace (HDLC rámec)
X	Mandatory parameter	Povinný parametr
X(U)	Use of this parameter is an user option	Použití tohoto parametru je uživatelsky volitelné

LITERATURA

[1] ERTMS/ETCS – Class1 – Euroradio FIS, SUBSET 037, issue 2.3.0 UIC, 2005 (http://www.era.europa.eu/public/Documents/ERTMSDocumentation/Mandatory Specifications/Subset-037v230.pdf), 22.10.2008

[2] ČSN EN 50159-2: 2002 – Drážní zařízení – Komunikace v otevřených přenosových zabezpečovacích systémech, Český normalizační institut, Praha, 2002

[3] Doc. Ing. Jiří Zahradník PhD., doc. Ing. Karol Rástrčný PhD., Ing. Milan Kunhart PhD.: Bezpečnost železničných zabezpečovacích systémov, Žilinská univerzita v Žilině, ISBN 80-8070-296-9, 2004

[4] Hana Kanisová, Miroslav Muller: UML srozumitelně, Computer Press, a.s., Brno, 2006, 2. aktualizované vydání, ISBN 80-251-1083-4

[5] Alistair Cockburn: USE CASES, CP Books, a.s., Brno, 2005, Bydání první, ISBN 80-251-0721-3

[6] Petr Gregar: Analýza vlastností komunikačního protokolu Euroradio+ s ohledem na její využití v zabezpečovací technice, ročníkový projekt II, Univerzita Pardubice 2009

Příloha A: CFM – Communication Functional Module

Tato práce se CFM modulem zabývá pouze okrajově z informačních důvodů, proto je tato část vložena jako příloha.

Tato kapitola specifikuje CFM, jeho služby a „protocol stack“ založený na službách GSM PLMN a pevných sítí. CFM odpovídá OSI vrstvě 4 (transportní vrstvě), 3 (síťové vrstvě) a 2 (linkové vrstvě).

A.1 Definice:

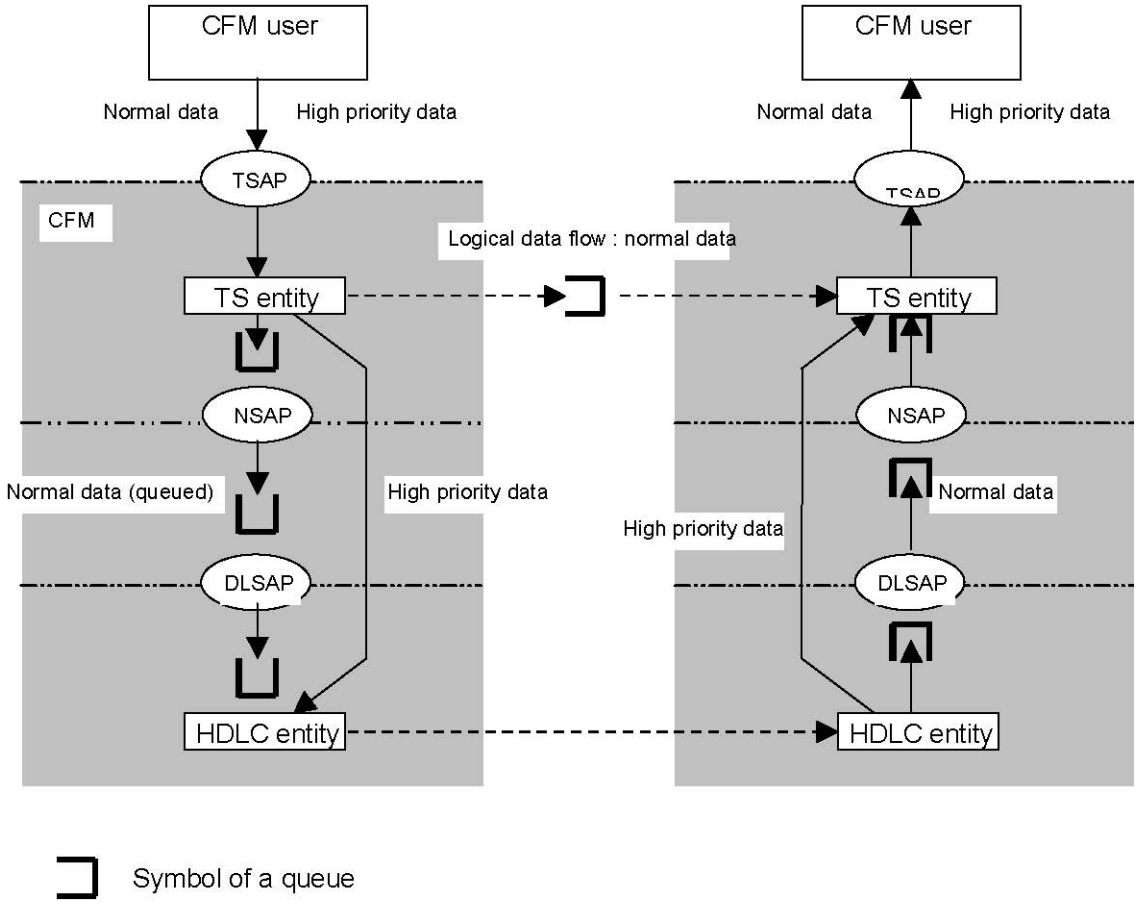
A.1.1 Model komunikačních služeb

Komunikační služby, jež RCS CFM poskytuje svým uživatelům (SFM a volitelně nikoli bezpečný uživatel) jsou založeny na službách poskytnutých transportní vrstvou ISO/OSI referenčního modelu X.214. Tyto služby se týkají:

Navázání a ukončení transportního spojení
Spolehlivého přenosu dat
Transparentního přenosu dat
Dodatečně je poskytnut přenos dat s vysokou prioritou.
CFM také zvyšuje spolehlivost přenosového kanálu.

Entita CFM komunikuje s jejími uživateli (CFM uživatel) skrze jeden nebo více TSAP pomocí základních operací přenosové služby. CFM entity podporují výměnu TPDU pro normální data použitím služeb nižších vrstev, skrze příslušný SAP.

Volitelně může CFM podporovat více než jedno spojení na jeden fyzický kanál. Tato volba není vyžadována pro ETCS level 1 RIU.



Obr.22 Model komunikační služby

A.1.2 Navázání spojení

Proces navázání transportního spojení je zahájen v čase, kdy uživatel komunikačních služeb žádá navázání spojení po CFM. Služba je přístupná skrze T-CONNECT.request s jeho přidruženými parametry v TSAP. V čase požadování vytvoření spojení má uživatel možnost specifikovat jeho potřeby, jako třídu QoS a typ aplikace.

CFM zohledňuje hodnotu třídy QoS a typ aplikace. Asociovaný soubor hodnot parametru QoS se využije pro:

1) výběr řádné přenosové služby pro navázání fyzického spojení, jestliže takové spojení ještě neexistuje

2) nebo volitelně k výběru rysů multiplexingu transportní vrstvy.

A.1.3 Přenos dat

Služba přenos dat je poskytována po úspěšném navázání transportního spojení. Tato služba je přístupná skrze T-DATA.request s jeho přidruženými parametry TSAP. CFM poskytuje transparentní a spolehlivý přenos uživatelských dat v obou směrech současně a ukrývá jeho uživatelům vnitřní cestu ve které jsou řízená data.

A.1.4 Ukončení spojení

Ukončení přenosového spojení je poskytováno CFM použitím T-DISCONNECT.request s jeho přidruženými parametry. Ukončení spojení kvůli CFM, nebo nižším vrstvám, bude indikováno uživateli.

A.1.5 Data s vysokou prioritou

Služba přenosu HP dat je dodatečná služba poskytovaná pro přenosové spojení pouze s aplikačním typem ATP (viz. dále). HP data jsou přenášena s nejvyšší prioritou přenosu vzhledem k datům všech přenosových spojení multiplexovaných na jednom fyzickém přenosovém spojení.

Služba je přístupná skrze T-HP-DATA.request s přidruženými parametry v TSAP.

Vrstvy 4 a 3 protocol stack-u jsou přeskočeny. Uživatelská data jsou vyměňována mezi CFM uživateli a vrstvou 2. Tyto data jsou ihned přenesena (obcházejí každou existující frontu). Všechny data budou směrována k peer CFM uživateli, tj. CFM uživatel s aplikací typu ATP. Multiplexování HP datových toků pro různá spojení na úrovni transportní vrstvy na stejné fyzické spojení není možné.

Poznámka: V případě více než jednoho přijímajícího CFM uživatele s aplikačním typem ATP multiplexovaného na stejném fyzickém spojení, přijímající CFM entita přenese HP data všem CFM uživatelům aplikačního typu ATP.

Vrstva 2 posílá/přijímá tyto data (a pouze tento typ dat) jako UI-rámce (Unnumbered Information HDLC frames). V případě chybných či ztracených UI rámců, vrstva 2 neopakuje přenos. Potvrzení a opakování bude poskytnuto CFM uživatelem, je-li vyžadováno.

Segmentování a skládání uživatelských dat není možné. Velikost uživatelských dat je omezena na velikost datového pole UI rámce.

Požadavek Class1: Je povinné být schopen přenášet HP data z RBC na vlak.

A.1.6 QoS – Quality of Service

Termín QoS (kvalita služby) se odkazuje na jisté charakteristiky přenosového spojení pozorované mezi dvěma koncovými body.

Parametry QoS definují uživateli přenosové služby (Transport Service - TS) způsob specifikace jejich potřeb a dávají poskytovateli TS základ pro výběr protokolu, nebo požadování služeb nižších vrstev. QoS je běžně vyjednaná mezi uživatelem TS a poskytovatelem TS za pomoci základního přenosového spojení, použitím T-CONNECT.request, indication, response a confirm TS základních operací. Sjednané QoS hodnoty se poté používají po celou dobu přenosového spojení. Pro účely této práce a použití v přenosových protokolech jsou hodnoty všech parametrů neměnné v daném aplikačním typu, v tom případě je vyjednávání QoS na základě peer transportního spojení omezeno na místní vyjednávání mezi žádající stranou a jeho entitou poskytující místní přenosové spojení.

Neexistuje žádná záruka, že vyjednaná QoS bude udržena po celou dobu přenosového spojení. Poskytovatel přenosových služeb výslovně nesignalizuje změny v QoS.

Možné volby a implicitní hodnoty pro každý parametr budou běžně specifikovány v době spuštění služby TS poskytovatele.

A.2 Komunikační protokoly

A.2.1 Úvod

Tato část poskytuje přesné specifikace komunikačních protokolů uživatelského kanálu. Specifikace protokolu jsou popsány vrstvu po vrstvě a jsou popsány prostřednictvím rozdílů oproti standardům.

A.2.2 Linková vrstva

Dle referenčního modelu OSI poskytuje bezpečný (nikoli ve smyslu zabezpečovací techniky) přenos dat linková vrstva. Linková vrstva B/Bm-kanálu poskytuje funkční a procedurální prostředky k navázání, udržení a ukončení spojení a k přenosu dat. Zjistí a opraví chyby v přenosu dat, které mohou vzniknout ve fyzické vrstvě.

Protokol vrstvy 2 (DTE-DTE komunikace) přenáší data dle sekvence svých základních operací - data request.

Protokol vrstvy 2 je popsán HDLC standardy. Aplikační podmínky jsou popsány jako rozdílové specifikace.

Může být užívána struktura rámců odpovídající ISO/IEC3309 a prvky kontrolních procedur odpovídající ISO/IEC 4335.

Mohou být použity procedury třídy HDLC balanced asynchronous class (BAC). Základní procedury HDLC mohou poskytnout následující detekce chyb a opravovací mechanismy:

automatické opětovné zaslání zprávy v případě, že nebylo obdrženo potvrzení
16ti bitová rámcová zabezpečovací sekvence

Elementy podporující procedury a možnosti jsou popsány v ISO/IEC7776 s výjimkou následujících pravidel:

Užívají se pouze single link procedury.

V každém B/BM kanálu je použitý nezávislý HDLC protokol.

V případě souběžných žádostí o datové přenosy (jeden I rámec a jeden UI rámec), musí být UI rámec přenesen s vyšší prioritou.

Nevyžádané DM není použito.

V případě FRMR condition link nesmí být použit reset. Přijímač FRMR může poslat DISC rámec jako odpověď (viz ISO/IEC7776).

Nevyžádaný UA rámec ve fázi přenášení informací je ignorován.

Není použit basic mode of operation.

Je použita rozšířená posloupnost číslování (modulo 128).

Volající systém hraje roli DTE a volaný systém DCE. Systém jež začne navazovat B/BM kanál je považován za volající systém.

Koncový systém DTE je zodpovědný za navázání a ukončení spojení vrstev 2. Jen koncový systém DTE má povoleno poslat SABME rámce. Nicméně jiný systém může také ukončit spojení.

V případě přikázaného ukončení spojení, může být ukončeno spojení vrstvy 2 před B/BM kanálem.

Vyplnění času mezi snímky může být „mark“.

Vrstva 2 nevloží žádnou výplň v čase mezi bajty (ISO4335 §4.1.4.2).

Bude užívána pouze kontrol escape transparency (ISO/IEC7776 §3.5.2.2).

Pořadí přenášených bitů v každém oktetu v poli informací: nejprve se přenese nejméně signifikantní bit.

Odpovídající I rámec může být poslán pouze s F=1. Odpovědní I rámec s F=0 nebude poslán.

SREJ může být poslán pouze jako odpovídající rámec.

UI rámec může být poslán jako příkaz i jako odpověď, to přijímač nekontroluje. Přijímač nekontroluje P/F bit, který může být nastaven na 1 či 0.

A.2.3 Síťová vrstva

A.2.3.1 Koordinační funkce

Koordinační funkce posykuje synchronizační mechanismus potřebný k součinnosti protocol stacku B/Bm kanálu a signalizačního protocol stacku.

Koordinační funkcí budou vykonány následující funkce:

- Registrace s žádanou/příslušnou sítí GSM PLMN.
- Navázání síťového spojení prostřednictvím GSM 07.07 a ETS300102 signalizačního protokolu.
- Přiřazení požadovaných QoS parametrů do signalizační informace.
- Odmítnutí spojení, je-li použito.
- Ukončení spojení pomocí GSM07.07 a ETS300102 signalizačních protokolů.
- Zpracování informací doplňkových služeb GSM/ISDN.
- Hlášení chyb a získávání informací o důvodech chyb ze GSM07.07 a ETS300102 signalizačních protokolů.
- Odpojení linkové vrstvy následované ukončením fyzického spojení v případě fáze odpojení (například když počet pokusů o opětovné zaslání převýší N2, nebo v případě detekované FRMR podmínky).

Když je ustaveno vrstvou 1 B/BM channel spojení, koordinační funkce informuje entitu linkové vrstvy B/BM kanálu a entitu síťové vrstvy B/Bm kanálu. Entita linkové vrstvy poskytuje synchronizaci s jeho peer entitou linkové vrstvy a informuje entitu síťové vrstvy o úspěšné synchronizaci.

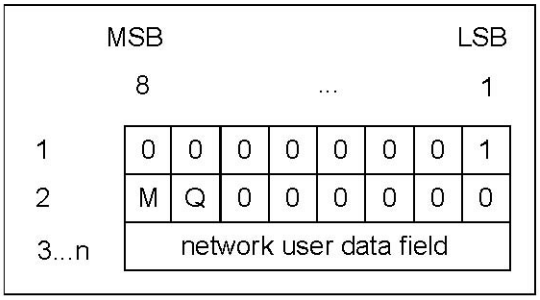
Každý RCS musí obsluhovat jeden či více B/Bm kanálů s peer RCS. Entity vrstvy 2 a 3 jsou zpracovány nezávisle v každém B/Bm kanálu.

Když je přijat N-DISCONNECT.request, B/BM kanál je přerušen dle GSM 07.07 a ETS300102.

A.2.3.2 Síťová vrstva B/Bm kanálu

Dle referenčního modelu síťové vrstvy OSI B/Bm kanálu, poskytuje funkční a procedurální prostředky k navázání, udržení a ukončení síťového spojení mezi otevřenými systémy, které obsahují komunikující transportní entity nezávislé na směrování.

Pro vrstvu 3 v B/Bm kanálu bude použito protokolu síťové vrstvy T.70 pro CSPDN. Je použita pouze hlavička T.70: Segmentace/skládání NSDU z/do sekvence NPDU a nastavování M-bitu.



Obr.23 Formát NPDU

Je-li nastaven do „1“ příznak M (More data mark), signalizuje, že budou následovat další data. Q-bit je rezervová, jeho současná hodnota je „0“.

Poznámka: Obsluha chyb v hlavičce T.70 je věcí implementace.

A.2.4 Transportní vrstva

A.2.4.1 Funkce

Transportní vrstva pouze ustavuje přenosové spojení, jestliže existuje síťové spojení. Když síťové spojení neexistuje v ten okamžik, kdy je požadováno spojení, přenosová entita nejprve zažádá o navázání takového spojení a poté automaticky zřídí přenosové spojení. Každý odlišný aplikační typ by měl navázat své vlastní přenosové spojení na zamýšlenou dobu komunikace. TP2 bude užit k tomu, aby poskytoval více než jedno přenosové spojení v rámci jednoho síťového spojení.

Tab.36 Elementy procedury TP2

Mechanismus protokolu	X.224 Cross-ref.	Varianta nebo možnost	TP Class 2	Použito	Nepoužito
Přidělení síťového spojení	6.1.1		x	*	
TPDU přenos	6.2		x	*	
Segmentace a spojování	6.3		x	*	
Zřetězení a separace	6.4		x		*
Navázání spojení	6.5		x	*	
Odmítnutí spojení	6.6		x	*	
Normální ukončení	6.7	Explicitní	x	*	
Chybové ukončení	6.8		x	*	
Asociace TPDU s přenosovým spojením	6.9		x	*	
Číslování TPDU	6.10	Normální Rozšířené	m (Pozn.1) o (Pozn.1)	*	*
Urychlený přenos dat	6.11	„Network Expedited“	x (Pozn.1)		*
Opětovné přidělení po selhání	6.12		na		*
Registrace příjmu a potvrzení TPDU	6.13	Potvrzení příjmu	na		*
Opětovná synchronizace	6.14		na		*
Multiplexování a de-multiplexování	6.15		x (Pozn.2)	(Pozn.3)	*
Explicitní řízení toku	6.16		m	*	

Mechanismus protokolu	X.224 Cross-ref.	Varianta nebo možnost	TP Class 2	Použito	Nepoužito
Kontrolní součet	6.17		x		*
Zmrazená reference	6.18				*
Opětovný přenos při překročení času	6.19		na		*
Opětovné skládání	6.20		na		*
Kontrola nečinnosti	6.21		na		*
Ošetření chyb protokolu	6.22		x	*	
Štěpení a rekombinace	6.23				*

POZNÁMKY

X Procedura vždy zahrnuta v class 2.

na Nepoužito v TP class 2.

m Sjednávací procedura jejíž implementace ve vybavení je povinná.

o Sjednávací procedura jejíž implementace ve vybavení je volitelná.

1 Nepoužito v class 2, když je vybráno: neužívat explicitní kontrolu toku.

2 Multiplexování může vést k degradaci QoS když se neužívá explicitní kontrola toku.

3 Volitelné. Tato volba není požadována pro ETCS level1 RIU.

A.2.4.2 Obsluha priorit

Priorita může být řízena:

1) Během fáze navazování fyzického spojení (eMLPP prority): Doplňková služba GSM phase 2+ „Enhanced Multi-level Precedence“ a „Per-emption service“ (GSM 02.67) poskytuje různé úrovně priority pro navázání volání a pro kontinuitu volání. GSM PLMN operátor přiděluje „set-up classes“ a „capabilities pre-emption“ každé úrovni priority dle specifikací dráhy (EIRENE SRS). Priorita je požadována během navazování fyzického spojení koordinační funkcí. Úroveň priority 1 (control-command safety) bude užita pro veškeré aplikační typy.
2) Plánovacím algoritmem během multiplexování (transport priority): Priorita přenosu je pro různé aplikační typy různá.

Poznámka: Veškeré ovládání priority přenosové vrstvy se odkazují na přenosové priority.

Akce vykonané přenosovým protokolem během doby trvání spojení nejsou explicitně definovány v X.224.

Při požadavku na navázání přenosového spojení má být přijat následující postup v každém CFM:

Jsou-li vhodné zdroje pro poskytnutí služby (v místním i vzdáleném systému) bude ustaveno nové spojení.

Jinak bude požadavek na spojení odmítnut.

Řízení přenosové priority během fáze dat přenosového spojení je popsáno v následující části.

A.2.4.3 Multiplexování

Multiplexování dvou či více přenosových spojení na jedno síťové spojení může být poskytnuto volitelně. Tato volba není požadována pro ETCS level 1 RIU.

Multiplexování vyžaduje následující funkce:

Identifikace přepravního zdroje je poskytnuto příslušným DST-REF parametrem každé DT PDU a dodatečně SRC-REF parametrem CR, CC, DR a DC TPDUs. Tyto parametry jsou použity k identifikaci každé TPDU v daném přenosovém spojení a zajistí, že data z odlišných přenosových spojení se nesmíchají, nebo nejsou chybně směrována.

Peer kontrola toku reguluje rychlost se kterou jsou TPDUs, jednotlivých přenosových spojení, posílána peer přenosové entitě. Použití jednoznačné kontroly toku v každém přenosovém spojení bude přizpůsobeno dle doporučení X.224 podsekce 10.2.4.2 a bude použito k formě kontroly toku vykonávané v nižších vrstvách.

Plánování dalšího přenosového spojení bude obslouženo přes síťové spojení: Spojení přidružené k aplikačnímu typu ATP musí být obslouženo přednostně (první).

Transport connection endpoint identifier (TCEPID) v TSAP poskytuje místní identifikaci přenosového spojení. Kontrola toku informací rozhraním je poskytnuta jako věc implementace. Tyto místní mechanismy řízení toku budou souhlasit s požadavky přenosové priority.

A.2.4.4 Ukončení síťového spojení

Ukončení síťového spojení nastává když jsou ukončena všechna přenosová spojení přidružená k tomuto síťovému spojení.

V případě nenormálního ukončení sítí, jsou veškerá přidružená přenosová spojení ukončena a uživatelé služeb jsou ihned informováni.

A.2.4.5 Segmentace/Reassembling

Je-li velikost transport service data unit (TSDU), která je požadována k přenesení do přenosové vrstvy, větší než maximální velikost uživatelských dat DT TPDU, musí být vykonáno nejprve rozdělení TSDU. Jedna TSDU je přiřazena více než jednomu TPDU s přidanou informací (protocol control information).

Segmentace/reassembling snižuje výkonnost, protože zvyšuje režii TPDU. Data s normální prioritou jsou segmentována, když se nevejdou do jednoho TPDU. Doporučená délka TSDU je ≤ 123 oktetů.

Vysílající přenosová entita by měla použít délku 128 oktetů pro všechny TPDU mimo poslední.

Peer přenosová entita musí identifikovat přenosové spojení přijímaných segmentů a opětovně je sloučit do TSDU.

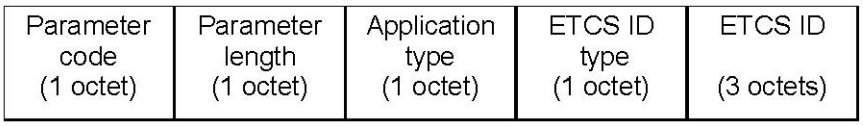
Přijímající přenosová entita bude schopná přijmout TPDU různé délky: od 1 do 128 bajtů.

Jestliže jeden TPDU (jež požaduje přenos k síťové vrstvě jako NSDU) je ovládán síťovou entitou, další TPDU musí čekat. Segmentace long lower priority TSDU poskytuje možnost multiplexovat TPDUs vyšší priority s tokem segmentů TSDU nižší priority.

ConnectRequest TPDU (CR TPDU) a ConnectConfirm TPDU (CC TPDU) obsahuje informaci o adrese: volající přenosový selektor a volaný přenosový selektor, nebo

odpovídající přenosový selektor v příslušných TSAP IDs. Přenosový selektor obsahuje sub-parametr aplikační typ, typ ETCS ID a ETCS ID (obr.24 a tab.37).

Poznámka: Kód parametru a délka je zachycena na obr. 24 – ukazuje strukturu dle X.224 část 13.3.4.



Obr.24 Struktura přenosového selektoru

První oktet přenosového selektoru je použit pro určení aplikačního typu (tab.37). Prvních 5 bitů specifikuje hlavní aplikační typ. Doplňující aplikační typy specifikují hlavní aplikační typy podrobněji. Každý hlavní aplikační typ může obsahovat 8 aplikací. Struktura parametru „typ aplikace“ je: main application type (5b) + minor application type (3b).

Aplikační typ volajícího a volaného přenosového selektoru musí být identické. Když volaný CFM nepodporuje požadovaný aplikační typ, požadavek navázání spojení bude odmítnut DR TPDU.

Tab.37 Formát a kódování přenosového selektoru

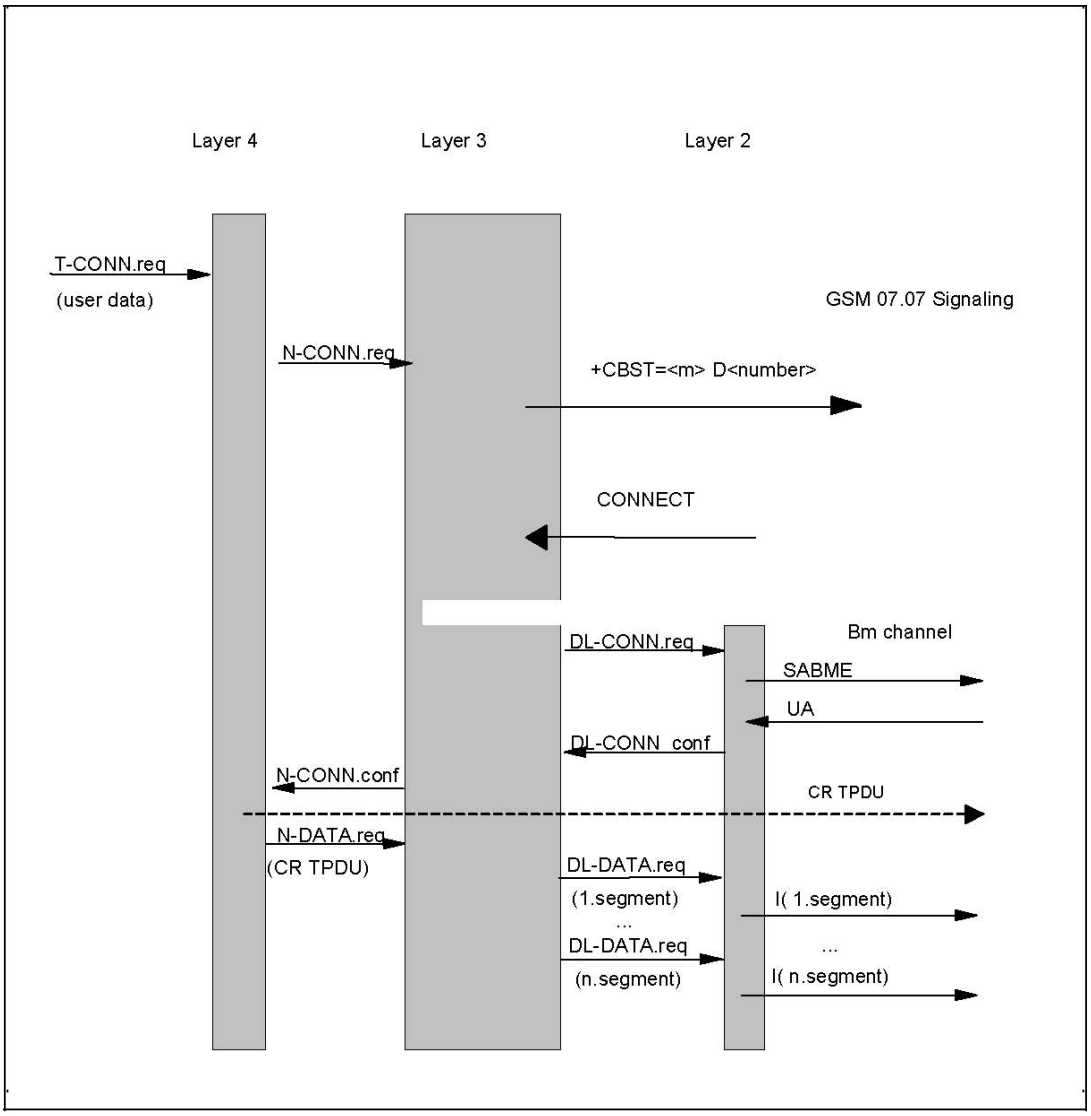
Oktet	Bit 8765 4321	**Obsah**
1	1100 0001 1100 0010	Kód parametru volající TSAP, nebo Kód parametru volané TSAP
2	0000 0101	Délka parametru (pevná délka=5)
3	xxxx xxxx	Aplikační typ[1]
	0001 0xxx 0001 0000 0001 0001 0001 0111	ATP ERTMS/ETCS level 2/3 ERTMS/ETCS level 1 K národnímu použití[2]
	0001 1xxx 0001 1010 0001 1011 0001 1100	Národní použití pro traťové vybavení RBC-Ostatní stacionární zab. zař. komunikace RBC-RBC komunikace Ostatní stacionární zab. zař. - Ostatní stacionární zab. zař. komunikace
	0010 0xxx 0010 0000 0010 0001	Key management KMC/KMC komunikace KM domain internal komunikace
	1111 1111	Rezervováno pro řízení chyb
4	 0000 0000 0000 0001 0000 0010 0000 0011 0000 0100 0000 0101 0000 0110 1111 1111	ETCS ID typ RIU RBC Pohon Rezervováno pro balízu – nepožadováno pro Class1 Rezervováno pro úsekový element (úrovňové křížení, ...) – nepožadováno pro Class1 Entita key managementu Entita stacionární zab. zař. (stavědla) Neznámý 3
Oktet	Bit 8765 4321	**Obsah**

5-7		ETCS ID
POZNÁMKA: 1. Aplikační typ ATP je povinný. Všechny ostatní hodnoty aplikačních typů jsou rezervovány. 2. Doplňující aplikační typ k národnímu použití je rezervován pro národní aplikace. 3. Může být použit pouze s hodnotou ETCS ID "neznámý".		

A.2.5 Časové posloupnosti

Časové sekvence jsou ukázány v příslušných standardech služeb vrstev dle OSI (např. pro vrstvu 4 viz X.214). Tato kapitola ilustruje interakci vrstev.

Obr.25 ukazuje pouze navázání spojení traťovým RCS. Signalizační spojení mezi RCS a mobilní stanicí je navázáno po "zapnutí" (power-on) mobilní stanice. Toto spojení poskytuje "radio-zdroje" a mobilní management.



Obr.25 Detailní sekvence protokolu během navázání spojení (pouze požadující strana)

Poznámka: Nižší část obr.25 ukazuje segmentaci CR TPDU z důvodu velikosti TPDU (TPDU > 123 bajty).

A.2.6 Závislosti PDU a SDU

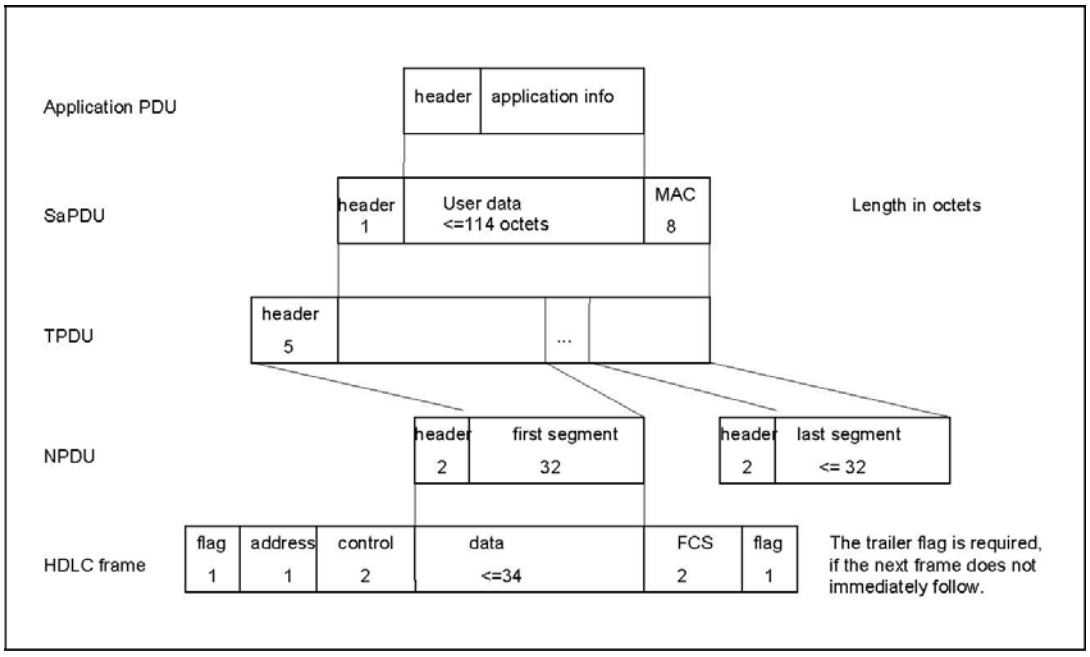
Tato kapitola obsahuje příklady režie vrstvy při zpracování 25 bajtového datového pole HDLC rámce.

Je-li použita bezpečná vrstva, přidá hlavičku a MAC k uživatelským datům.

Přenosové spojení je multiplexováno na síťové spojení podle přenosové priority. Vrstva 4 přidá k uživatelským datům hlavičku.

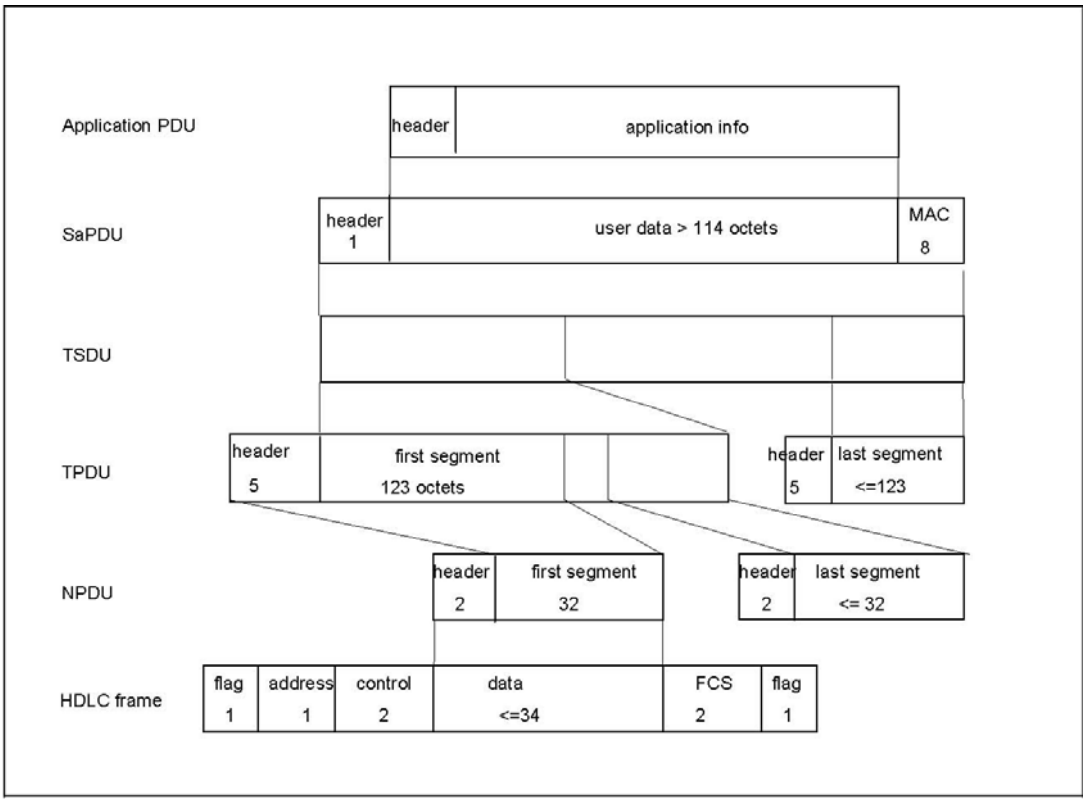
Když TS uživatel poskytne TSDU data s normální prioritou vhodné délky (<= 123 oktetů), vrstva 4 nedělí/neskládá uživatelská data (obr.26). Dělení a skládání ve vrstvě 3 má za následek dvoubajtovou adresu segmentu.

V případě nikoli-bezpečného spojení je obr.26 stále platný, ale bez druhého řádku (SaPDU).

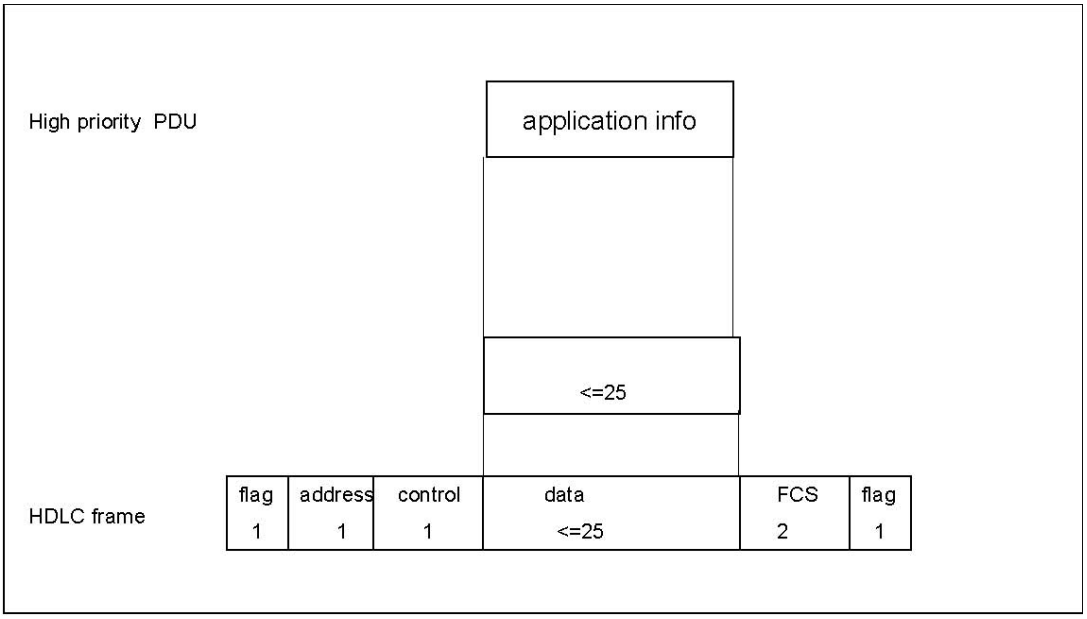


Obr.26 Příklad segmentace/reassemblingu ve vrstvě 3

Neposkytne-li TS uživatel TSDU data normální priority vhodné délky, vrstva 4 rozdělí/složí uživatelská data do/z TPDUs standardní délky 128 bajtů. Dělení a skládání vrstvou 4 má za následek 5 bajtovou hlavičku přidanou ke každému segmentu (obr.27). Hlavička vrstvy 3 je dodatečně požadována, aby bylo dosaženo shody s formátem NPDU dalších spojení.



Obr.27 Příklad segmentace/reassemblingu ve vrstvě 4 a vrstvě 3



Obr.28 Příklad režie vrstvy vysoce prioritních dat

A.3 Řízení CFM

A.3.1 Volání a ID-management

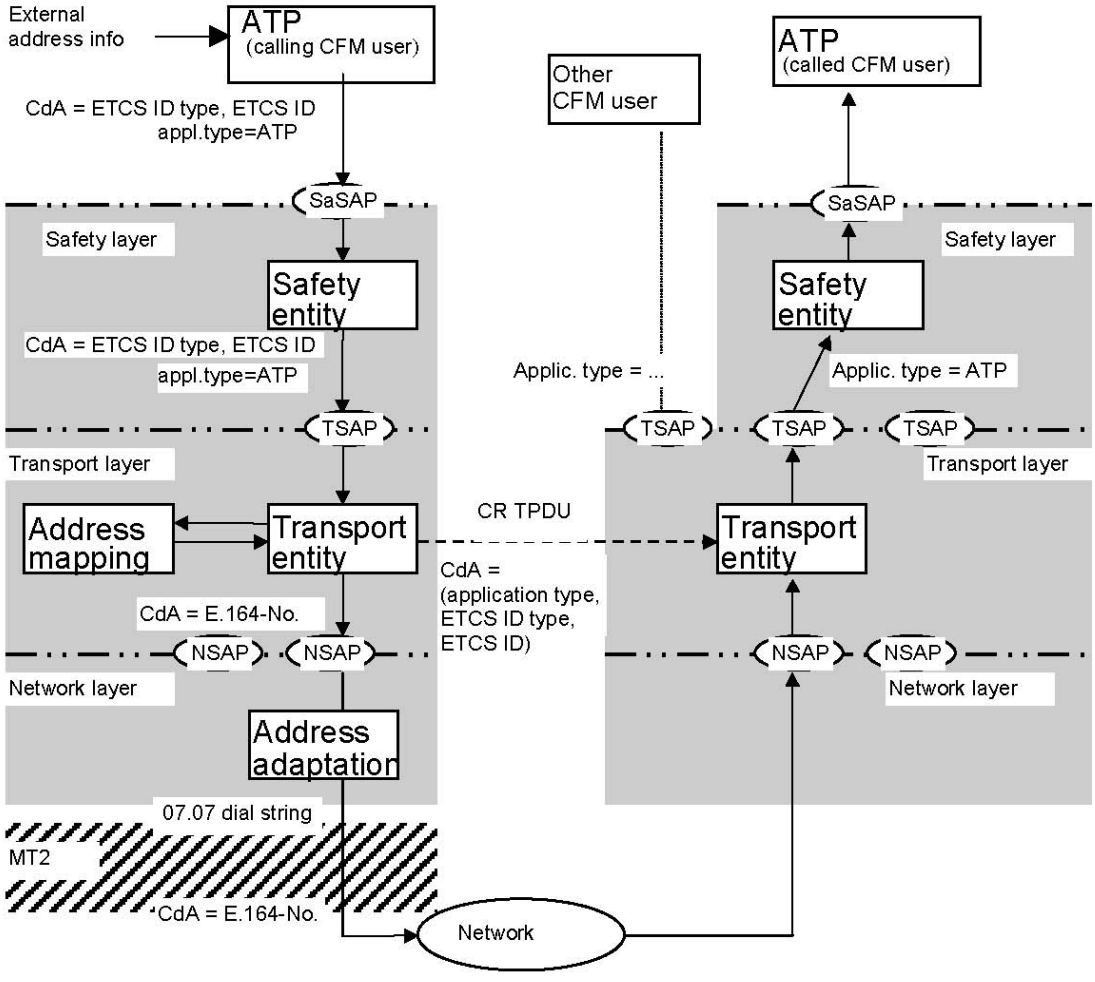
CFM musí navázat spojení na požádání peer aplikací (tj. CFM uživatele). Detaily následujících úkolů jsou věcí implementace.

RCS CFM volitelně nabízí několik logických spojení mezi traťovým a palubním vybavením skrze stejný fyzický kanál. Tato volba není požadována ETCS level 1 RIU.

"Přenosová adresa" je obecné pojmenování, jež je použito pro identifikaci skupiny TSAPs, které jsou umístěny na rozhraní mezi vyšší a přenosovou vrstvou CFM.

Přenosová adresa je použita pro zpřístupnění jediné transportní služby (TS) uživatelské entity. Síťová adresa sama o sobě není dostatečná k identifikaci jedné CFM uživatelské entity. Je nezbytné použít speciální identifikátor či kvantifikátor adresy, pro označení požadované uživatelské entity CFM: aplikační typ.

Entity přenosových vrstev a entity CFM uživatelů jsou spolu vázány v TSAP-ech. Každá entita CFM uživatele je vázaná na jeden či více TSAP-ů. Toto je věcí implementace. Neexistuje žádná závislost mezi TSAP-y a multiplexováním. Multiplexované přenosové spojení může končit v různých TSAP-ech.



Obr.29 Příklad mapování adresy

Adresy jsou použity v T-CONNECT (přenosová adresa) a N-CONNECT (síťová adresa) v rozhraní služby. Když entita CFM uživatele (např. entita bezpečné vrstvy) chce navázat spojení s jinou entitou CFM uživatele, poskytne informaci k tomu, aby určila volaného CFM uživatele (např. typ ETCS ID, ETCS ID) a aplikační typ. Tato adresa musí být mapována do formátu a struktury požadované CFM pro navázání spojení.

Obr.29 ukazuje příklad mapování informace o adrese během navazování spojení vlakovým CFM směrem k traťovému CFM. Volající entita TS uživatele (např. v tomto případě entita bezpečné vrstvy) získává volanou přenosovou adresu od aplikace (typ ETCS ID a ETCS ID). Informace o adrese prochází skrze SFM směrem k CFM.

Volající CFM má následující úkoly:

1) Zkontrolovat, že je mobilní stanice přihlášena do mobilní sítě obsažené v T-CONNECT.request.
2) Přiřadit požadované spojení příslušné mobilní stanici.
3) Odvodit volanou síťovou adresu z informace o adrese, která označuje volaného CFM uživatele.
4) Vložit do žádosti o spojení (CR) TPDU volaný transport selektor (v případě, že vlak zahájil navazování fyzického spojení) a volající transport selektor.
5) Vybrat místní NSAP, kterým budou poskytovány síťové základní operace služby (jsou-li použity.

Následující pravidla jsou použita k odvození volané síťové adresy v případě, že vlak zahájil navazování fyzického spojení:

Jestliže T-CONNECT.request obsahuje síťovou adresu, tato adresa musí být použita pro navázání fyzického spojení. Síťová adresa je pro CFM transparentní.

Neobsahuje-li T-CONNECT.request síťovou adresu, nebo typ ETCS ID a ETCS ID, či v případě chyby mapování, volání musí být spojení navázáno s nevíce vhodnou RBC prostřednictvím krátkého volajícího kódu (viz. EIRENE SRS).

V případě, že RBC zahájila navazování fyzického spojení, ETCS ID palubního vybavení, poskytnuté T-CONNECT.request bude mapováno na volanou síťovou adresu (tj. MSISDN).

Poznámka: Detaily místního volání a ID managementu (např. mapování adres) jsou mimo rozsah specifikací Euroradio. Podrobnosti v EURORADIO FFFIS a SUBSETu 040.

Tab.38 ukazuje definované kombinace hodnot informace o adrese.

Tab.38 Informace o adrese (vlak iniciuje spojení)

typ ETCS ID	ETCS ID	Síťová adresa	Akce	Poznámky
RBC	RBC ID	RBC síťová adresa poskytnuta	Použití síťové adresy	
RBC	RBC ID	Síťová adresa neposkytnuta, nebo Standardní hodnota ”NA unknown”	Použití krátkého volacího kódu “Nejvhodnější RBC”	Kód krátkého volání 15xx [EIRENE SRS]
“neznámý”	Standardní hodnota ”RBC unknown”	Síťová adresa neposkytnuta, nebo Standardní hodnota ”NA unknown”	Použití krátkého volacího kódu ”Přesměrování k nejvíce vhodné RBC”	Implicitní pro adresování

CR TPDU a CC TPDU obsahuje volající a volaný transport selektor ve formátu specifikovaném pro TPDUs.

Síťová adresa volané traťové části je všeobecnou adresou pro identifikaci skupiny NSAPs, které jsou vázány na „primary rate access" (sítě jako ISDN). Volané síťové číslo by mělo být „hunting number": příchozí volání síťového čísla bude distribuováno „terminating exchange" mezi skupinu rozhraní. Jedno z nečinných rozhraní bude vybráno pro příjem volání.

Skupiny TSAPs traťové části jsou vázány speciálními entitami CFM uživatelů. Entita CFM uživatele A je vázána na TSAP ale aktuálně není použita (možná je to nikoli-bezpečná entita aplikační vrstvy, která musí používat další TSAP a aplikační typ).

Entita přenosové vrstvy ve volaném CFM používá:

Informaci o adrese obsaženou v CR TPDU k odvození volaného typu ETCS a ETCS ID a k výběru jednoho vhodného TSAP (na základě přijatého aplikačního typu).

Odpovídající typ ETCS ID a ETCS ID obsažené v T-CONNECT.response ke generováni CC TPDU.

Není-li entita přenosové služby volané strany schopna vybrat TSAP vázaný na požadovaný aplikační typ, bude CR TPDU odmítnuto.

A.3.2 Konfigurační management

Místní stack O&M poskytuje počáteční soubor konfiguračních parametrů. Tento soubor může být nastaven během výroby. Existuje-li více než jeden standardní soubor, může být vybrán prioritně jeden z nich akcí místního managementu, založenou na národních směrnicích železnice. Všechny tyto akce off-line managementu jsou mimo rozsah této práce.

Konfigurační parametry

Tab.39 Konfigurační parametry vrstvy 2*

Parametr	Symbol	Definovaný rozsah hodnot	Použitá hodnota(y)	Poznámky
Adresa		A, B	Volající entita: A Volaná entita: B	
Velikost okna	k	1 - 127	9 - 61	Velikost okna může být rozdílná v obou směrech. Doporučená hodnota = 20
Čas "na odpověď"	T1	> 500 ms	0,8 - 2 s	T1>T2+2*přenosové zpoždění
Zpoždění místním zpracováním	T2		< 80 ms	Závisí na implementaci.
Čas "mimo provoz"	T3		T3 >> T4	Je věcí implementace (bude užito pouze je-li podporován T4)
Čas "neaktivity"	T4		Doporučená hodnota T4 >N2 * T1	T4 >> T1 Je věcí implementace.
Maximální počet bitů v I rámci	N1	> 0	240≤N1≤1024.	Nejsou zahrnuty příznaky. Přijímající zásobník podporuje N1 =1024. Doporučená hodnota pro vysílání = 312 (odpovídá 4 rámcům na 1 TPDU)

Parametr	Symbol	Definovaný rozsah hodnot	Použitá hodnota(y)	Poznámky
Maximální počet pokusů o opětovné poslání	N2	> 0	3 – 6.	Poznámka: ISO/IEC 7776 specifikuje počet přenosů = N2+1 Doporučená hodnota: 5
Detekce a oprava chyb			FCS-16	Žádné volby

* Všechny doporučené hodnoty v této tabulce mohou být optimalizovány (např. s ohledem na trakční charakteristiky, průmyslové/venkovské lokality atd.)

Popis konfiguračních parametrů vrstvy 2 poskytuje ISO/IEC7776 oddíl 5.7.

Časovač T5 nebude použit.

Tab.40 Konfigurační parametry vrstvy 3

Parametr	Symbol		Použitá hodnota	Poznámky
Maximální počet bajtů v rámci	N_{L3seg}		N_{L3seg}=(N1/8)-5	Hlavička vrstvy 3 je zahrnuta. N_{L3seg} souvisí s délkou rámců N1 vrstvy 2

Popis konfiguračních parametrů vrstvy 3 je uveden v T.70.

Tab.41 Konfigurační parametry vrstvy 4

Parametr	Symbol	Rozsah hodnot	Použitá hodnota	Poznámky
Třída TP	TP x		TP 2	
Elementy procedury				Viz tab.36
Standardní délka TPDU	N_{TPDU}	1 - 128 bajtů	128 bajtů	
Initial credit	N_{TIC}	1 – 15	15 1	Aplikační typ = ATP Všechny ostatní aplikační typy

Popis konfiguračních parametrů vrstvy 4 poskytuje X.224.

A.3.3 QoS parametry

Běžně, dávají QoS parametry CFM uživatelům metodu specifikování jejich potřeb a dávají CFM základy pro výběr protokolu, nebo požadování služeb nižších vrstev. Pro náš účel jsou specifikovány soubory hodnot QoS parametrů.

Každá hodnota parametru třídy QoS je přidružena k souboru hodnot QoS parametrů, které reprezentují požadavky na fyzické spojení, jež má být navázáno. Požadavky nejsou závislé na aplikačním typu.

Základní hodnota QoS parametru USER DATA RATE je 4800bit/s.

Rozsah QoS parametru transportní priorita je 0-5. Tab.42 ukazuje asociaci s aplikačními typy.

Tab.42 Transportní priorita

Hodnota	Přidružený aplikační typ	Poznámky
0	-	Není použita
1	Aplikační typ ATP	Použita nejvyšší hodnota
Všechny ostatní hodnoty jsou rezervovány.		

Třídy QoS 0-9 jsou rezervovány pro aplikační typ ATP ERTMS/ETCS. Parametry data rate a eMLPP priorita budou požity během navazování spojení.

Tab.43 Mapování QoS tříd 0- 9

Třída QoS	Data rate [bit/s]	eMLPP priorita
0	9 600	1
1	4 800	1
2	2 400	1
Všechny ostatní hodnoty třídy QoS jsou rezervovány pro budoucí využití.		

A.3.4 Dohled / diagnostika

A.3.4.1 Ošetření chyb

Nastane-li chyba v CFM, nebo když CFM přijme hlášení o chybě, bude signalizována chyba a její příčina. Různé příčiny vyžadují různé akce pro jejich ošetření. Chyby mohou být ignorovány, místně ignorovány, nebo signalizovány.

Nastane-li problém s navazováním spojení, CFM by se měl sám o sobě pokusit vyřešit problém. Pouze nemůže-li být problém vyřešen (tj. přenosové spojení nemůže být navázáno), CFM informuje CFM uživatele.

Tab.44 Typy chyb CFM a opatření

Reason / kód	Sub-reason		Akce ošetřující chybu
Chyba sítě Kód =1	1 2 3	Číslo není přiřazeno či neplatný formát čísla. Neakceptovatelný kanál. Nemožnost navázat fyzické spojení z jiného důvodu. (např. odpověď V.25 NO DIALTONE)	Indikace trvalé chyby je vytvořena poskytovatelem a je obsažena v parametru reason T-DISCONNECT.indication
Síťové zdroje nejsou dostupné Kód =2	1 2 3	Žádný kanál k dispozici Přetížení sítě Jiný důvod. (např. odpověď V.25 NO CARRIER)	Indikace přechodné poruchy je vytvořena poskytovatelem a je obsažena v parametru reason T-DISCONNECT.indication.
Služba nebo volba není dočasně dostupná Kód =3	1 2	QoS není k dispozici Přenosová kapacita není k dispozici	Indikace přechodné poruchy je vytvořena poskytovatelem a je obsažena v parametru reason T-DISCONNECT.indication
Neznámý důvod Kód =5			Indikace chyby je vytvořena volaným CFM a je obsažena v parametru reason T-DISCONNECT.indication.
Volaný TS uživatel není k dispozici Kód =6	1 2 3	Aplikace požadovaného typu není k dispozici Volaný uživatel neznámý (např. odpověď V.25 NO ANSWER) Volaný uživatel není k dispozici (např. odpověď V.25 BUSY)	Indikace chyby je vytvořena volaným CFM a je obsažena v uživatelských datech DR TPDU. Volající CFM oznámí chybu volající aplikaci pomocí T-DISCONNECT.indication

Reason / kód	Sub-reason		Akce ošetřující chybu
Vnitřní chyba Kód =7	1 2 3	Hlavní element místní aplikace chybí (např. element TS základní operace) Nevhodný stav Ostatní sub-důvody (např. odpověď V.25 ERROR)	Záznam chyby. Vymazání neplatné zprávy.
1	8	Žádné mobilní stanice nebyly registrovány	T-DISCONNECT.indication Aplikace by měla opětovně zkusit síťovou registraci
Poznámky: 1. Všechny ostatní reasons / sub- reasons jsou rezervovány. 2. Reasons / sub- reasons jsou věcí implementace. 3. Reason kód 0 je rezervován pro běžné ukončení požadované CFM uživatelem.			

A.3.5.1 Hlášení chyb

SFM a/nebo aplikace jsou informovány o chybových situacích, vedoucích k odpojení použitím T-DISCONNECT.indication.

Tab.45 Parametr T-DISCONNECT a její obsah

Parametr T-DISCONNECT	Obsah
Důvod	TS uživatel „invoked“ / TS poskytovatel „invoked“ V případě odpojení TS poskytovatelem: typ chyby/sub-reason (viz. tab.45)
Uživatelská data	Uživatelská data DISCONNECT.request vzdáleného TS uživatele (vnitřní informace od vzdáleného TS uživatele)

A.3.6.1 Záznam chyb

Záznam chyb je věcí implementace.

Příloha B: ROZHRANÍ KE KOMUNIKAČNÍM SLUŽBÁM (volitelné)

Tato práce se rozhraním zabývá pouze velmi okrajově z informačních důvodů, proto je tato část vložena jako příloha.

Komunikační služby jsou přístupné prostřednictvím základních operací služeb podobných základním operacím služeb definovaných v X.214 pro „connection mode service“.

Poznámka: Je věcí implementace přizpůsobit toto rozhraní požadavkům a omezením, kde se data nepřenáší vzdušnou cestou a kde nemá dopad na chování systému.

Požadavky Class1: Vnitřní rozhraní mezi SFM a CFM není povinné.

Rozhraní ke komunikačním službám může být poskytnuto i nikoli bezpečným aplikacím.

B.1 Základní operace služby pro navázání spojení

Následující tabulka ukazuje základní operace služby použité pro navázání spojení a jejich parametry.

Tab.46 Základní operace služby komunikační vrstvy pro navázání spojení

Parametry	T-CONNECT request	T-CONNECT indication	T-CONNECT response	T-CONNECT confirm
TCEPID		X	X(=)	X
Volaná adresa • Typ adresy • Síťová adresa • ID mobilní sítě • Volaný typ ETCS ID • Volané ETCS ID	 X X(D) X(U) X X	 X X		
Volající adresa • Volající typ ETCS ID • Volající ETCS ID	 X X	 X(=) X(=)		
Odpovídající adresa • Odpovídající typ ETCS ID • Odpovídající ETCS ID			 X X	 X(=) X(=)
Typ aplikace	X	X(=)		
Třída QoS	X(D)			
Uživatelská data	X(U)	X(=)	X(U)	X(=)

X Povinný parametr.

(=) Hodnota parametru je stejná jako hodnota korespondujícího parametru předchozí základní transportní operace.

X(U) Použití tohoto parametru je pro CFM volitelné.

X(D) Použití tohoto parametru je volitelné. Není-li poskytnut, CFM použije defaultní hodnotu.

Parametr TCEPID je místně poskytován k rozlišení různých transportních spojení.

Typ adresy kvalifikuje použití dalších parametrů volané adresy (viz příslušná sekce).

ID mobilní sítě identifikuje mobilní síť. ID mobilní sítě může obsahovat kód země a kód mobilní sítě, dle ITU-T E.212.

V případě, že navazování spojení zahájila mobilní strana, požadavek na spojení bude obsahovat parametr ID mobilní sítě, k vyžádání vhodné sítě spojené s volaným uživatelem.

Síťová adresa (jestliže je poskytnuta) identifikuje adresu volaného CFM uživatele. Tento parametr je složen z dílčích parametrů: délka volaného čísla, typ čísla, „numbering plan“ a samotného čísla.

Parametr typ ETCS ID společně s parametrem ETCS ID jsou jedinečné v rozsahu ETCS. Tyto parametry jsou použity transportní vrstvou během navazování spojení.

Parametry typ ETCS ID, ETCS ID a typ aplikace identifikuje uživatele služeb.

Volající ETCS ID společně s typem aplikace identifikuje iniciátora transportního spojení. Parametry volané ETCS ID a typ aplikace identifikuje volaného CFM uživatele.

Velikost uživatelských dat je omezena na 32 oktetů.

B.2 Základní operace služby pro přenos dat

Následující tabulka ukazuje základní operace služby komunikační vrstvy použité pro přenos dat.

Tab.47 Základní operace služby komunikační vrstvy pro přenos dat

Parametry	T-DATA.request	T-DATA.indication
TCEPID	X	X
Uživatelská data	X	X(=)

Požadavek na přenos dat je vyslán uživatelem (po navázání transportního spojení) použitím T-DATA.request s uživatelskými daty jako parametrem. Tyto data jsou doručena odpovídajícímu uživateli prostřednictvím T-DATA.indication s uživatelskými daty jako parametrem.

Uživatelská data jsou pro CFM transparentní. Doporučená délka je ≤ 123 oktetů. Jestliže je větší než 123 oktetů CFM rozdělí/složí uživatelská data.

B.3 Základní operace služby pro přenos HP dat

Přenos HP dat je přípustný pouze pro aplikační typ ATP.

Následující tabulka zachycuje základní operace služby komunikační vrstvy pro přenos HP dat.

Tab.48 Základní operace služby komunikační vrstvy pro přenos HP dat

Parametry	T-HP-DATA.request	T-HP-DATA.indication
TCEPID	X	X
Uživatelská data	X	X(=)

Žádost o přenos HP dat je vyslána uživatelem (po navázání transportního spojení) použitím T-HP-DATA.request s uživatelskými daty jako parametrem. Tyto data jsou doručena odpovídajícímu uživateli prostřednictvím T-HP-DATA.indication s uživatelskými daty jako parametrem.

Velikost uživatelských dat je omezena na délku datového pole UI rámce (v současnosti nejvíce 25 oktetů).

B.4 Základní operace služby pro ukončení spojení

Ukončení přenosového spojení je realizováno prostřednictvím T-DISCONNECT.request. Ukončení spojení je indikováno uživateli pomocí T-DISCONNECT.indication. Ukončení spojení je uživateli indikováno jako důsledek požadavku na zrušení spojení od uživatele (normální stav), jako důsledek odmítnutí navázání spojení, nebo jako důsledek chyby sítě.

Následující tabulka ukazuje základní operace služby pro ukončení spojení.

Tab.49 Základní operace služby komunikační vrstvy pro ukončení spojení

Parametry	T-DISCONNECT.request	T-DISCONNECT.indication
TCEPID	X	X
Důvod		X(U)[1]
Uživatelská data	X(U)	X(=)
Poznámka: 1 Musí být použito v případě chyby.		

Volitelně mohou být připojena uživatelská data (maximálně 64 oktetů).

B.5 Základní operace služby pro registraci do sítě

Pro přihlášení mobilních stanic (MS) do sítě jsou použity 2 základní: žádost o přihlášení a indikace statusu přihlašování

Tyto základní operace služby jsou aplikované pouze na palubní části.

Tab.50 Základní operace služby pro přihlášení do sítě

Parametr	T-REGISTRATION.request	T-REGISTRATION.indication
Seznam MNID	X (>= 0 MNIDs)	(>= 0 MNIDs)

Seznam MNID je seznam identifikátorů mobilní sítě.

Použitím základní operace služby T-REGISTRATION.request je schopen uživatel žádat o registraci jedné, nebo více mobilních stanic do jedné, nebo více mobilních sítí.

MNID identifikuje mobilní síť do které se chce přihlásit mobilní stanice. Tento parametr se může skládat z kódu země a kódu mobilní sítě dle ITU-T E.212.

Interpretace seznamu MNID je věcí implementace - například:

1) Prázdný seznam (0 záznamů): Všechny mobilní stanice se budou přihlašovat pomocí automatické registrace do sítě (viz GSM 02.11).
2) Jeden MNID: Všechny mobilní stanice se budou přihlašovat registrací do sítě (nikoli automatickou ve smyslu automatické detekce dostupných sítí) s použitím tohoto záznamu. Přihlásí se tedy pomocí tohoto jediného záznamu.
3) Dva odlišné MNID: Mobilní stanice se může rozdělit na dvě části a přihlásit každou z těchto částí do jiné sítě. Není-li mobilní stanice schopna přihlášení do obou sítí přihlásí se do jedné z nich dle priority (např. první záznam odpovídá záznamu s vyšší prioritou).

Status přihlašování se signalizuje prostřednictvím T-REGISTRATION.indication uživateli. To obsahuje seznam MNID, do nichž je mobilní stanice registrována.

Poznámka: Asociace mezi MS a MNID v této základní operaci je věcí implementace.

Uživatel není informován kolik mobilních stanic je k dispozici, protože přijímá pouze status registrovaných sítí, což znamená, že na těchto sítích může, ale nemusí, být vydán požadavek na navázání spojení.

Je-li indikovaný seznam mobilních sítí prázdný, registrace mobilní stanice se nezdařila, nebo byl ztracen signál.

Indikace bude poskytnuta nezávisle na žádosti. Tato vlastnost dovoluje indikaci po zapnutí, nebo po ztrátě signálu. Může být indikována jakákoli změna registrace.