ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

Katedra aplikované elektroniky a telekomunikací

DIPLOMOVÁ PRÁCE

Návrh úložiště kryptografických klíčů protokolu EURORADIO pro železniční zabezpečovací zařízení

vedoucí práce: **Ing. Petr Hloušek, Ph.D.**
autor: **Bc. Pavel Šmejkal**

2012

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2011/2012**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel ŠMEJKAL**
Osobní číslo:	**E10N0168P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Dopravní elektroinženýrství a autoelektronika**
Název tématu:	**Návrh úložiště kryptografických klíčů protokolu EURORADIO pro železniční zabezpečovací zařízení**
Zadávající katedra:	**Katedra aplikované elektroniky a telekomunikací**

Zásady pro vypracování:

1. Popis vlastností protokolu EURORADIO.
2. Návrh vhodného HW a SW řešení úložiště kryptografických klíčů protokolu EURORADIO s ohledem na bezpečnostní požadavky.
3. Zhodnocení dosažených výsledků.

Rozsah grafických prací:	**dle doporučení vedoucího**
Rozsah pracovní zprávy:	**dle doporučení vedoucího**
Forma zpracování diplomové práce:	**tištěná/elektronická**
Seznam odborné literatury:	

Student si vhodnou literaturu vyhledá v dostupných pramenech podle doporučení vedoucího práce.

Vedoucí diplomové práce:	**Ing. Petr Hloušek, Ph.D.** Katedra aplikované elektroniky a telekomunikací
Konzultant diplomové práce:	**RNDr. Štěpán Klapka, Ph.D.** AŽD Praha
Datum zadání diplomové práce:	**17. října 2011**
Termín odevzdání diplomové práce:	**11. května 2012**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Dr. Ing. Vjačeslav Georgiev
vedoucí katedry

V Plzni dne 17. října 2011

Anotace

Předkládaná diplomová práce je zaměřena na popis protokolu EURORADIO, který je používán v systému ETCS. V souvislosti s protokolem EURORADIO je zde popsán jeho klíčový management. Dále jsou zde uvedeny požadavky na kryptografické moduly a následně je proveden návrh kryptografického modulu pro protokol EURORADIO.

Klíčová slova

ERTMS/ETCS, protokol EURORADIO, kryptografický modul, kryptografické klíče, bezpečnostní požadavky

Abstract

This magister thesis is focused on a proposal EURORADIO protocol, which is used in the ETCS system. In context with the EURORADIO protocol the key management is described. Furthermore the requirements on the cryptographic modules are described and a draft of the cryptographic module for EURORADIO protocol is created.

Key words

ERTMS/ETCS, EURORADIO protocol, cryptographic module, cryptographic keys, security requirements

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci, zpracovanou na závěr studia na Fakultě elektrotechnické Západočeské univerzity v Plzni.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

V Plzni dne 2.5.2012 Pavel Šmejkal

Obsah

Seznam pojmů a zkratek

AES……	(Advanced Encryption Standard) Pokročilý šifrovací standard
AR…….	(Authentication Response) Autentizační odpověď
ATC.....	(Automatic Train Control) Automatické vedení vlaku
ATP……	(Automatic Train Protection) Vlakové zabezpečovací zařízení
AU1, 2, 3……...	(Authentication message) Autentizační zpráva první, druhá a třetí
CFM……..	(Communication Funkctional Module) Komunikační funkční modul
CSP……	(Critical security parametr) Informace vztahující se k bezpečnosti
DA…….	(Destination Address) Adresa cíle
DES……...	(Data Encryption Standard) Datový šifrovací standard
DRAM……	(Dynamic Random Access Memory) Dynamická paměť s náhodným přístupem
DT……..	Data
ERTMS……...	(European Rail Traffic Management System) Evropský systém řízení železniční dopravy
ETCS……...	(European Train Control System) Evropský vlakový zabezpečovací systém
GMSK…….	(Gauss Minimal Shift Keying) Gaussovské klíčování s minimálním zdvihem
GSM……	(Global System for Mobile Communications) Globální systém pro mobilní komunikace
GSM-R……	(Global System for Mobile Communications - Railway) Globální systém pro mobilní komunikace - Železnice
HP……...	(High Priority) Vysoká priority
I&A…….	(Identification and Authentication) Identifikace a autentizace
IIC (I2C)…….....	(Inter-Integrated Circuit) Meziobvodová sběrnice
ISDN……...	(Integrated Services Digital Network) Digitální síť integrovaných služeb
K_{AB}, KMAC….....	(Authentication key) Autentizační klíč
KM……	(Key Management) Klíčový management
KMC……..	(Key Management Centre) Klíčové management centrum
KMS…….....	(Key Management System) Klíčový management systém
$K_{S,}$ KSMAC.....	(Session key) Relační klíč

KTRANS……	(Transport key) Transportní klíč
LEU…….	(Lineside Electronic Unit) Traťová elektronická jednotka
MAC……...	(Message Authentication Code) Kód autentizace zprávy
MTBF……..…..	(Mean Time Between Failures) Střední doba mezi poruchami
NSAP……	(Network Service Access Point) Přistupový bod síťové služby
O&M……..	(Operation and Maintenance) Provoz a údržba
OBU……...	(On-board unit) Palubní jednotka
PLMN……	(Public Land Mobile Network) Veřejná pozemní mobilní síť
PSTN……..	(Public Switched Telephone Network) Veřejné komutované telefonní sítě
QoS…….	(Quality of Service) Kvalita služby
RBC...…….....	(Radio Block Centre) Rádio bloková centrála
RCS…….....	(Radio Communication System) Rádiový komunikační systém, také používáno pro EURORADIO systém
RIU ……...	(Radio In-ill Unit) Mezilehlá rádiová jednotka
RTC……	(Real Time Clock) Obvod reálného času
SA…….……....	(Source Address) Adresa Zdroje
SaPDU…….....	(Safety Service Protocol Data Unit) Bezpečná protokolová datová jednotka
SaS……	(Safety Service) Bezpečné služby
SaSAP…….……..	(Safety Service Acess Point) Bezpečný služební přístupový bod
SaUD……..	(Safety User Data) Bezpečná uživatelská data
SFM…….....	(Safe Functional Module) Bezpečný funkční modul
SIL……....	(Safety Integrity Level) Úroveň integrity bezpečnosti
SRAM…….	(Static Random Access Memory) Statická paměť s náhodným přístupem
STM……	(Specific Transmission modul) Specifický přenosový modul
TC…….....	(Transport Connection) Transportní spojení
TSAP…….....	(Transport Service Aces Point) Přístupový bod transportní služby
USB…….	(Universal Serial Bus) Univerzální sériová sběrnice

Úvod

Se začátkem sjednocování Evropy a rušením hranic mezi jednotlivými členskými státy, se také objevil požadavek na neomezené provozování dopravních systémů. Tento požadavek bylo na železnici velmi obtížné splnit , protože od počátků železnice se vyvinulo v Evropě přes 20 národních systémů, které jsou značně rozlišné co se týká např. návěstních systémů, vlakových zabezpečovacích zařízeních, ale i rozdílných provozních předpisů. To znamenalo, že při přechodu mezi těmito národními systémy bylo na hranicích potřeba např. přepřahat hnací vozidla a vyměnit personál, což vedlo ke značným časovým ztrátám. Propojení všech těchto národních systémů bylo z ekonomického, kapacitního a časového hlediska prakticky nemožné.

Proto v roce 1991 byl zahájen Mezinárodní železniční unií (UIC) projekt jednotného evropského vlakového zabezpečovacího systému ETCS, který má zastřešovat oblast zabezpečovací techniky. Tento systém má jednotným způsobem předávat strojvedoucímu podmínky pro jízdu vlaku získané z národních zabezpečovacích systémů. Projekt byl následně převzat Evropskou unií a byl začleněn do projektu ERTMS.

Diplomová práce je zaměřena na popis protokolu EURORADIO a návrh úložiště kryptografických klíčů. První kapitola obsahuje stručné seznámení se systémem ERTMS a jeho částmi. Druhá kapitola se zabývá popisem protokolu EURORADIO. Třetí kapitola popisuje klíčový management protokolu EURORADIO. Čtvrtá kapitola obsahuje stručný popis bezpečnostních požadavků pro kryptografické moduly a pátá kapitola je zaměřena na návrh kryptografického modulu protokolu EURORADIO.

1 Systém ERTMS

„V roce 1995 definovala Evropská komise globální strategii pro vývoj Evropského systému řízení železniční dopravy (ERTMS) s cílem připravit jeho budoucí implementaci na evropské železniční síti a promítla ji do směrnic a následně do technických specifikací pro interoperabilitu subsystémů řízení a zabezpečení jak pro vysokorychlostní, tak i konvenční evropský železniční systém.“[1]

ERTMS představuje projekt většího rozsahu, který pokrývá následující oblasti:

- **komunikace** – projekt EIRENE – v jehož rámci byly vytvořeny funkční a systémové specifikace, které umožnily realizaci systému GSM-R [2]
- **zabezpečení** – projekt ETCS [3, 4, 5]
- **řízení** – ETML – řeší řízení provozu na evropských koridorech z nadnárodního hlediska – projekt OPTIRAILS
- **provozu** – projekt EOR – řeší jednotné provozní předpisy na evropských tratích

1.1 Systém GSM-R

„Systém GSM-R je nový digitální systém sloužící ke komunikaci na železnici. Vychází ze standardu GSM. Oproti GSM je však rozšířen o celou řadu specifických funkcí, jež jsou pro komunikaci na dráze nezbytné.“[2]

GSM-R systém se používá ke spojení ETCS traťových subsystémů s palubními subsystémy pro přenos interoperabilních vlakových informací (přes protokol EURORADIO).

Rozdílů mezi GSM a GSM-R není mnoho a týkají se hlavně bezpečnosti a spolehlivosti. Jeden rozdíl je ve způsobu pokrytí daného území. GSM-R se snaží pokrýt jen omezené území v těsném okolí tratě, s vyloučením hluchých míst. Proto se GSM-R buňky vzájemně překrývají. S ohledem na to, že GSM-R uživatelů nebude mnoho, mohou být buňky značně rozsáhlé, to znamená úzké a dlouhé. GSM-R síť je použitelná pro rychlosti až do 350km/h na rozdíl od GSM, která zvládá rychlosti do 250km/h. Frekvenční pásma vyhrazená pro GSM-R jsou 876MHz až 880MHz pro vysílání a 921MHz až 925MHz pro příjem. Šířka kanálu 200kHz a použitá modulace GMSK jsou stejné jako u GSM.

Největším rozdílem GSM-R od GSM je rozdílný přístup ke službám. Přidanými službami jsou např. tyto:

- **Rozšířená víceúrovňová priorita a nucené přerušení** - Zatímco GSM nabízí všem uživatelům rovný přístup ke službám. GSM-R obsluhuje jednotlivé účastníky podle priority, která jim je v systému přidělena.

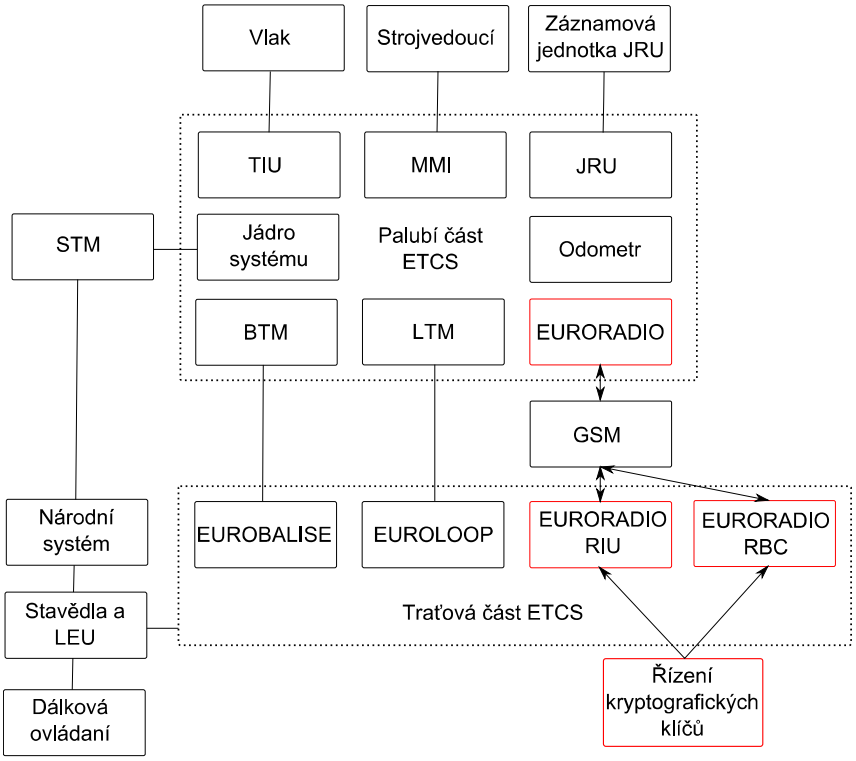
- **Potvrzení hovoru s vysokou prioritou** – Mobilní stanice automaticky generuje potvrzovací zprávu, která je dočasně uložena v radiotelefonní ústředně. Tohoto se využívá např. při vyšetřování nehody.
- **Funkční adresování** – umožňuje uživateli být dostupný pod číslem, které určuje příslušnou funkci a ne fyzický terminál.
- **Adresování závislé na poloze** – tato služba umožňuje nastavit pro každý typ hovoru na každé základnové stanici libovolné směrování.
- **Skupinové spojení** – umožňuje spojení s celou předem definovanou skupinou uživatelů.

1.2 Systém ETCS

„Systém evropského vlakového zabezpečovacího zařízení zajišťuje technickou interoperabilitu – vlaky jsou schopné bezpečné jízdy na základě informací, přijímaných od staničních, traťových a přejezdových zabezpečovacích zařízení. Technická interoperabilita je předpokladem pro interoperabilitu obecnou, při které je řízení vlaku založeno na ucelené informaci, zobrazované v kabině strojvedoucího v souladu s obecně platnými pravidly definovanými pro evropskou železniční síť.“[3]

Základní principy funkce ETCS lze stručně vyjádřit takto:

- pohyb vlaku je možný jen při platném oprávnění k jízdě s vymezeným koncem cesty a obvykle též časovým limitem k jeho dosažení.
- bezpečná kontrola rychlosti vlaku je stanovená na základě:
    - vzdálenosti ke konci jízdní cesty
    - rychlostních omezení v jízdní cestě
    - sklonových poměrů
    - charakteristik vlaku (délka, brzdění, …)



Obr. 1.1 Architektura systému ETCS

Popis architektury:

TIU - Train Interface Unit – jednotka vlakového rozhraní

MMI - Man-Machine Interface – rozhraní pro styk s obsluhou

JRU - Juridical Recording Unit – záznamová jednotka

BTM - Balise Transmission modul – modul pro komunikaci s balízou

LTM - Loop Transmission modul – modul pro komunikaci se smyčkou

EURORADIO- rozhraní mezi systémem GSM-R a ETCS

STM - Specific Transmission modul – specifický přenosový modul

RBC - Radio Block Centre – radiobloková centrála

RIU - Radio in-fill unit – doplňkové informace přenášené rádiem

LEU - Lineside Electronic Unit – traťová elektronická jednotka pro přepínatelnou balízu

V průběhu vývoje systému ETCS bylo vytvořeno několik základních aplikačních úrovní:

- aplikační úroveň L0
- aplikační úroveň STM
- aplikační úroveň L1
- aplikační úroveň L2

– aplikační úroveň L3

1.2.1 Aplikační úroveň L0

Trať není vybavena traťovou částí ETCS. Palubní část dohlíží na nepřekročení maximální rychlosti vlaku a nepřekročení povolené rychlosti pro tuto úroveň. Dále palubní část zajišťuje čtení balíz pro detekci přechodu do jiné úrovně a speciální příkazy.

1.2.2 Aplikační úroveň STM

Trať je vybavena národním systémem vlakového zabezpečovače. Palubní část ETCS je vybavena specifickým vysílacím modulem (STM), který je schopen komunikovat s národní traťovou částí. V takovém případě je možné získané informace zpracovat a zobrazovat pomocí palubní části ETCS, která navíc dále zajišťuje čtení balíz pro detekci přechodu do jiné úrovně a speciální příkazy.

1.2.3 Aplikační úroveň L1

Aplikační úroveň L1 je určena jako doplněk klasického zabezpečovacího zařízení. Zjišťování volnosti kolejových úseků je stále úkolem technologií, které spolupracují se staničním a traťovým zabezpečovacím zařízením (kolejové obvody, počítače náprav apod.) Na trati jsou osazeny přepínatelné balízy, které mají funkci referenčního bodu a zároveň předávají hnacímu vozidlu všechny relevantní informace. Časově proměnné informace (povolení k jízdě) jsou také předávány prostřednictvím přepínatelných balíz, které jsou přes kabel a interface LEU připojeny ke klasickému zabezpečovacímu zařízení (návěstidlu nebo stavědlu). Neproměnné informace mohou být přenášeny nepřepínatelnými balízami.

1.2.4 Aplikační úroveň L2

Tato úroveň je v principu také určena k aplikaci na tratích s klasickými staničními a traťovými zabezpečovacími zařízeními, které zjišťují volnost trati. Časově proměnné informace jsou předávány na vozidlo výhradně prostřednictvím rádia, a tak odpadá dodatečná kabeláž k přepínatelným balízám. Neproměnné balízy slouží jako referenční body, k orientaci směru jízdy a korekci odometru. Pro přispění ke zjednodušení architektury systému a snížení provozních nákladů je v této úrovni možno zrušit optická návěstidla, pokud všechny vozidla pohybující se po této trati jsou vybavena palubní částí ETCS L2

1.2.5 Aplikační úroveň L3

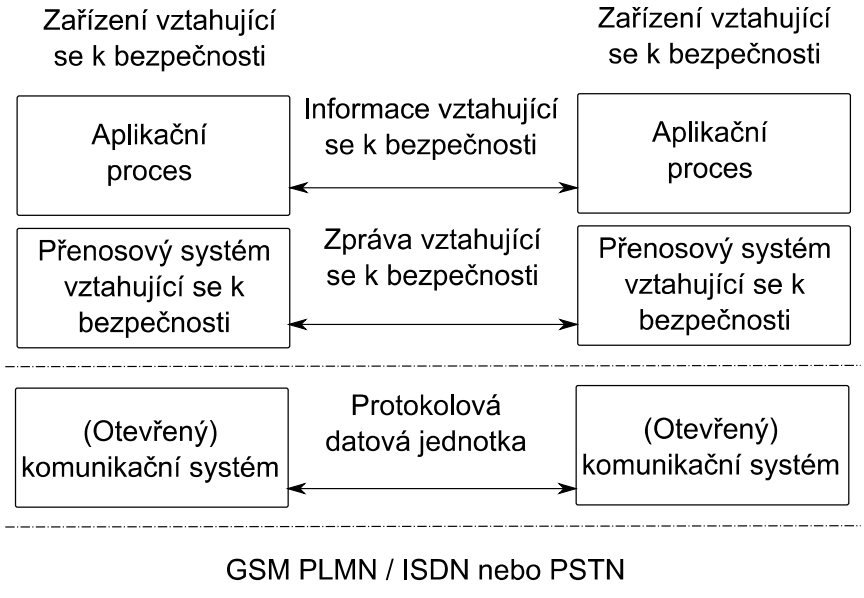
Tato úroveň je určena pro realizaci RBC. Pokud bude vlak na rozdíl od úrovně L2 vybaven prostředkem pro bezpečnou detekci celistvosti vlaku, může vlak prostřednictvím rádia bezpečně hlásit sám svou polohu. Tím odpadá potřeba klasických zařízení pro detekci vozidel. Lze pak prostřednictvím RBC realizovat i takovou funkci jakou je pohyblivý blok.

2 Protokol EURORADIO

Protokol EURORADIO je vztažený na radiokomunikační systémy poskytující své služby aplikacím vztahujícím se k bezpečnosti v otevřených sítích. Protokol zajišťuje slučitelnost rádiových systémů při výměně zpráv mezi vozidlovým a traťovým vybavením, se zohledněním v aplikacích, vztahujících se k bezpečnosti, jako je automatický vlakový zabezpečovací systém ETCS L2 nebo ETCS L3. Dodatečně specifikuje pro ETCS L1 volitelnou výměnu zpráv mezi palubním zařízením a RIU. [6]

2.1 Referenční architektura

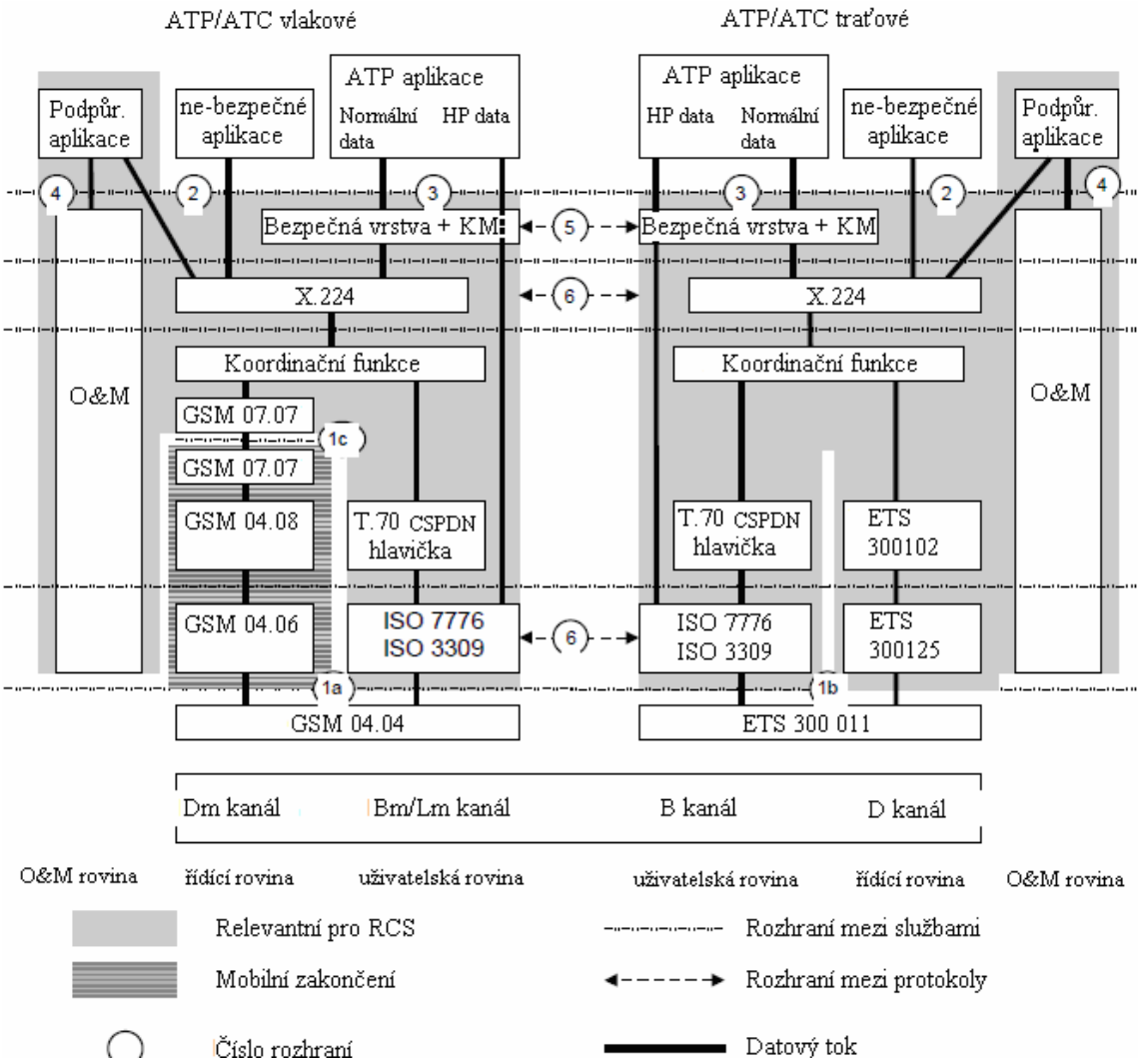
EN 50159-2 definuje referenční architekturu pro systémy, vztahující se k bezpečnosti, používající otevřených přenosových sítí. Obecná struktura systémů vztahujících se k bezpečnosti, jako je ETCS (obr. 2.1), je odvozena z EN 50159-2. Kromě informací vztahujících se k bezpečnosti, si mohou aplikace vztahující se k bezpečnosti vyměňovat informace nevztahující se k bezpečnosti se vzdálenými aplikacemi využívajících služeb rádiového komunikačního systému.



Obr. 2.1 Struktura rádiového komunikačního systému

Bezpečný funkční modul (SFM) rádiového komunikačního systému (RCS) poskytuje funkce přenosového systému vztahujícího se k bezpečnosti. Komunikační funkční modul (CFM) RCS poskytuje funkce komunikačního systému založeného na službách přepínání okruhů GSM-R PLMN. Obrázek 2.2 obsahuje detailní referenční architekturu rádiových komunikačních subsystémů založených na službách přepínání okruhů, definuje rozhraní mezi službami a rozhraní mezi protokoly.

Rozhraní 1 je rozhraní mezi RCS a vybraným přenosovým médiem. Rozhraní 1a je GSM PLMN rozhraní (na palubě). Rozhraní 1b je rozhraní do pevných sítí (na trati). Rozhraní 1c je doporučené rozhraní mezi RCS a mobilním terminálem MT2. Na obrázku 2.2 je znázorněno rozhraní primární přípojky ISDN. Rozhraní základní přípojky ISDN a PSTN nejsou vyloučeny.



Obr. 2.2 Referenční struktura protokolu EURORADIO

Rozhraní 2 je volitelné služební rozhraní mezi aplikacemi nevztahujícími se k bezpečnosti nebo rozhraní mezi podpůrnými aplikacemi a komunikačním funkčním modulem. Rozhraní 3 je služební rozhraní mezi bezpečnými aplikacemi (např. ATP/ATC) a bezpečným funkčním modulem (bezpečnou vrstvou). Rozhraní 2 a 3 nejsou povinná pro interoperabilitu. Provozní a údržbová (O&M) rovina pokrývá všechny činnosti a správy aspektů. Rozhraní 4 je místní služební rozhraní pro O&M zásobník. Rozhraní 5 a 6 jsou logická rozhraní pro rovnocenné jednotky a jsou povinná pro interoperabilitu.

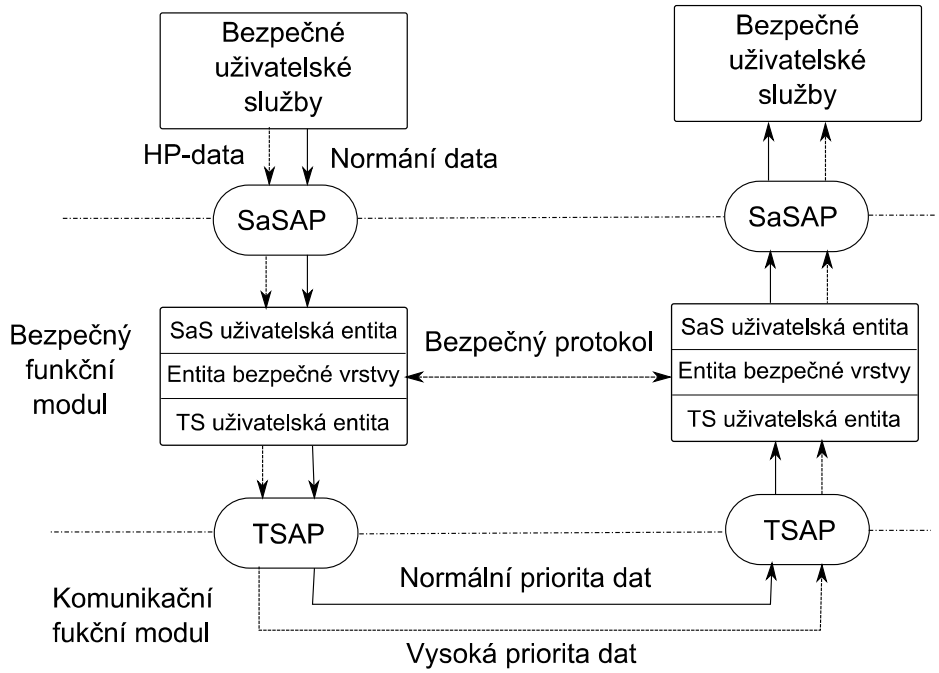
2.2 Bezpečný funkční modul – SFM

2.2.1 Definice služby

Specifikuje rozhraní mezi SFM a uživatelem SFM. To znamená toky dat do a z SFM, poskytující bezpečné služby. Uživatel bezpečných služeb (SaS) si vyměňuje data s poskytovatelem SaS. Bezpečné služby poskytují bezpečné vytvoření spojení a bezpečný přenos dat během spojení. Dále poskytují integritu a autenticitu dat. SFM ohlašuje chyby, které se vyskytly v bezpečné vrstvě a předává informace o chybách z nižších vrstev. [6]

Model bezpečných vrstev:

Bezpečná entita komunikuje s uživateli přes jeden či několik bezpečných přístupových bodů (SaSAP) pomocí bezpečné základní služby. Rovnocenné bezpečné entity podporují bezpečné spojení prostřednictvím bezpečné protokolové datové jednotky (SaPDU). Tyto přenosy používají služby transportní vrstvy přes jedno transportní spojení (TC) skrze jeden přístupový bod přenosové služby (TSAP). Výměna dat pomocí SaPDU je pouze logickým pohledem. Normální operace přenášejí normální data a HP-operace přenášení HP-data.



Obr. 2.3 Model bezpečných služeb

Navázání bezpečného spojení:

Autentizace rovnocenných entit se provádí bezpečným protokolem mezi entitami bezpečné vrstvy. Při požadavku na navázání bezpečného spojení bezpečná vrstva aktivuje odpovídající mechanismus na ověření autenticity entit. Proces zahajující vytváření bezpečného spojení je inicializován, když uživatel SaS požádá bezpečnou vrstvu o spojení. Uživatel SaS vyšle informaci o adrese a požadavek na kvalitu služeb (QoS), aby bezpečná vrstva sestavila spojení. Hodnota QoS je předána CFM a je interpretována jako požadavek na předdefinovanou množinu QoS. Služba poskytující bezpečné spojení je realizována provedením bezpečné procedury „autentizace rovnocenných entit“. Vytvoření transportního spojení mezi traťovou a vozidlovou částí je nutnou podmínkou k vytvoření bezpečného spojení. Každá chyba při bezpečné proceduře „autentizace rovnocenných entit“ musí vést k odmítnutí navázání spojení a k ukončení transportního spojení.

Bezpečný přenos dat:

Bezpečná vrstva zajišťuje výměnu uživatelských dat v obou směrech současně a ochraňuje integritu a rozsah uživatelských dat. Entita bezpečného funkčního modulu garantuje bezpečný přenos dat pro zprávy vztahující se k bezpečnosti. Služba bezpečného přenosu dat užívá bezpečnou proceduru „kód autentizace zprávy“. „Kód autentizace zprávy“ procedura poskytuje ochranu proti vložení zpráv neautorizovanými uživateli přenosového

kanálu. Tím se myslí jakákoliv modifikace zprávy aktivním útokem, či vinou náhodných chyb přenosového kanálu.

Ukončení bezpečného spojení:

Ukončení bezpečného spojení je provedeno:

- Jedním nebo oběma uživateli SaS ukončením vytvořeného bezpečného spojení.
- Bezpečnou vrstvou uvolněním vytvořeného bezpečného spojení.
- Jedním nebo oběma uživateli SaS přerušením vytvořeného bezpečného spojení.
- Bezpečnou vrstvou indikující svoji neschopnost vytvořit požadované bezpečné spojení.

Ukončení bezpečného spojení je možné vždy, bez ohledu na aktuální fázi bezpečného spojení. Požadavek na ukončení nemůže být odmítnut. Bezpečná služba negarantuje doručení uživatelských dat po zahájení ukončování spojení. Žádost o ukončení bezpečného spojení nevyžaduje bezpečnou ochranu, narozdíl od bezpečného vytvoření spojení.

Hlášení chyb:

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

Přenos dat s vysokou prioritou:

Bezpečná vrstva neposkytuje ochranu pro data s vysokou prioritou. Služba nesmí být použita před úspěšným vytvořením bezpečného spojení, to znamená, že může být použita pouze po úspěšném výkonu bezpečné procedury „autentizace rovnocenných entit“. Délka dat s vysokou prioritou je omezena.

2.2.2 Bezpečný protokol

Bezpečný protokol je založený na standardu EN 50159-2 [7]. Metoda použitá v SFM odpovídá typu A1 v EN 50159-2: kryptografický bezpečnostní kód používající tajný klíč.

Bezpečný protokol zahrnuje:

- Funkce bezpečné vrstvy
- Časové posloupnosti
- Strukturu a kódování SaPDU

- Stavovou tabulku

Funkce bezpečné vrstvy:

Bezpečná vrstva poskytuje bezpečný přenos uživatelských dat. To zahrnuje vytvoření a ukončení bezpečného spojení. Bezpečná vrstva obsahuje bezpečné procedury, které zajišťují autentizaci a integritu během přenosu.

Bezpečné procedury se používají pro ochranu zpráv proti modifikaci a zajištění, že nikdo se nemůže maskovat jako původce zprávy. Tyto procedury se nazývají „zprávy ověření původu“. Mezi tyto procedury patří:

Kód autentizace zprávy (MAC) při vysílání (m, K_S)

Vstup: Zpráva m a kryptografický klíč K_S, který je sdílen mezi odesílatelem (s adresou zdroje SA) a příjemcem (s adresou příjemce DA). SA a DA jsou ETCS identity.

Procedura:

1) Nastavení směrového příznaku zprávy m (hodnota 0 pro iniciátora a hodnota 1 pro odpovídajícího)
2) Připojení adresy příjemce (DA) před zprávu: „DA | m“.
3) Vypočte se délka l řetězce DA | m v bytech a připojí se před řetězec pro výpočet MAC, tj. „l | DA | m“.
4) Pokud délka zprávy (l | DA | m) není celočíselný násobek 64 v bitech, provede se vyplnění (padding) a připojí se jako data p: „l | DA | m | p“.
5) Provede se výpočet MAC pro řetězec „l | DA | m | p“ pomocí CBC-MAC funkce a kryptografického klíče K_S: MAC(m) = CBC-MAC(K_S, l | DA | m | p), kde | označuje zřetězení.

Výstup: Pokud nenastane chyba tak se MAC(m) připojí k m, jinak je informován chybový management.

Pro tyto SaPDU je pro výpočet MAC použit relační klíč K_S získaný během vytváření spojení. Délka klíče $K_S = (K_1, K_2, K_3)$ musí být 192 bitů včetně paritních bitů.

CBC-MAC(K,X) funkce používá tajný klíč K a libovolný datový řetězec X pro který má být MAC vypočítána následovně:

Nechť $K = (K_1, K_2, K_3)$, nechť X je představováno 64 bitovými bloky $X_1, X_2, \ldots, X_q$. Nechť $E(K_n, Y)$ je bloková šifra, jednoduchý DES, šifrující datový řetězec Y užívající klíč K_n ($n \in \{1, 2, 3\}$), $E^{-1}(K_n, Y)$ je bloková šifra v dešifrovacím režimu. Pak H_q je odvozeno následovně:

$$H_0 = 0 \tag{2.1}$$

$$H_i = E(K_1, H_{i-1} \oplus X_i), i = 1,2,...,q-1 \quad (2.2)$$

$$H_q = E(K_3, E^{-1}(K_2, E(K_1, H_{q-1} \oplus X_q))) \quad (2.3)$$

MAC datového řetězce X je pak roven H_q.

V případě DT SaPDU zpráva m = 000 | MTI | DF | SaUD obsahuje identifikátor zprávy (MTI) určující DT SaPDU, směrový příznak (DF) a bezpečná uživatelská data (SaUD).

V případě AU2 SaPDU zpráva m = ETY | MTI | DF | SA | SaF | auth2 obsahuje ETCS ID typ, identifikátor zprávy (MTI) indikující AU2 SaPDU, směrový příznak (DF), zdrojovou adresu (SA), bezpečnostní vlastnosti (SaF) a odpovídající autentizační zprávu (auth2 = Ra | Rb | B).

V případě AU3 SaPDU zpráva m = 000 | MTI | DF | auth3 obsahuje identifikátor zprávy (MTI) indikující AU3 SaPDU, směrový příznak (DF) a odpovídající autentizační zprávu (auth3 = Rb | Ra).

V případě AR SaPDU zpráva m = 000 | MTI | DF obsahuje identifikátor zprávy (MTI) indikující AR SaPDU a směrový příznak (DF).

Směrový příznak je použit jako ochrana proti útokům odrazem. Data vysoké priority jsou posílána bez MAC ochrany.

Kód autentizace zprávy (MAC) při příjmu (m, K_S, MAC‘(m‘))

Vstup: Zpráva m včetně směrového příznaku, kryptografického klíče K_S, který je sdílen mezi odesílatelem a příjemcem a MAC‘(m‘), což je MAC vypočtený pro m‘ odesílatele.

Procedura:

1) Připojení adresy příjemce (DA) před zprávu: „DA | m“.
2) Vypočte se délka l řetězce DA | m v bytech a připojí se před řetězec pro výpočet MAC, tj. „l | DA | m“.
3) Pokud délka zprávy (l | DA | m) není celočíselný násobek 64 v bitech, provede se vyplnění (padding) a připojí se jako data p: „l | DA | m | p“.
4) Provede se výpočet MAC pro řetězec „l | DA | m | p“ pomocí CBC-MAC funkce a kryptografického klíče K_S: CBC-MAC(K_S, l | DA | m | p),
5) Porovná se MAC s MAC‘
6) Ověří se hodnota směrového příznaku

Výstup: Zpráva m je předána uživateli SaS pokud MAC = MAC‘ a hodnota směrového příznaku je správná. Pokud ne, je informován chybový management.

Autentizace rovnocenných entit (ETCS ID A, ETCS ID B, K_{AB})

Vstup: ETCS ID entity A i B, autentizační klíč (K_{AB}) sdílený mezi entitami A a B.

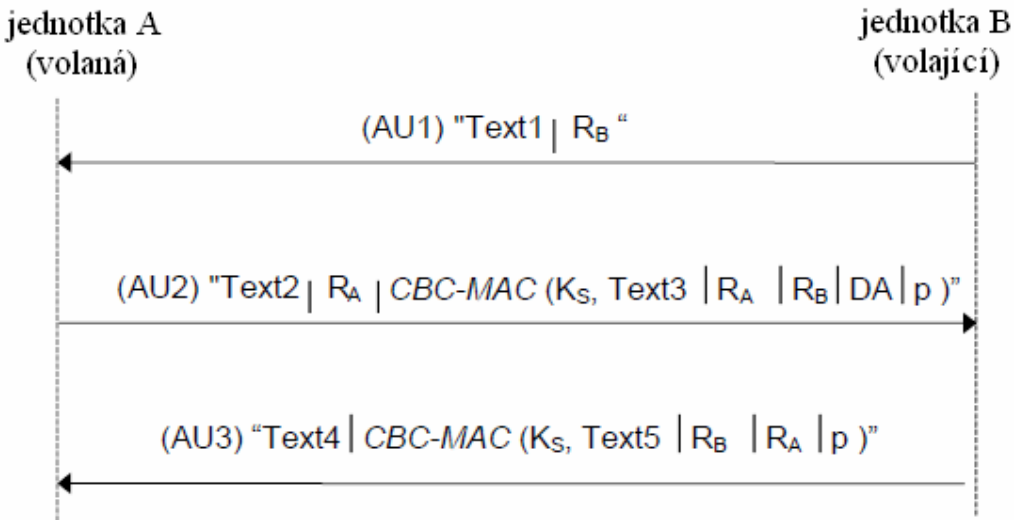
Procedura: Autentizační protokol je definován na obrázku 2.4.

Výstup: Pokud nenastane chyba, jsou úspěšně navzájem autentizovány jednotky A a B, mezi kterými je sdílen relační klíč.

Tato autentizace je vykonávána během vytváření spojení. Vstupní parametry ETCS ID jsou unikátní identifikátory. Autentizační klíč má být předtím vytvořen mezi A a B pomocí logických nebo fyzických klíčových mechanismů.

Iniciátor vytvoření spojení (B) začne s bezpečnostně relevantním protokolem, když vyžaduje transportní spojení.

Iniciátor (B) přenáší náhodné číslo Rb délky 64 bitů, které je generováno B jako část první autentizační zprávy AU1 SaPDU, svému komunikačnímu partnerovi (A). Náhodné číslo Rb musí být uloženo před odesláním AU1 SaPDU. Po přijetí této zprávy, generuje A jako část druhé zprávy AU2 SaPDU náhodné číslo Ra délky 64 bitů a MAC vypočtený přes textové pole text3, náhodná čísla Ra a Rb, identitu B (ETCS ID B) a vyplněné bity (padding). Pro výpočet MAC je vypočtený relační klíč K_S pomocí funkce na generování relačních klíčů, parametrů Ra, Rb a autentizačního klíče K_{AB}. Po přijetí zprávy AU2 SaPDU a odvození K_S klíče, B zkontroluje správnost druhé autentizační zprávy přijaté od A. Pak, B vypočte MAC přes textové pole text5, náhodná čísla Ra a Rb a odešle to jako část AU3 SaPDU. Nakonec A zkontroluje AU3 SaPDU pomocí klíče K_S.



Obr. 2.4 Sa-Protokol použitý pro autentizaci rovnocenných jednotek a generování klíče

Časové posloupnosti:

Zde bude popsán tok kontrolních informací a uživatelských dat při navazování spojení, výměně dat a ukončování spojení.

Vytváření spojení:

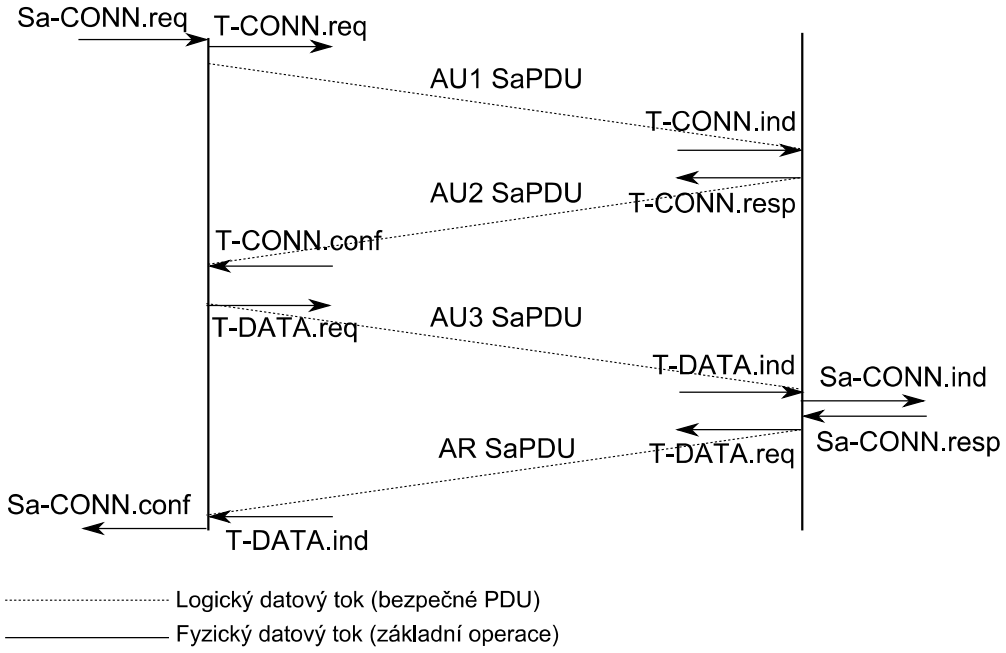
Když pomocí **Sa-CONNECT.request** je požadováno základní bezpečné spojení, bezpečná vrstva požaduje vytvoření transportního spojení prostřednictvím **T-CONNECT.request**. Tato základní operace zahrnuje první zprávu procedury „autentizace rovnocenných entit“. Transportní vrstva volané entity indikuje požadavek na vytvoření spojení svojí bezpečné vrstvě pomocí základní operace **T-CONNECT.indication**. Je-li vše v pořádku, tak bezpečná entita odpoví na požadavek o vytvoření transportního spojení základní operací **T-CONNECT.response**. Ta zahrnuje druhou zprávu procedury „autentizace rovnocenných entit“.

Při příjmu, informuje volající transportní entita bezpečnou vrstvu o úspěšném vytvoření transportního spojení, použitím základní operace **T-CONNECT.confirmation.** Bezpečná entita pak generuje třetí zprávu procedury „autentizace rovnocenných entit“. Poté použije základní operaci **T-DATA.request** pro předání zprávy transportní vrstvě. Při přijmu použije transportní entita základní operaci **T-DATA.indication** pro předání zpráv bezpečné vrstvě.

Při úspěšném vyhodnocení pošle bezpečná entita základní operaci **Sa-CONNECT.indication** bezpečnému uživateli (např. ATP aplikaci). Pokud bezpečný uživatel akceptuje požadavek na vytvoření bezpečného spojení, odpoví základní operací **Sa-CONNECT.response**.

Bezpečná entita na volané straně odesílá odpověď **AR SaPDU** prostřednictvím základní operace **T-DATA.request** a **T-DATA.indication** svojí rovnocenné bezpečné entitě.

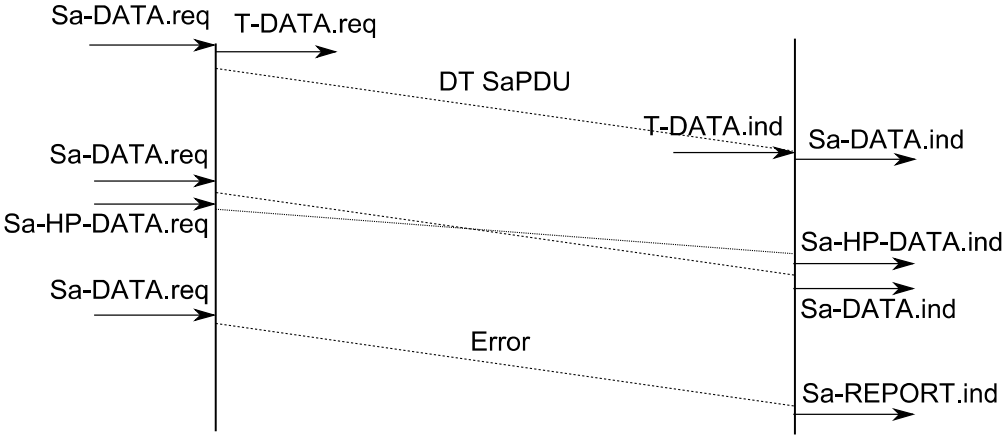
Po úspěšném vyhodnocení **SaPDU** informuje bezpečná entita uživatele SaS, že bylo vytvořeno bezpečné spojení pomocí základní operace **Sa-CONNECT.confirmation**. Pokud je **Sa-CONNECT.confirmation** přijata, tak volající uživatel SaS je schopný odesílat data přes bezpečné spojení. Volaný uživatel SaS je schopný žádat data okamžitě po základní operaci **Sa-CONNECT.response**.



Obr. 2.5 Časové posloupnosti během vytváření spojení

Přenos dat:

Protokolová sekvence na obrázku 2.6 ukazuje jak jsou data přenášena SFM.



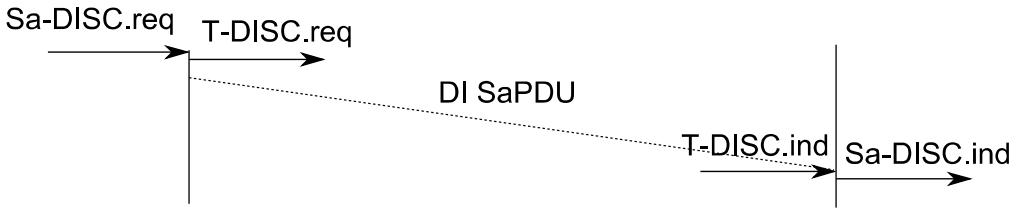
Obr. 2.6 Časová posloupnost během přenosu dat (příklad)

Uživatelská data bezpečného přenosu DT SaPDU jsou obsažena v základní operaci **Sa-DATA.indication**. Přenos dat s vysokou prioritou je podobný normálnímu datovému přenosu. V případě problému s bezpečnostní DT SaPDU, signalizuje toto uživateli základní operace **Sa-REPORT.indication** nebo **Sa-DISCONNECT.indication**.

Ukončení spojení:

Ukončení spojení je prováděno pomocí základní operace **Sa-DISCONNECT.request**. Potom bezpečná vrstva žádá transportní vrstvu o odpojení pomocí **T-**

DISCONNECT.request. Rovnocenné entity jsou informovány o odpojení pomocí **T-DISCONNECT.indication** a **Sa-DISCONNECT.indication**.



Obr. 2.7 Časová posloupnost při ukončení spojení

Struktura SaPDU:

Všechny bezpečné protokolové datové jednotky (SaPDU) budou obsahovat celý počet oktetů. Oktety v SaPDU jsou číslovány od 1. Bity v oktetu jsou číslovány od 8 do 1, kde bit 1 je nejnižší hodnoty.

SaPDU obsah bude následující:

- Hlavička (obsahující příznak směru a identifikátor typu zprávy, délka = 1 oktet)
- Datové pole (pokud existuje, délka = variabilní)
- MAC pole (pokud je použito, délka = 8 oktetů)

Stavová tabulka:

Přechodový stavový diagram a stavová tabulka jsou shodné pro traťový a palubní SFM. Stavové tabulky ukazují stav bezpečné vrstvy entity, událostí, které se vyskytují v protokolu, prováděné akce a výsledné stavy. Stavové tabulky jsou koncepční a nevytváří žádné omezení implementaci. Stavové tabulky také definují mapování mezi bezpečnými základními operacemi a protokolovými událostmi, které uživatel SaS může očekávat.

2.2.3 Management bezpečného protokolu

Management bezpečného protokolu definuje konfigurační management potřebný pro práci s parametry bezpečného protokolu, dohled a diagnostiku bezpečného protokolu. Hlavní důraz se klade na dosažení technické interoperability mezi palubní a traťovou jednotkou respektující management bezpečného protokolu.

Management konfigurace definuje parametry potřebné pro správnou činnost bezpečného protokolu, jeho managementu a funkce k jeho řízení. Tyto parametry jsou:

- Adresové parametry (bezpečný protokol používá ETCS Identity)
- Časovací parametry (určení maximálního zpoždění při navazování spojení)

Dohled a diagnostika popisuje chybový management bezpečné vrstvy, který monitoruje a kontroluje události vztahující se k bezpečnosti.

Chybový management definuje chybové řízení a chyby hlásí aplikační vrstvě, tak jak je to potřebné z hlediska interoperability.

2.3 Komunikační funkční modul – CFM

CFM koresponduje s OSI vrstvou 4 (transportní), 3 (síťovou) a 2 (linkovou).

Komunikační služby, které RCS komunikační funkční modul nabízí jeho uživatelům (jako bezpečný funkční modul) jsou založeny na službách poskytovaných transportní vrstvou ISO/OSI. Tyto služby obsahují:

- Vytvoření a ukončení transportního spojení
- Spolehlivý datový přenos
- Transportní datový přenos
- Přenos dat s vysokou prioritou (při tomto přenosu jsou vynechány vrstvy 4 a 3)
- Kvalitu služby (QoS – je vyjednána na začátku každého přenosu)[6]

2.3.1 Komunikační protokoly:

Zde budou poskytnuty specifikace komunikačních protokolů uživatelského kanálu. Protokolové specifikace popisují vrstvu po vrstvě s ohledem na rozdíly od existujících standardů.

Linková vrstva:

Podle referenčního modelu ISO poskytuje linková vrstva spolehlivý přenos dat. Linková vrstva B/Bm-kanálu poskytuje funkční a procedurální prostředky k vytvoření spojení, udržení spojení, ukončení spojení a přenosu dat. Detekuje a opraví chyby v přenosu dat, které mohou vznikat ve fyzické vrstvě.

Protokol této vrstvy (DTE-DTE komunikace) transportuje data podle sekvence svých základních datových operací. Protokol této vrstvy patří pod HDLC standardy. Díky základním procedurám HDLC mohou být poskytnuty následující detekce chyb a opravné mechanismy:

- Automatický opětovný přenos po chybějícím potvrzení příjmu
- Rámcová 16ti bitová zabezpečovací sekvence

Síťová vrstva:

Podle referenčního modelu ISO síťová vrstva B/Bm-kanálu poskytuje funkční a procedurální prostředky k vytvoření, udržení a ukončení síťového spojení mezi otevřenými systémy obsahující komunikační transportní entity nezávislé na směrování a přenosových vlastnostech.

Pro tuto vrstvu bude použit v B/Bm-kanálu protokol síťové vrstvy T.70 pro CSPDN. Aplikována je pouze hlavička T.70: Segmentace a zpětné skládání NSDU z, nebo do sekvence NPDU a nastavování M-bitu.

Transportní vrstva:

Transportní vrstva vytváří transportní spojení, pokud existuje síťové spojení. Když síťové spojení neexistuje v momentě, kdy je spojení požadováno, transportní entita nejdříve ze všeho požádá o vytvoření tohoto spojení a pak automaticky zřizuje transportní spojení. TP2 bude použit pro poskytování více než jednoho transportního spojení po stejném síťovém spojení.

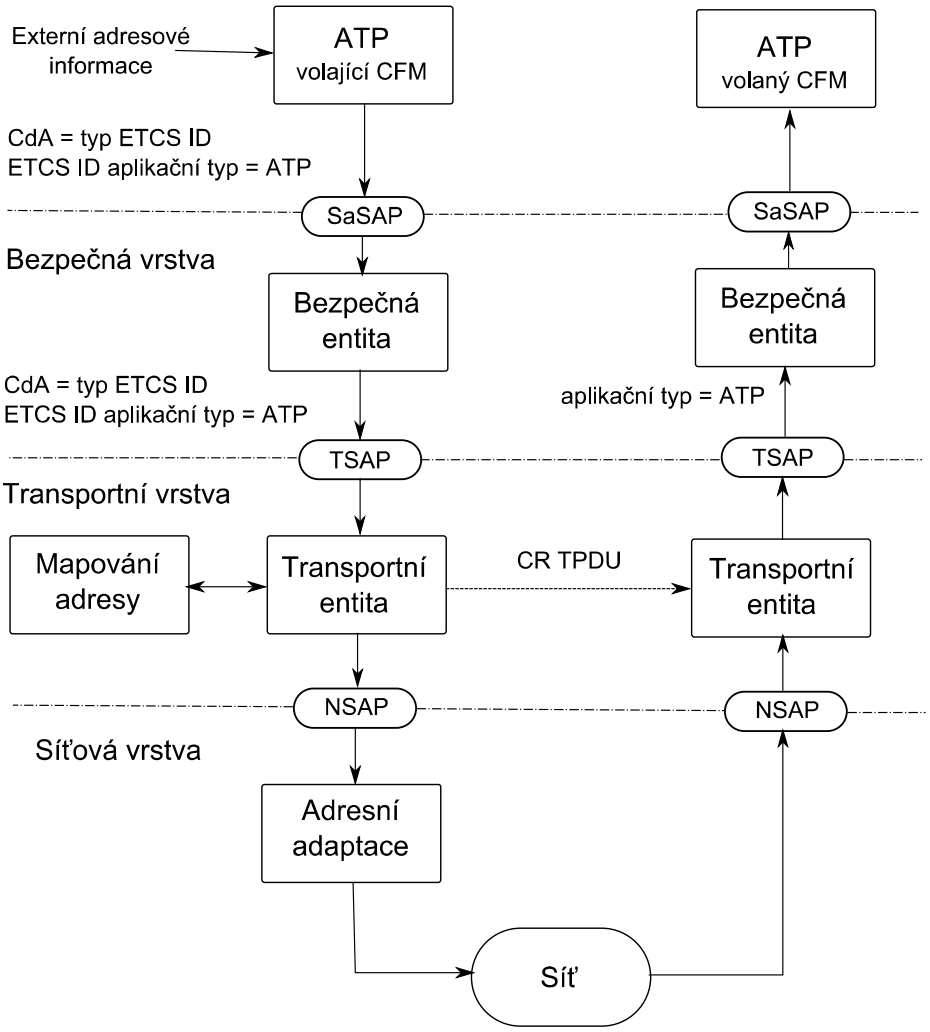
Protokol této vrstvy je začleněn pod ITU-T Rec. X.224 „Protokol pro poskytování OSI spojovacího režimu transportní služby“.

2.3.2 Management komunikačního funkčního modulu:

Volání a ID-manager:

CFM musí vytvořit spojení na požádání mezi rovnocennými aplikacemi (např. CFM uživateli). RCS komunikační funkční modul volitelně nabízí několik logických spojení mezi traťovým a palubním vybavením přes stejný fyzický kanál.

Transportní adresa je obecné pojmenování, které je použito k identifikaci nastavení transportních přístupových bodů (TSAP), které jsou všechny umístěny na rozhraní mezi vyšší vrstvou a transportní vrstvou CFM. Transportní adresa je použita pro přístup k jedné transportní službě (TS) uživatelské entity. Síťová adresa není dostatečná k identifikaci jednotlivé CFM uživatelské entity. Je třeba upozornit na požadovaný typ CFM uživatelské entity pomocí speciálního identifikátoru nebo adresového kvalifikátoru: aplikační typ.



Obr. 2.8 Příklad mapování adresy

Transportní vrstvy entit a CFM uživatelské entity jsou spolu vázány v TSAP. Každá CFM uživatelská entita může být vázána na jeden nebo více TSAP. Neexistuje žádná souvislost mezi TSAP a multiplexováním.

Adresy jsou užity v základních operacích T-CONNECT (transportní adresa) a N-CONECT (síťová adresa) na rozhraní služby. Pokud CFM uživatelská entita (např. entita bezpečné vrstvy) chce vytvořit spojení s další CFM uživatelsko entitou, poskytne informace o adrese volaného CFM uživatele (např. typ ETCS ID a ETCS ID) a aplikační typ. Tato adresní informace musí být mapována do formátu a struktury požadované CFM pro vytvoření spojení.

Obrázek 2.8 dává příklad o mapování adres během vytváření spojení mezi vlakovým a traťovým CFM. Volající TS uživatelská entita získala volanou transportní adresu od aplikace (typ ETCS ID a ETCS ID). Adresové informace bude procházet skrz SFM směrem k CFM.

Volající CFM má za úkoly:

- Zkontrolovat, že mobilní stanice je registrovaná do mobilní sítě obsažené v T-CONNECT.request.
- Přiřadit požadované spojení k příslušné mobilní stanici.
- Získat síťovou adresu volaného z adresové informace označující volaného CFM uživatele.
- Vložit do spojovací žádosti (CR) TPDU volané transportní voliče (pokud vlak inicioval vytvoření fyzického spojení) a volající transportní voliče.

Dohled / diagnostika:

Pokud se vyskytne chyba v komunikačním funkčním modulu nebo pokud komunikační funkční modul přijme hlášení o chybě, chyba a její důvod bude ohlášen. Různé důvody vyžadují různé akce pro odstranění chyb.

Pokud existuje problém s vytvořením spojení, CFM se pokusí tento problém sám odstranit. Jen když problém nelze vyřešit, bude CFM informovat CFM uživatele.

Typy chyb:

- Chyba sítě
- Síťové zdroje nejsou dostupné
- Služba nebo volba je dočasně nedostupná
- Neznámý důvod
- Volaný TS uživatel není dostupný
- Vnitřní chyba

Bezpečný funkční modul a/nebo aplikace jsou informovány o chybových situacích, které vedou k odpojení pomocí základní operace T-DISCONNECT.indication.

3 Klíčový management protokolu EURORADIO

V ERTMS systému, palubní jednotky a RBC nebo jiné podobné zařízení vyměňující informace pomocí protokolu EURORADIO, používá klíčový management k zabezpečení komunikace přes otevřené nedůvěryhodné médium.

Když ERTMS palubní jednotka chce komunikovat s RBC, musí být schopna ověřit, že je vytvořená komunikace s autorizovaným RBC a naopak. V důsledku toho je autentizace a integrita každé informace vyměněné mezi ERTMS palubním zařízením a RBC ověřena.

Způsob jak zajistit, aby oba komunikující subjekty byly ty za které se vydávají, je založen na identifikačním a autentizačním (I&A) dialogu. S cílem zajistit komplexní ochranu, musí tento postup probíhat pokaždé, když vzájemně rovnocenné entity zahajují nové bezpečné připojení.

Po každém úspěšném I&A dialogu jsou data chráněna pomocí „zprávy ověření původu“ (MAC). Výpočet tohoto kódu je založen na existenci společné tajné informace, kterou znají entity, které spolu komunikují.

I&A dialog a MAC výpočtové postupy jsou uvedeny v kapitole Bezpečný protokol. Tyto postupy jsou založeny na konkrétních kryptografických technikách, které používají tajné klíče. Nicméně, neposkytují žádné prostředky pro vytváření, distribuci a aktualizaci těchto klíčů. Navíc, jejich plný výkon se opírá o klíčové tajemství, které lze zaručit pouze při jasně definovaných klíčových management funkcích v souladu s konstrukční implementací a provozními scénáři železnice. [8, 9]

3.1 Hierarchie klíčů

Tab. 3.1 Hierarchie klíčů

Hierarchická úroveň	Název klíče	Použití
3	K-KMC	Tento transportní klíč se používá pro ochranu KMS komunikace mezi KMC
	KTRANS	Tento transportní klíč se používá pro ochranu KMS komunikace mezi KMC a traťovými nebo palubními zařízeními a pro zřízení nebo zrušení autentizačního klíče.
2	KMAC	Autentizační klíč se používá k odvození relačního klíče pro vytvoření bezpečného spojení mezi dvěma ETCS entitami. (také označován jako K_{AB})
1	KSMAC	Relační klíč se používá k ochraně dat přenášených mezi dvěma bezpečnými jednotkami. (také označován jako K_S)

Tab. 3.2 Použití klíčů

jednotky	Klíč použitý pro I & A	Klíč použitý pro Ochranu dat	Klíč použitý pro šifrování	Interoperabilita
traťová – palubní jednotka	KMAC	KSMAC	neaplikováno	relevantní pro interoperabilitu
KMC – ETCS entita	neaplikováno (off-line režim)	KTRANS1	KTRANS2	relevantní pro interoperabilitu
KMC - KMC	neaplikováno (off-line režim)	K-KMC1	K-KMC2	relevantní pro interoperabilitu

3.2 Definice klíčů

Triple-klíč je definován jako pole 192 bitů složených ze tří dlouhých DES-klíčů K1, K2, K3, každý o délce 64 bitů. Stručně řečeno: triple-klíč = K1 | K2 | K3, kde symbol "|" znamená zřetězení.

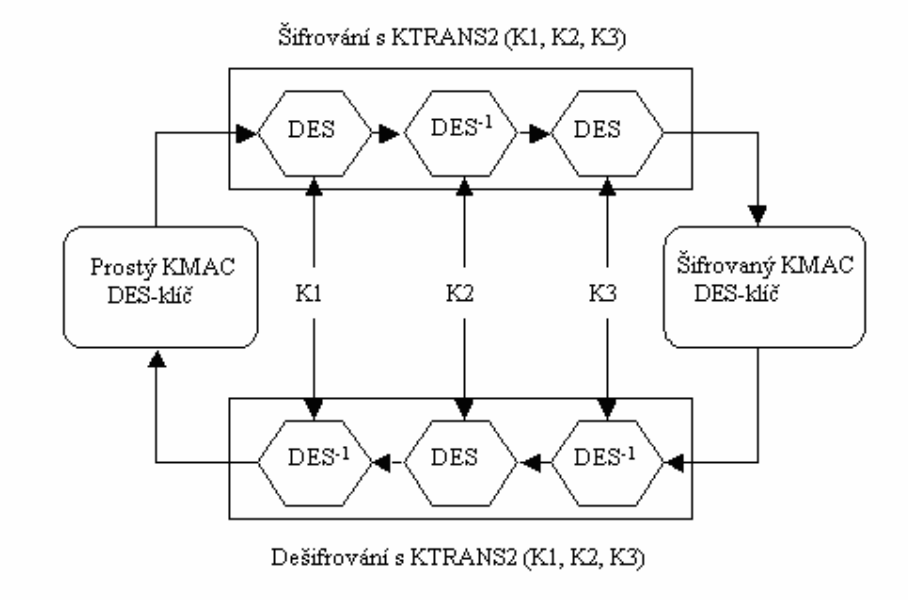
Pro platnost triple-klíče každý osmí bit ze 192 bitů musí být doplněn na lichou paritu.

Tab. 3.3 Struktura triple-klíče

triple-klíč délka 192 bitů		
$b_0, b_1,$ … b_{191}		
DES-klíč K1 délka 64 bitů	DES-klíč K2 délka 64 bitů	DES-klíč K3 délka 64 bit
$b_0,$ … b_{63}	$b_{64},$ … b_{127}	$b_{128},$ … b_{191}

KTRANS je definován jako 384 bitů skládajících se ze dvou triple-klíčů KTRANS1 a KTRANS2.

Každý DES-klíč KMAC je šifrován a dešifrován pomocí KTRANS2 podle triple-DES procesu. KMAC je triple-klíč (skládá se ze 192 bitů).



Obr. 3.1 KMAC šifrování s KTRANS2 (K1, K2, K3) a triple-DES

Relační klíč je odvozen během autentizace rovnocenných jednotek pomocí KMAC klíče. Relační klíč je pro každé spojení jiný a může být sdílen pouze jednotkami, které sdílejí autentizační klíč (KMAC klíč). Jedná se o jeden klíč (192 bitů), který je složen ze tří 64 bitových DES klíčů.

Odvození relačního klíče mezi ETCS jednotkami:

Náhodné číslo $R_X (x \in \{A,B\}$ je rozděleno na levý (R_X^L) a pravý (R_X^R) 32 bitový bloky.

$$R_A = R_A^L \mid R_A^R \tag{3.1}$$

$$R_B = R_B^L \mid R_B^R \tag{3.2}$$

$$K_{S1} = MAC\ (R_A^L \mid R_B^L, K_{AB}) = DES\ (K_3, DES^{-1}(K_2, DES(K_1, R_A^L \mid R_B^L))) \tag{3.3}$$

$$K_{S2} = MAC\ (R_A^R \mid R_B^R, K_{AB}) = DES\ (K_3, DES^{-1}(K_2, DES(K_1, R_A^R \mid R_B^R))) \tag{3.4}$$

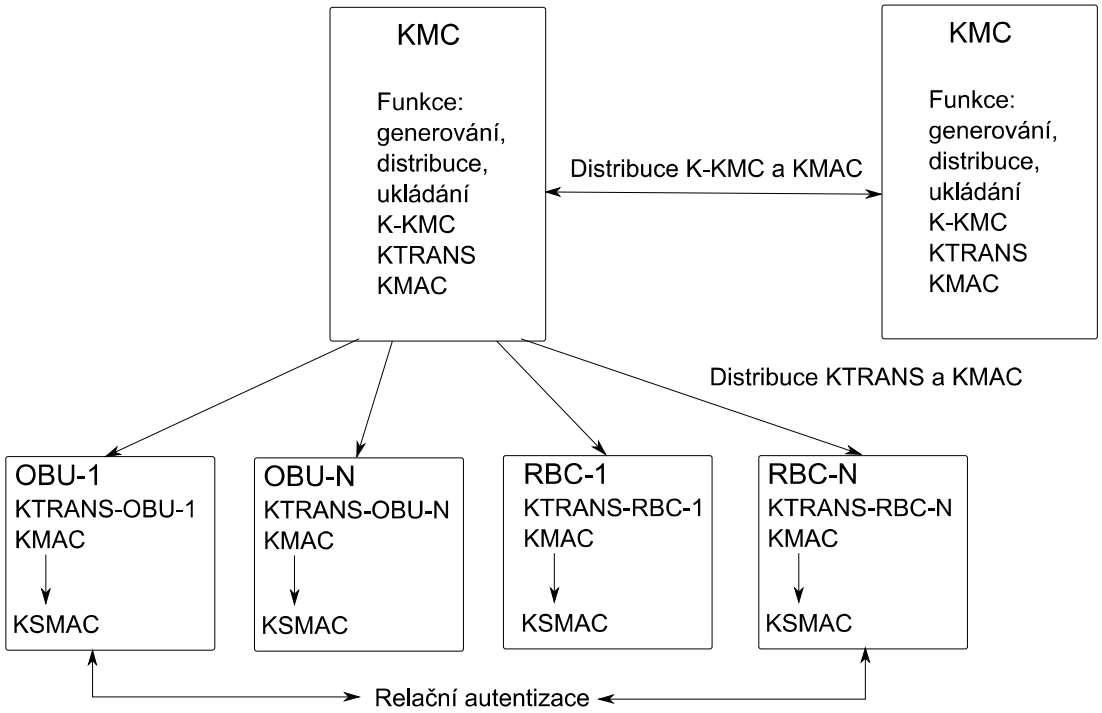
$$K_{S3} = MAC\ (R_A^L \mid R_B^L, K'_{AB}) = DES\ (K_1, DES^{-1}(K_2, DES(K_3, R_A^L \mid R_B^L))) \tag{3.5}$$

3.3 Platnost klíčů

Doba platnosti má být definována začínajícím datem následovaná konečným datem platnosti pro KMAC (Formát data je HH DD MM RR). Formát 0xFFFFFFFF je určen pro neomezenou dobu platnosti. Datum platnosti je kontrolován před každým navázáním spojení. Pokud datum platnosti vyprší během navázaného bezpečného spojení, toto spojení není přerušeno.

3.4 Obecný princip

Následující obrázek popisuje architekturu používanou pro klíčový management systém.



Obr. 3.2 Systémová architektura klíčového managementu

3.4.1 Klíčové management centrum – KMC

Jedna z domén je definována jako KMC a všechny palubní a traťové jednotky používají svou KMC (domácí KMC). KMC je zodpovědný za generaci klíčů potřebných ke zřízení bezpečného spojení mezi traťovými prvky, patřícími do jeho domény a všemi palubními jednotkami. KMC musí být schopna jednoznačně identifikovat všechny generované klíče. I když je možné přidělit stejný klíč pro KMAC různých palubních jednotek, klíčové identifikátory musí být rozdílné pro každou palubní jednotku. KMC je také zodpovědný za distribuci, aktualizaci a rušení KMAC pro všechny traťové a palubní jednotky jeho domény a propojení na příslušné KMC. KMC musí zajistit, že se doba platnosti pro dva následující klíče, pro stejný účel, nebude překrývat. KTRANS1 se používá k zajištění ochrany dat mezi subjektem a jejím domácím KMC. KTRANS2 se používá k posílání zašifrovaného KMAC klíče z domácího KMC jeho subjektům, z bezpečnostních důvodů. Každá transakce mezi ETCS entitou a domácím KMC je iniciována domácí KMC. Každý požadavek mezi domácí KMC a ETCS entitou je označen číslem transakce. Toto číslo transakce slouží pouze k tomu, aby KMC odpovídalo na správný požadavek. KMC je odpovědný za vytváření

transakčního čísla pro své účely. ETCS entita musí odpovídat s odpovídajícím transakčním číslem vysílaným s KMC žádostí v příslušné odpovědi.

3.4.2 ETCS entita

Každá palubní a traťová jednotka obdrží všechny potřebné klíče od svoji domácí KMC a každý subjekt odpovídá pouze jedné domácí KMC. Palubní a traťové jednotky používají pouze svoji domácí KMC pro účely správy klíčů. Každá ETCS entita očekává obdržení unikátního identifikátoru pro každý distribuovaný klíč. Unikátní ID klíče se skládá z ID ETCS KMC, který vydal klíč a klíčové sériové číslo. Dohled nad vlakem pomocí ETCS nesmí být ovlivněn transakcí klíčů. Nesmí dojít ke změně klíčů, pokud to nenařídil domácí KMC. Palubní jednotka má být schopna uložit 2000 klíčových relací, které obsahují spojitost mezi traťovou jednotkou, KMAC a dobou platnosti.

3.5 Funkce klíčového managementu

3.5.1 Základní funkce KM

Zde budou uvedeny základní KM funkce důležité pro řádnou interoperatibilitu. Základní KM funkce jsou povinné.

Definice KMC domény:

Na základě rozhodnutí železničních řídících a schvalovacích orgánů, KMC správce definuje, které ERTMS entity musí být součástí KM domény. KMC správce obsahuje následující informace:

- ETCS-ID KM domény.
- Seznam traťových jednotek zařazených v doméně.
- Seznam OBU jednotek, které patří do domény.
- Definice KMAC přidělovacích pravidel.
- Identifikace dalších domén, kde by její domácí OBU jednotky měly mít možnost být přijaty.
- Identifikace dalších domén, ze kterých by zahraniční OBU jednotky mohly být přijaty.

Instalace KMC:

KMC správce má zajistit úplnost všech zajišťovaných úkolů k nastavení zařízení schopné provádět následující operace s určeným zabezpečením.

- Generování klíčů

- Odeslání klíčů dalším KMC
- Přijmutí klíčů od dalších KMC
- Vymazání klíčů
- Archivování klíčů
- Ověřování klíčů
- Vypracovat protokol o činnosti

Vyjednání K-KMC:

KMC správce má vyjednat K-KMC pro každý KMC s kterým je požadována výměna klíče. Různé řešení jsou možná a dohoda je potřebná mezi dotčenými správci, např.:

- Jeden KMC správce generuje, ověřuje a distribuuje klíč dalším.
- Každý KMC správce generuje část klíče, distribuuje ho dalším, pak oba ověří výsledný klíč a používají ho, pokud bylo ověření úspěšné.
- Oba KMC správci obdrží klíč od nezávislého generátoru klíčů, zodpovědného za vytváření a ověřování klíče.

Bez ohledu na přijaté řešení, důvěrnost K-KMC musí být garantována nezúčastněnou KMC.

Generování KMAC:

Generování klíčů má být provedeno KMC podle bezpečnostních požadavků interoperabilních aplikací ERTMS. Konkrétní technická řešení není třeba harmonizovat (za předpokladu, že je bezpečnost zajištěna). Generované KMAC pro interoperabilní jednotky musí být ověřena generující KMC. Unikátní sériové číslo musí být spojeno s každým generovaným KMAC.

Výměna KMAC s dalším KMC:

Vysílací KMC správce má indikovat, které OBU entitě je KMAC určena. Přijímací KMC správce má potvrdit přijetí a přijmout nezbytná opatření při zavádění KMAC do provozu.

Distribuce KMAC:

Aktualizace KMAC:

KMC správce rozhodne, kdy je vhodné aktualizovat KMAC. Rozhodnutí o aktualizaci klíče je přijato podle předdefinovaného klíčového plánu obnovy nebo v případě detekce nebezpečné situace (ztráta důvěrnosti). Klíčový obnovovací plán musí být přijat v rámci dohody mezi KMC. Mělo by být možné aktualizovat KMAC jak během údržby tak v normálním provozu.

Mazání KMAC:

KMC správce má mít možnost žádat další KMC administrátory o vymazání klíčů. Důvod k žádosti vymazání má být uveden. V případě vymazání klíče je požadováno, aby všechny kopie klíče byly vymazány. KMC správce musí potvrdit původci požadavku, že odstranění klíče bylo kompletní.

Mazání K-KMC:

KMC správce má informovat ostatní KMC správce o vymazání K-KMC klíče. KMC správce má zajistit, že všechny kopie klíče byly vymazány.

Archivování klíčů a KM transakcí:

KMC správce má uchovávat všechny důvěrné informace o vyrobených klíčích, včetně:

- Přiřazení klíčů jednotkám
- Stav klíče (např. v současné době používaný, odstraněný, ohrožený, čeká na potvrzení o výměně/vymazání)

Správa různých typů uživatelů:

KMC má umožnit řídit následující typy uživatelů:

- KMC správce
- KMC operátora
- KMC údržbáře

3.5.2 Funkce KM mezi KMC a ETCS entitami

Následující část specifikuje základní funkce klíčového managementu, které jsou požadované pro efektivní klíčový management mezi KMC a ETCS entitami. Jsou definovány dva různé řídící klíčové způsoby pro instalaci, aktualizaci a odstranění klíčů:

- „all“ řídící klíčová metoda – kompletní sada klíčů je instalována v ETCS entitě, pokud KMC chce přidat, upravit nebo vymazat klíče, úložiště klíčů této jednotky je kompletně automaticky vymazáno před změnou.
- „single“ řídící klíčová metoda – KMC požaduje instalaci, úpravu nebo vymazání pouze jednoho klíče v ETCS entitě.

Každá ETCS entita musí implementovat minimálně jednu z těchto metod. KMC musí znát řídící metodu použitou v každé ETCS entitě, která se nachází v jeho doméně a musí vydávat odpovídající kompatibilní žádosti, kterými jsou:

Instalace transportního klíče:

Tato funkce je používaná k distribuci transportního klíče z KMC do ETCS entit. Když je instalovaný nový KTRANS do ETCS entity, starý je nahrazen, pokud existuje. Instalace sama o sobě nemá vliv na platnost již nainstalovaných autentizačních klíčů v ETCS entitě.

Nahrazení všech autentizačních klíčů:

Tato funkce má být použita KMC k nahrazení kompletní sady autentizačních klíčů ETCS entity pod vedením KMC. Efektem této funkce je odstranění všech autentizačních klíčů před nainstalováním nových klíčů. K následnému provedení instalace je potřebný vhodný transportní klíč.

Vymazání všech klíčů:

Tato funkce je používána domovským KMC k mazání různých druhů klíčů nainstalovaných domácí KMC v ETCS entitě.

Vymazání má být doloženo u následujících druhů klíčů:

- Všechny autentizační klíče nainstalované domácí KMC.
- Transportní klíče nainstalované domácí KMC.
- Všechny klíče distribuované KMC do ETCS entity, včetně transportních klíčů.

Vymazání musí být provedeno takovým způsobem, že vymazané klíče nemohou být obnoveny. K mazání je potřebný odpovídající transportní klíč. Pokud je požadováno vymazání transportního klíče, oznamovací zpráva má použít předdefinovaný klíč ke generování autentických kódu.

Přidání autentizačního klíče:

Tato funkce má být použita KMC k přidání jednoho autentizačního klíče do ETCS jednotky. K provedení instalace je potřebný vhodný transportní klíč.

Vymazání autentizačního klíče:

Tuto funkci používá KMC k odstranění jednoho autentizačního klíče v ETCS entitě. Vymazání se musí provést tak, že v ETCS entitě nedojde k obnovení klíče. ETCS entita nesmí nikdy odstranit svůj autentizační klíč, ani v případě vypršení platnosti. Příkaz k vymazání má být vždy nařízen domácí KMC. K provedení vymazání je potřebný vhodný transportní klíč.

Výměna ETCS entity:

Tato funkce má být použita KMC k výměně seznamu rovnocenných ETCS entit instalovaného autentického klíče. Alespoň jedna ETCS rovnocenná entita má být uvedena v žádosti. Po přijetí žádosti, ETCS entita nahradí seznam ETCS entit napojených na autentický klíč seznamem přiloženým v žádosti. Tato funkce se vztahuje pouze na palubní jednotky. K provedení výměny je potřebný vhodný transportní klíč.

Aktualizace doby platnosti klíče:

Tato funkce se má používat k aktualizaci doby platnosti klíčů (začátek a konec data), klíčů již nainstalovaných v ETCS entitě. Aktualizace doby platnosti klíče nemá vliv na další vlastnosti klíčů. K provedení aktualizace je nutný vhodný transportní klíč. Povinností KMC je, že žádné dva klíče nainstalované v ETCS entitě nebudou platit ve stejnou dobu.

3.6 Klíčový management transakcí

Tato část definuje strukturu transakční zprávy vyměňující se mezi KMC a ETCS entitami. Je třeba rozlišovat dva typy zpráv.

- klíčové management žádosti (Instalace transportního klíče, vymazání všech klíčů, atd.)
- klíčové management oznamující zprávy

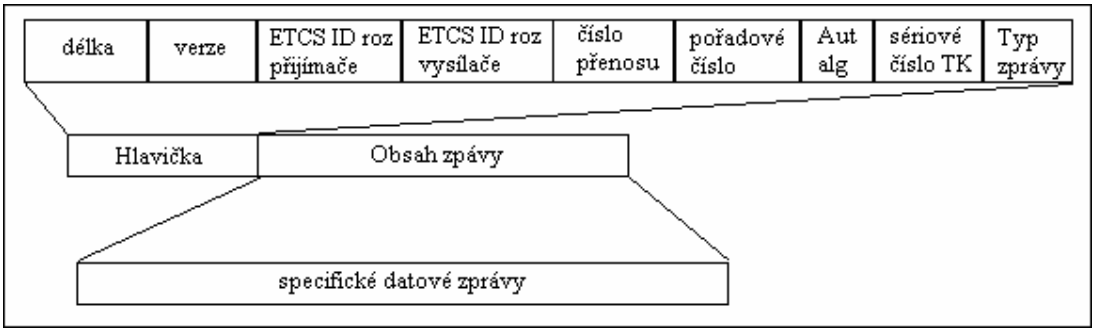
Klíčové management žádosti jsou generovány v KMC a předkládány ETCS entitě. ETCS entita odpovídá na žádost pomocí oznamujících zpráv. Tyto oznamující zprávy buď potvrdí přijetí žádosti nebo obsahují pozitivní či negativní výsledek zpracování.

Jedinečný identifikátor se skládá z ETCS ID a typu ETCS ID a je přiřazen ke každé ETCS entitě a KMC. Dále se používá fráze „ETCS ID rozšířená“ pro tento identifikátor. Kódování je následující:

Tab. 3.4 Kódování ETCS ID rozšířené

7654 3210 (bit)	Kódování polí
xxxx xxxx	Typ ETCS ID (1 oktet)
yyyy yyyy yyyy yyyy yyyy yyyy	ETCS ID (3 oktety)

Všechny zprávy jsou uváděny v binárním kódu, použití big-endian reprezentace.



Obr. 3.3 Obecná struktura zprávy

Záhlaví zprávy se skládá z délky, verze, unikátního identifikátoru přijímače a vysílače, čísla přenosu, pořadového čísla, autentizačního algoritmu, transportního klíčového sériového čísla a typu zprávy.

3.6.1 Oznamující zprávy

Po přijmutí a zpracování klíčové management žádosti, ETCS entita vrátí oznamující zprávu KMC. Na každou žádost je odpovídáno oznamující odpovědí. Na úspěšné zpracování žádosti je odpovídáno použitím návratového kódu „úspěch“.

Je-li zpracování kódu opožděné, může být přijetí žádosti oznámeno použitím návratového kódu „přijetí úspěšné“. Toto je pouze indikační zpráva pro KMC a jednotka stále musí vrátit výsledek po zpracování žádosti.

Selhání při zpracování, neznámý příjem nebo nepodporované žádosti jsou indikovány ETCS entitou, použitím odpovědi s návratovým kódem jiným než „úspěch“ nebo „úspěšný příjem“. Po obdržení neznámé, nepodporované žádosti nebo selhání musí toto být indikováno ETCS entitou.

Číslo transakce oznámení musí být nastaveno podle čísla transakce příslušné žádosti, za účelem vytvoření žádost – oznámení relace. Pořadí čísel uvedené v záhlaví oznamující zprávy musí být nastaveno na pořadové číslo příslušné žádosti.

4 Bezpečnostní požadavky na kryptografické moduly

V normě FIPS 140-2 jsou stanoveny bezpečnostní požadavky na kryptografické moduly využívané v rámci bezpečných systémů pro ochranu citlivých dat v počítačových a telekomunikačních systémech. V této normě jsou definovány čtyři úrovně zabezpečení, které pokrývají široké spektrum možného použití kryptografických modulů. Požadavky pro jednotlivé úrovně jsou popsány v jedenácti oblastech, které se vztahují k bezpečnému návrhu a implementaci modulu. [10]

Kryptografický modul má být testován podle požadavků každé oblasti. Kryptografický modul má být nezávisle ohodnocen v každé z těchto oblastí a pak je mu přidělena jeho bezpečnostní úroveň v každé oblasti zvláště. Výsledná bezpečnostní úroveň kryptografického modulu je pak určena podle nejnižší získané úrovně, třebaže tato nejnižší úroveň byla prokázána jen v jediné testované oblasti.

Bezpečnostní úroveň 1 poskytuje nejnižší úroveň bezpečnosti. Jsou zde specifikovány pouze základní požadavky na kryptografický modul (např. má být použit alespoň jeden schválený algoritmus nebo uznaná bezpečnostní funkce). Touto úrovní nejsou

vyžadovány žádné specifické fyzické bezpečnostní mechanismy kryptografického modulu. Příkladem bezpečnostní úrovně 1 jsou šifrovací desky u osobního počítače.

Bezpečnostní úroveň 2 zajišťuje větší bezpečnost zvýšením fyzického zabezpečení kryptografického modulu, protože je vyžadována evidence průniků, která se zjišťuje použitím kvalitních zámků či pečetí. Tato úroveň požaduje minimálně autentizaci založenou na rolích, kterými kryptografický modul ověřuje oprávnění provozovatele převzít určitou roli a provést odpovídající sadu služeb.

Bezpečnostní úroveň 3 dále zvyšuje fyzickou bezpečnost oproti bezpečnostní úrovni 2. Fyzické bezpečnostní mechanismy mají mít velkou pravděpodobnost odhalení průniku. Při odhalení průniku pomocí speciálních obvodů budou citlivá data vymazána. Bezpečnostní úroveň 3 vyžaduje autentizaci založenou na ověřování identity, což je rozšíření oproti rolím. Citlivá data, která nejsou zašifrována při opouštění modulu, by měla použít speciální porty či rozhranní, které jsou fyzicky oddělené.

Bezpečnostní úroveň 4 je tou nejvyšší úrovní zabezpečení, kterou definuje norma. Zařízení této úrovně by měla být schopna reagovat na všechny neautorizované pokusy o fyzický průnik. Tato zařízení jsou určena pro provoz v nechráněných prostředích. Bezpečnostní úroveň 4 také chrání kryptografický modul proti napadaní skrz změnu okolního prostředí v rozsahu, který neodpovídá normálnímu operačnímu rozsahu napětí a teplot. Tyto nestandardní provozní podmínky by mohly být využity k získání citlivých informací. Moduly tedy musí být testovány, aby tyto útoky nemohly vést k získání citlivých informací.

4.1 Dokumentace kryptografického modulu

Požadavky na dokumentaci se vztahují na veškerou bezpečnost konkrétního hardwaru, softwaru a firmwaru obsaženého v kryptografickém modulu.

Dokumentace má obsahovat hardwarové, softwarové a firmwarové komponenty kryptografického modulu, konkrétní kryptografickou hranici kolem těchto komponentů a popsané fyzické konfigurace modulu. Dokumentace má specifikovat porty, logická rozhraní a všechny definované vstupní a výstupní datové cesty kryptografického modulu. Dokumentace má specifikovat manuální nebo logické kontroly kryptografického modulu, fyzické nebo logické stavové indikátory a platné fyzikální, logické a elektrické charakteristiky.

Dokumentace má obsahovat seznam všech bezpečnostních funkcí, jak schválených tak neschválených, které jsou použity kryptografickým modulem. Má specifikovat všechny operační módy, jak schválené tak neschválené.

Dokumentace má specifikovat blokové schéma zobrazující všechny hlavní hardwarové komponenty kryptografického modulu a propojení komponentů, včetně všech mikroprocesorů, vstupních/výstupních bufferů, řídících bufferů, klíčového úložiště, pracovní paměti a programové paměti.

Dokumentace má obsahovat veškeré informace vztahující se k bezpečnosti, včetně tajných a soukromých kryptografických klíčů (textu a šifrování), autentizačních dat (např. heslo, PIN), CSP, a dalších chráněných informací, jejichž zpřístupnění nebo modifikace může ohrozit bezpečnost kryptografického modulu.

Dokumentace má určit bezpečnostní politiku kryptografického modulu. Bezpečnostní politika má zahrnovat pravidla vyplývající z požadavku normy a pravidla vyplývající z dalších požadavků na dodavatele.

4.2 Porty a rozhraní kryptografického modulu

Kryptografický modul má omezit veškerý informační tok a fyzické přístupové body fyzických portů a logických rozhraní, které definují všechny vstupní a výstupní body modulu. Rozhraní kryptografického modulu má být od sebe navzájem logicky odlišné, přestože může sdílet jeden fyzický port, nebo může být rozdělen do více fyzických portů.

Kryptografický modul má mít následující čtyři logické rozhraní:

Vstupní datové rozhraní:

Veškeré údaje (s výjimkou ovládacích údajů zadaných přes ovládací vstupní rozhraní), které jsou vstupem ke zpracování kryptografickým modulem, mají vstoupit přes toto rozhraní.

Výstupní datové rozhraní:

Veškeré údaje (s výjimkou stavového datového výstupu přes stavové výstupní rozhraní), které jsou výstupem z kryptografického modulu, mají vystoupit přes toto rozhraní. Všechny datové výstupy přes výstupní datové rozhraní mají být zakázány, pokud existuje chybový stav a během automatických testů.

Ovládací vstupní rozhraní:

Veškeré vstupní povely, signály a řídící data používané k řízení operací kryptografického modulu mají vstupovat přes toto rozhraní.

Stavové výstupní rozhraní:

Veškeré výstupní signály ukazatele, a údaje o stavu používané k indikování stavu kryptografického modulu mají výstup přes toto rozhraní.

4.3 Role, služby a autentizace

Kryptografický modul má podporovat povolené role pro operátory a odpovídající služby pro každou roli. Autentizační mechanismy mohou být požadovány kryptografickým modulem k autentizaci operátorova přístupu k modulu, a ověření, že operátor je autorizovaný převzít požadovanou roli a výkon služby v rámci role.

4.3.1 Role

Kryptografický modul má podporovat následující autorizované role pro operátory:

Uživatelská role – Role předpokládá provést obecné bezpečnostní služby, včetně kryptografických operací a jiných schválených bezpečnostních funkcí.

Role kryptografického úředníka – Role předpokládá provádět kryptografické inicializace nebo řídící funkce.

Pokud kryptografický modul umožňuje operátorům provést servisní služby, pak má modul podporovat následující autorizované role:

Role údržby – Role předpokládá provádět fyzickou a/nebo logickou údržbu. Všechny tajné prosté texty, soukromé klíče a nechráněné CSP mají být vymazány při vstupu a výstupu z role údržby.

4.3.2 Služby

Služby se mají vztahovat na všechny služby, operace nebo funkce, které mohou být provedeny kryptografickým modulem.

Kryptografický modul má poskytovat následující služby operátorům:

Zobrazit stav – Výstupem je aktuální stav kryptografických modulů.

Provést automatické testy – Iniciovat a spustit automatické testy.

Provést schválené bezpečnostní funkce – Provede alespoň jednu schválenou bezpečnostní funkci použitou ve schváleném provozním režimu.

Kryptografický modul má poskytovat další služby, operace, nebo funkce, a to schválené i neschválené, včetně služeb uvedených výše. Zvláštní služby mohou být poskytovány ve více než jedné roli.

4.3.3 Autentizace

Autentizační mechanismy mohou být požadovány v kryptografickém modulu k ověření operátorova přístupu a k ověření, že operátor je autorizovaný k převzetí požadované

role a služby v této roli. V závislosti na bezpečné úrovni, kryptografický modul má podporovat alespoň jeden následující mechanismus pro kontrolu přístupu k modulu:

Na rolích založená autentizace: Pokud je tento mechanismus podporován kryptografickým modulem, modul má vyžadovat, aby jedna nebo více rolí byly vybrány buď implicitně nebo explicitně operátorem. Má ověřit předpoklad vybrané role (nebo soubor rolí). Kryptografický modul nepožaduje ověřovat totožnost jednotlivých operátorů. Výběr rolí a ověření převzetí vybraných rolí může být kombinované. Pokud kryptografický modul umožňuje operátorovi změnit role, pak modul má ověřit převzetí každé role, která nebyla ověřena dříve.

Na identitě založená autentizace: Pokud tento mechanismus je podporovaný kryptografickým modulem, modul má vyžadovat, aby operátor byl identifikován individuálně. Má požadovat, aby jedna nebo více rolí byla vybrána explicitně nebo implicitně operátorem a má ověřit identitu operátora a autorizaci operátora k převzetí vybrané role (nebo souboru rolí). Ověření identity operátora, výběr rolí a autorizace k převzetí vybrané role mohou být kombinovány. Pokud kryptografický modul umožňuje operátorovi změnit roli, pak modul má ověřit autorizaci identifikovaného operátora k převzetí role, která nebyla dříve povolena.

4.4 Konečný stavový model

Provoz kryptografického modulu má být popsán pomocí stavového modelu (nebo ekvivalentně) representovaného stavovým přechodovým diagramem a/nebo stavovou přechodovou tabulkou.

Stavový přechodový diagram a/nebo tabulka obsahuje:

- Všechny provozní a chybové stavy kryptografického modulu
- Odpovídající přechody z jednoho stavu do jiného
- Vstupní události, které způsobí přechod z jednoho stavu do jiného
- Výstupní události vyplývající z přechodu z jednoho stavu do druhého

4.5 Fyzická bezpečnost

Kryptografický modul má mít k dispozici fyzické bezpečnostní mechanismy s cílem omezit neoprávněným fyzickým přístupům k obsahu a zabránit neoprávněnému použití nebo změně modulu (včetně nahrazení celého modulu) při instalaci. Všechny hardwarové, softwarové, firmwarové a datové komponenty mají být chráněny v kryptografické oblasti.

Fyzické bezpečnostní požadavky jsou specifikovány pro tři definované typy kryptografického modulu:

- O **Jednočipové kryptografické moduly** jde v případech, ve kterých může být použit jeden integrovaný obvodový čip. Ten je použit buď jako samostatné zařízení nebo může být zabudován ve výrobku, který nemusí být fyzicky chráněný. Například jednočipový kryptografický modul včetně jednoho IC čipu nebo inteligentní karty s jedním čipem.
- O **Vícečipové vestavěné kryptografické moduly** se jedná, pokud je integrováno dva nebo více čipů a jsou vloženy v uzavřeném prostoru nebo výrobku, který může být fyzicky chráněn. Příkladem vícečipových zabudovaných kryptografických modulů jsou adaptéry a rozšiřující desky.
- O **Vícečipové samostatné kryptografické moduly** se jedná, když je propojeno dva nebo více čipů, které jsou fyzicky chráněny krytem. Příkladem jsou samostatné kryptografické moduly včetně šifrovacích routerů.

V závislosti na fyzických bezpečnostních mechanismech kryptografického modulu budou mít pokusy o neautorizovaný fyzický přístup, použití nebo modifikaci modulu vysokou pravděpodobnost odhalení.

- Při pokusu o zanechání viditelných znaků (tj. **sabotážní důkaz**) a/nebo
- Při pokusu, že příslušná opatření by mohla být přijata kryptografickým modulem na ochranu tajného prostého textu, soukromých klíčů a CSP (tj. **sabotážní reakce**)

4.6 Operační prostředí

Operační prostředí kryptografického modulu odkazuje na správu softwarových, firmwarových a hardwarových komponentů potřebných pro funkci modulu. Operační prostředí může být nemodifikovatelné (např. firmware obsažený v ROM), nebo modifikovatelné (např. firmware obsažený v paměti RAM). Operační systém je důležitou součástí operačního prostředí kryptografického modulu.

Obecný účel operačního prostředí odkazuje na použití komerčně dostupných obecně určených operačních systémů, které řídí softwarové a firmwarové komponenty v kryptografické oblasti. Dále řídí systém a operátorské procesy, včetně obecného užití aplikačního softwaru jako jsou textové procesory.

4.7 Klíčový management

Bezpečnostní požadavky na kryptografický klíčový management zahrnují celý životní cyklus kryptografického klíče, kryptografických klíčových komponentů a CSP, které využívá kryptografický modul. Klíčový management zahrnuje náhodné číslo, generování klíče,

distribuci klíče, vstup/výstup klíče, uložení klíče a vymazání klíče. Kryptografický modul může také využívat klíčové management mechanismy jiného kryptografického modulu.

Tajné klíče, soukromé klíče a CSP mají být chráněny v rámci kryptografického modulu před neoprávněným zveřejněním, modifikací a nahrazením. Veřejné klíče mají být chráněny v kryptografickém modulu proti neoprávněným modifikacím a nahrazením.

4.8 Automatické testy

Kryptografický modul má provést spouštěcí testování a podmíněné testování k zjištění, že modul pracuje správně. Spouštěcí testy mají být provedeny, při spuštění kryptografického modulu. Podmíněné testy mají být provedeny, když je vyvolána bezpečnostní funkce nebo operace. Kryptografický modul může provádět další spouštěné nebo podmíněné testy.

Pokud kryptografický modul selže, má vstoupit do chybového stavu a indikovat chybu přes rozhraní stavového výstupu. Kryptografický modul nemá vykonávat žádné kryptografické operace, když je v chybovém stavu. Všechny výstupní data přes rozhraní datového výstupu mají být zakázána, když existuje chybový stav.

4.9 Prohlášení výrobce

Odkazuje na použití nejlepších postupů ze strany dodavatele kryptografického modulu při návrhu, nasazení a provozu kryptografického modulu. Poskytuje záruku, že modul je dostatečně testován, konfigurován, dodán, instalován a vyvíjen, a že je k dispozici řádně vedená dokumentace. Bezpečnostní požadavky jsou určeny pro konfigurační management, dodávku a provoz, vývoj a vedení dokumentace.

4.10 Zmírnění dalších útoků

Kryptografické moduly mohou být citlivé na útoky, pro které testovatelné bezpečnostní požadavky nebyly k dispozici v době, kdy byla vydána tato verze standardu, nebo byly útoky mimo rámec standardu.

5 Úložiště kryptografických klíčů protokolu EURORADIO

V této kapitole je popsán hlavní účel úložiště kryptografických klíčů. Je zde provedena analýza rizik, která jsou spojená s provozováním kryptografického modulu. Dále zde jsou uvedeny požadavky kladené na systém a nakonec je proveden návrh kryptografického

modulu. Tyto kroky jsou provedeny s ohledem na životní cyklus dle normy ČSN EN 50126. [11, 12]

5.1 Koncepce a definice systému

Úložiště kryptografických klíčů protokolu EURORADIO je navrhováno v souvislosti s výstavbou systému ETCS L2. Úložiště kryptografických klíčů protokolu EURORADIO je pouze část systému pro vytváření bezpečné komunikace mezi oprávněnými účastníky v systému ETCS L2. Kryptografický modul slouží v tomto systému k bezpečnému uchovávání a generování kryptografických klíčů, které jsou následně využívány k vytváření bezpečného spojení mezi dvěma oprávněnými účastníky. Kryptografický modul by měl být umístěn na všech lokomotivách vybavených systémem ETCS L2.

Kryptografický modul má podporovat 3DES šifrovací algoritmus, který slouží k získání kryptografického klíče KMAC pomocí klíče KTRANS a také se používá k vytvoření kryptografického klíče K_S. Dále musí modul generovat pseudonáhodná čísla, která jsou potřebná k vytvoření kryptografického klíče K_S. Kryptografický modul dále předává klíče K_S a vygenerovaná pseudonáhodná čísla své nadřazené jednotce, která pomocí nich vytváří bezpečná spojení a zajišťuje integritu a autenticitu vysílaných a přijímaných dat. Dále musí být k dispozici aktuální čas, podle kterého se bude kontrolovat platnost kryptografických klíčů.

Mezi hlavní úkoly kryptografického modulu patří bezpečné uchovávání kryptografických klíčů. Kryptografický modul má zajistit, aby nedošlo k odcizení klíčů a jejich následnému zneužití. Při pokusu o odcizení klíčů, nebo samotného kryptografického modulu, má dojít k vymazání všech citlivých informací.

Přenos kryptografických klíčů KMAC z KMC do kryptografického modulu může probíhat dvěmi metodami. První metoda je přenos klíčů pomocí rádia (online metoda) a druhá metoda je přenos pomocí vyměnitelného média (např. flash disku), které bude manuálně vkládáno do kryptografického modulu (offline metoda).

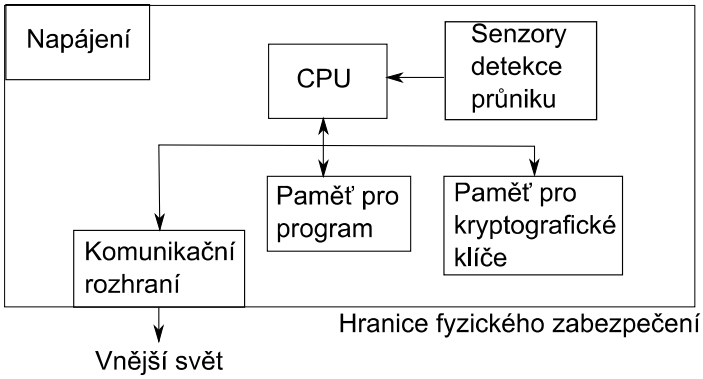
O údržbě kryptografického modulu se může hovořit, když je kryptografický modul vybaven USB konektorem, který je využit pro instalaci nových kryptografických klíčů. Pokud by byly kryptografické klíče posílány pouze pomocí rádia, jednalo by se o bezúdržbové zařízení.

Kryptografický modul je využíván, když se lokomotiva vybavená systémem ETCS L2 pohybuje po trati, která je taktéž vybavena systémem ETCS L2 a dochází ke komunikaci mezi vlakovou a traťovou částí. Protože je třeba chránit uložené kryptografické klíče i po dobu, kdy

se vlak nenachází na trati, která je vybavena ETCS L2, musí kryptografický modul pracovat v úsporném módu po celou dobu, kdy jsou v něm kryptografické klíče uloženy. Z toho vyplývá, že je zapotřebí zařízení nepřetržitě napájet.

Elektrická zařízení na lokomotivě jsou napájena z palubní sítě (24V, 48V a 110V), kde je tolerance napájení -30% a +20% a krátkodobě může dojít u elektrických lokomotiv k poklesu až o 80%. Po vypnutí lokomotivy je stále několik zařízení napájených z baterie (např. požární ústředna, osvětlení). Pokud je to možné, jsou lokomotivy při odstavení napojeny na externí dobíječ.

Kryptografický modul bude umístěn na lokomotivě v místech určených pro systém ETCS L2. Provozní podmínky na lokomotivě jsou nevlídné. Zařízení musí pracovat v prostředí, kde se průměrná roční teplota v místech pro systém ETCS L2 pohybuje okolo 35°C. Teplota vyskytující se v místě pro systém ETCS L2 dosahuje maximálních hodnot až 70°C a minimálních až -25°C. Mezi další nepříznivé vlivy, které se zde vyskytují, patří zejména otřesy, způsobené pohybem lokomotivy, prach a elektromagnetické rušení od dalších elektrických systémů umístěných na lokomotivě.



Obr. 5.1 Architektura kryptografického modulu

5.2 Analýza rizik

Předmětem analýzy rizik je identifikace hazardů ve směru bezpečnosti a spolehlivosti zařízení, určení událostí vedoucích k hazardu a určení závažnosti rizika.

Při poruše kryptografického modulu, dochází k tomu, že není možné navázat bezpečné spojení. Při nemožnosti navázání bezpečného spojení, není možné přenášet povolení k jízdě. To znamená, že lokomotiva dojede až na konec vymezeného úseku, kam má jízdu povolenou a dál se pohybovat nesmí. V takovémto případě musí následně přejít řízení pohybu lokomotivy na náhradní systémy (např. návěstní systém, rádio). Z toho vyplývá, že samotná porucha kryptografického modulu nemůže mít za následek ohrožení bezpečnosti železniční

dopravy (SIL0), ale v důsledku poruchy může dojít ke snížení bezpečnosti železniční dopravy, protože se přejde na náhradní řízení pohybu lokomotivy. Proto je vhodné provést zálohování kryptografického modulu a jako vhodný způsob zálohování může být např. systém 1 ze 2. Při poruše jednoho ze dvou systémů by mělo dojít při nejbližší možné příležitosti k jeho nahrazení (opravě).

Odcizení kryptografických klíčů uložených v kryptografickém modulu by mohlo vést k možnému zneužití těchto klíčů, které by mohlo vést k velmi nepříznivému ovlivnění až ohrožení železniční dopravy. V žádném případě klíče nesmí po uložení do kryptografického modulu tento modul opustit. Pokud by došlo k pokusu o odcizení těchto klíčů z kryptografického modulu, musí být tento pokus identifikován a všechny klíče musí být vymazány. K vymazání všech klíčů musí dojít také v případě, že dojde k pokusu o odcizení kryptografického modulu. Když jsou klíče vymazány, tak není možno navazovat bezpečné spojení. Proto mechanismy pro identifikaci napadení by měly pracovat spolehlivě a nemělo by docházet k náhodnému vymazání klíčů, což by opět snížilo bezpečnost železniční dopravy, z důvodu přechodu na náhradní řízení pohybu lokomotivy.

Další riziko pro kryptografické klíče spočívá v přenosu na kryptografický modul. Když v kryptografickém modulu nejsou nainstalované klíče, musí se tam nejprve nainstalovat transportní klíč, pomocí kterého jsou zašifrované klíče KMAC. Protože transportní klíč KTRANS nemůže být zašifrovaný, je nevhodné ho posílat pomocí rádia. Proto je klíč KTRANS dopraven na lokomotivu pověřenou osobou, která klíč KTRANS přepravuje na přenosném úložném zařízení (např. USB flash disku). To je následně umístěno do USB portu kryptografického modulu a klíč KTRANS je tak nainstalován. Teprve pak mohou být zašifrované klíče KMAC přepravovány do kryptografického modulu pomocí rádia, kde jsou pomocí nainstalovaného KTRANS dešifrovány.

Kdyby došlo k takové poruše kryptografického modulu, při které v něm zůstanou kryptografické klíče uloženy, pak při pokusu o odcizení těchto klíčů nemusí dojít k jejich vymazání. Proto je nutné zajistit, aby při takovéto poruše došlo k rychlé náhradě (opravě) kryptografického modulu. Kdyby tak nebylo učiněno, nebo nebylo zajištěno, že se klíče při jakékoliv poruše kryptografického modulu vymažou, mohlo by dojít ke ztrátě klíčů a prozrazení klíčového tajemství. I kdyby přes všechna opatření došlo k odcizení kryptografických klíčů, tak musí být toto odcizení identifikováno a ukradené klíče musí být vyřazeny z provozu.

Aby nedošlo k prolomení klíčového tajemství, mají se klíče po určité době vyměňovat.

Kryptografický modul by měl splňovat požadavky bezpečnostní úrovně 3 podle normy FIPS 140-2. Úroveň 3 by měla být dostatečná s ohledem na to, že samotný modul je umístěn v chráněném prostoru (lokomotivě).

5.3 Požadavky na systém

Tato část, na základě výše zmíněné studie, doplňuje požadavky na systém a to jak z hledisek funkčních tak i bezpečnostních.

5.3.1 Porty

Pro vytvoření portů existují následující možnosti:

1) Fyzické porty používané pro vstup a výstup prostého textu, kryptografických klíčových materiálů, ověřovacích dat, a CSP mají být fyzicky odděleny od všech ostatních portů kryptografického modulu.
2) Logické rozhraní užívané pro vstup a výstup prostého textu, kryptografických klíčových materiálů, ověřovacích dat, a CSP mají být logicky odděleny od všech dalších rozhraní s využitím důvěryhodných cest.

Prostý text, kryptografický klíčový materiál, ověřovací data, a CSP mají být přímo vloženy do kryptografického modulu (např. přes důvěryhodnou cestu přímo připojenou kabelem).

5.3.2 Fyzická bezpečnost

Při provádění fyzické údržby mají být vymazány všechny tajné prosté texty, soukromé klíče a CSP. Vymazání má být buď procedurální, provedeno operátorem, nebo automatické, provedeno kryptografickým modulem.

Kryptografický modul má poskytnout údaje o manipulaci (např. na krytu, umístěním a těsněním), při pokusu o fyzický přístup k modulu.

Pokud kryptografický modul obsahuje vyměnitelné kryty nebo pokud je definované rozhraní přístupu údržby, pak má modul obsahovat sabotážní reakce a mazací obvod. Sabotážní reakce a mazací obvod má neprodleně vymazat všechen tajný prostý text, soukromé klíče a CSP, když je kryt odstraněn. Sabotážní reakce a mazací obvod má zůstat funkční, když tajný prostý text, soukromé klíče a CSP jsou obsaženy v kryptografickém modulu.

Pokud kryptografický modul obsahuje ventilační otvory nebo štěrbiny, pak otvory nebo štěrbiny mají být konstruovány takovým způsobem, který zabraňuje nepozorovanému fyzickému sondování uvnitř uzavřeného prostoru (např. požaduje alespoň jeden 90° ohyb).

Obvody kryptografického modulu mají být pokryty tvrdým materiálem (např. pevným epoxidovým materiálem), který je neprůhledný ve viditelném spektru. Nebo má být kryptografický modul umístěn v prostoru tak, že pokusy o odstranění nebo vniknutí do uzavřeného prostoru budou mít za následek poškození nebo zničení modulu.

5.3.3 Operační systém

Všechen software a firmware určený pro šifrování má být instalován ve formě, která chrání softwarové a firmwarové zdroje a spustitelný kód před neoprávněným zveřejněním a modifikací.

Šifrovací mechanismy používající schválené integritní techniky (např. schválený ověřovací kód zprávy), mají být aplikovány na všechny šifrovací softwarové a firmwarové komponenty v kryptografickém modulu. Tento požadovaný šifrovací mechanismus může být začleněn jako součást softwarového/firmwarového testu integrity, pokud se používá pro tento test schválená ověřovací technika.

Pro ochranu prostých textových dat, šifrovacího softwaru a firmwaru, kryptografických klíčů, CSP a ověřovacích dat, se diskrétní mechanismy řízení přístupu k operačnímu systému nakonfigurují tak, aby:

- Určily množinu rolí, které mohou vykonat uložení šifrovacího softwaru a firmwaru.
- Určily množinu rolí, které mohou upravit (tj. psát, nahradit a odstranit) následující softwarové nebo firmwarové složky uložené v kryptografické oblasti: šifrovací programy, šifrovací data (např. kryptografické klíče a auditorská data), CSP a prostá textová data.
- Určily množinu rolí, které mohou číst následující šifrovací softwarové komponenty uložené v kryptografické oblasti: šifrovací data (např. kryptografické klíče), CSP a prostá textová data.
- Určily množinu rolí, kterými mohou vstoupit kryptografické klíče a CSP.

Operační systém má bránit všem operátorům a vykonávajícím procesům v modifikaci probíhajících šifrovacích procesů (např. načtení a provádění šifrovacích programů).

Operační systém má bránit provozovatelům a vykonávajícím procesům ve čtení šifrovacích softwarů uložených v kryptografické oblasti. Operační systém má zajistit audit mechanismů zaznamenávajících modifikace, přístupy, vymazání a přidání kryptografických dat a CSP.

Všechny kryptografické klíče a CSP, ověřovací data, řídící vstupy a stavy výstupů mají být sdělovány prostřednictvím důvěryhodného mechanismu.

5.4 Rozdělení požadavků na subsystémy a návrh

V této kapitole je provedeno přiřazení funkčních, bezpečnostních a spolehlivostních požadavků k jednotlivým subsystémům. Navrhnutí subsystémů a dílů odpovídajících požadavkům.

5.4.1 Napájecí obvody

Napájení kryptografického modulu je zajištěno pomocí dvou DC-DC konvertorů. Každý napájí jeden mikroprocesor, aby byla zajištěna funkce i při poruše jednoho DC-DC konvertoru. DC-DC konvertory budou umístěné jako samostatné moduly, jelikož bude třeba tří různých druhů konvertorů pro tři různé palubní sítě, jež se mohou vyskytovat na lokomotivě (24V, 48V a 120V). Kryptografický modul je z palubní sítě napájen nepřetržitě, aby byla zajištěna stálá ochrana kryptografických klíčů.

DC-DC konvertory, které odpovídají všem požadavkům jsou např. RSD-100 series od firmy Mean Well. Do této série patří tři typy konvertorů, které se liší ve velikosti vstupního napětí. Typ RSD-100B-5 mění vstupní napětí 24V (14,4V – 33,6V) na výstupní napětí 5V. Typ RSD-100C-5 mění vstupní napětí 48V (28,8V – 67,2V) na výstupní napětí 5V a typ RSD-100D-5 mění vstupní napětí 120V (57,6V – 154V) na výstupní napětí 5V. Tento DC-DC konvertor je schopný pracovat při teplotách od -40°C do +70°C. Jelikož je konvertor navrhován přímo pro použití na lokomotivě, je odolný proti otřesům a splňuje evropské normy pro EMC. Účinnost těchto konvertorů se pohybuje okolo 90%. MTBF těchto konvertorů je 254 100 hodin. Zařízení indukuje pomocí LED, že pracuje správně.

Napětí z obou konvertorů jsou odděleně přivedeny do kryptografického modulu přes odrušovací kondenzátory. Potom napětí dále vedou přes Schottkyho diody na zálohovací kondenzátory. Zálohovací kondenzátory jsou zde pro zajištění dodávky elektrické energie po odpojení zdroje po takovou dobu, která je potřebná pro vymazání kryptografických klíčů. Za zálohovacími kondenzátory jsou napětí dále rozdělena. Jedna část je použita na napájení obvodů požadujících napětí 5V (4,7V) a druhá část je přivedena na nastavitelný regulátor LM217, který sníží napětí na 2,5V, které je potřebné pro napájení jádra mikroprocesoru XC167CI.

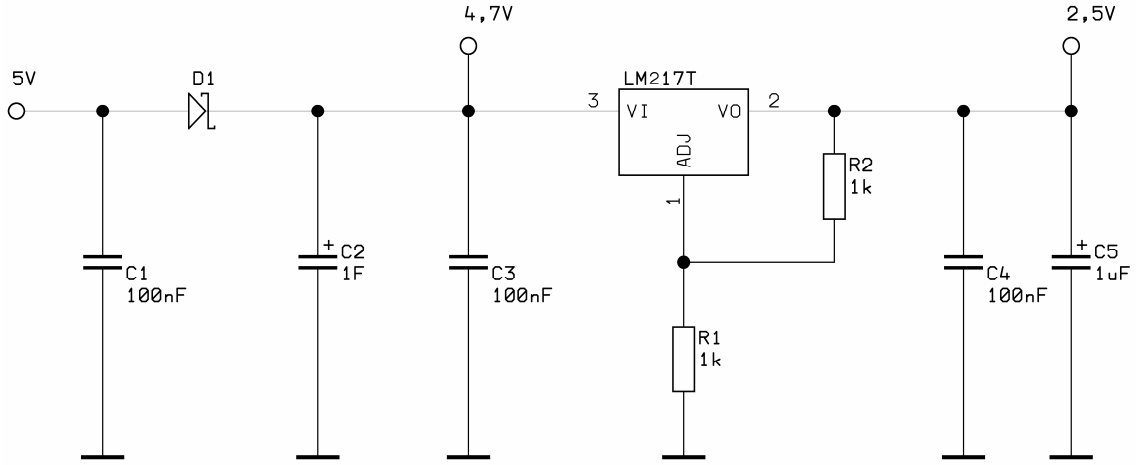
Výstupní napětí regulátoru je nastaveno pomocí dvou odporů R_1 = 1kΩ a R_2 = 1kΩ. Odpory byly určeny z rovnice (5.1). Před a za regulátor jsou přiřazeny kondenzátory o velikosti 100nF a jeden o velikosti 1µF, které zabraňují jeho rozkmitání.

$$U_{OUT} = 1{,}25 \cdot \left(1 + \frac{R_1}{R_2}\right)[V] \tag{5.1}$$

Jako zálohovací kondenzátory jsou použity superkapacitory. Jedná se o dvouvrstvé elektrolytické kondenzátory s vysokou kapacitou, které jsou schopny nahradit záložní baterie. Hlavní výhodou těchto kondenzátorů oproti bateriím je jejich dlouhá životnost, neboť jejich elektrody nepodléhají degradaci ani po mnoha tisících cyklech. Velikost kondenzátoru byla zvolena 1F s ohledem na vyráběné velikosti kondenzátorů a dobu, po kterou je schopen kondenzátor napájet obvody.

$$E = \frac{1}{2} \cdot C \cdot U^2 = \frac{1}{2} \cdot 1 \cdot 4{,}7^2 = 11{,}045J = 11{,}045Ws \tag{5.2}$$

Při maximálním odběru systému (100mA) je schopen kondenzátor napájet tento systém po dobu 23,5s. Tato doba je dostatečná pro vymazání kryptografických klíčů.



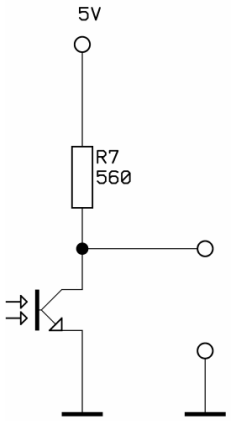
Obr. 5.2 Schéma zapojení napájecích obvodů

5.4.2 Senzory detekce průniku

Hlavním úkolem senzorů detekce průniku je kontrolovat, zda je kryptografický modul chráněn svým krytem, nedošlo k odstranění nebo poničení tohoto krytu a tím k ohrožení kryptografických klíčů uložených v modulu. Pokud senzory detekují odstranění krytu, musí okamžitě informovat mikroprocesor, který následně odstraní všechny citlivé informace (kryptografické klíče).

Jako senzory detekce průniku kryptografického modulu mohou být například použity vhodně umístěné fototranzistory. Na fototranzistory při odstranění krytu dopadne světlo, což

způsobí jejich otevření a tím je detekováno odstranění krytu. Aby byla zajištěna vyšší spolehlivost senzorů, jsou zálohovány a jejich výstupy jsou porovnávány (systém 2 ze 3). Výstupy ze senzorů jsou vedeny přímo na porty mikroprocesoru (49 – 54), kde jsou následně softwarově porovnány a vyhodnoceny. Pokud by alespoň 2 senzory ze 3 měly výstup na úrovni log. 0, došlo by k vymazání klíčů. Senzory jsou zapojeny po dvou trojicích u každého mikroprocesoru a jsou umístěny na opačných stranách desky plošných spojů. Tímto způsobem pokryjí celý prostor kryptografického modulu. Použitelný fototranzistor je např. fototranzistor OP500DA od firmy OPTEK TECHNOLOGY, který detekuje viditelné spektrum elektromagnetického vlnění s pozorovacím úhlem 150°.



Obr. 5.3 Schéma zapojení senzoru pro detekci průniku

Takto zapojený fototranzistor kromě detekce odstranění krytu, také kontroluje zda je kryptografický modul napájen. V případě odpojení napájení, je toto odpojení indikováno mikroprocesoru. Mikroprocesor díky tomu, že je napájen ze zálohovacích kondenzátorů, provede vymazání kryptografických klíčů. Kdyby se klíče se ztrátou napětí nevymazaly, zůstaly by v kryptografickém modulu uloženy bez hlídání. Tímto je zároveň kontrolována poloha kryptografického modulu.

5.4.3 Mikroprocesory

Jako vhodný mikroprocesor byl na doporučení vybrán mikroprocesor XC167CI, jelikož s tímto mikroprocesorem jsou dobré a dlouhodobé zkušenosti.

Tab. 5.1 Specifikace mikroprocesoru XC167CI [13]

Napájení:	2,35 - 2,7V
	4,4 - 5,5V
Architektura:	16-bit kombinace RISC a CISC
Programování:	JTAG
Teplotní rozmezí:	od -40°C do 125°C
komunikace:	USART, CAN, IIC
Paměť:	2 kB DPRAM
	4 kB DSRAM
	2 kB PSRAM
	128 kB Flash
A/D převodník:	10 (8) bitový
Komparátor:	integrovaný
Obvod reálného času:	integrovaný
MTBF	1 546 366 hodin

Pro komunikaci s nadřazenou jednotkou může být využita IIC sběrnice. IIC komunikace je vhodná zejména z toho důvodu, že umožňuje adresování, které se využije k rozlišení obou mikroprocesorů (hlavního a záložního). IIC sběrnice mikroprocesoru XC167CI umožňuje přenosovou rychlost až 400 kbit/s a podporuje jak adresování pomocí 7 bitů tak pomocí 10 bitů. Mikroprocesor je vybaven celkově třemi IIC kanály. Pomocí IIC sběrnice by byly přenášeny kryptografické klíče a náhodná čísla.[14]

Mikroprocesor je programovatelný přes rozhraní JTAG. Joint Test Action Group (JTAG) je standardizovaný normou IEE 1149.1. Druhy signálů, které jsou všeobecně použity pro jakýkoliv JTAG jsou: TDI (Test Data In), TDO (Test Data Out), TCK (Test ClocK), TMS (Test Mode Select). nTRST (Test ReSeT) je volitelný. Přestože je JTAG standardizovaný, konektory k připojení standardizované nejsou.[15]

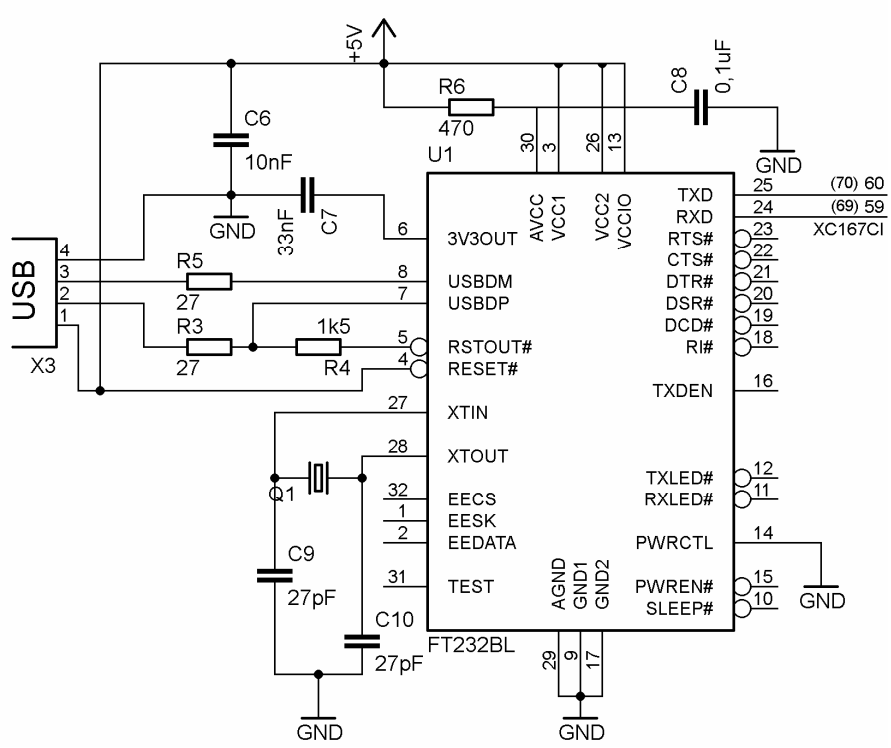
Mikroprocesor je vybaven 128 kB flash pamětí, která slouží k uložení programu. Tuto paměť je možné uzamknout, což zabrání nežádanému přepsání nebo úpravě firmwaru.

Kryptografické klíče budou ukládány na externí datovou paměť SRAM. Zvolená paměť je od firmy ON Semiconductor o velikosti 1Mb [16], aby na ní bylo možno uložit až 2000 klíčů dle požadavků. Kryptografický modul obsahuje dvě tyto paměti, pro každý mikroprocesor jednu.

Obvod reálného času (RTC) je již integrovaný v mikroprocesoru. Tento obvod je využíván pro kontrolu platnosti kryptografických klíčů a také ke generování náhodných čísel. Pro korekci času RTC modulu může být využita nadřazená jednotka, která při každém spuštění pošle aktuální čas na kryptografický modul.

Mikroprocesor generuje výstupní signál, který bude přiveden do nadřazené jednotky a bude ji informovat, že kryptografický modul nepracuje správně. Pokud by hlavní mikroprocesor přestal pracovat nebo nepracoval správně, nadřazená jednotka by začala pracovat se záložním mikroprocesorem. Porucha kryptografického modulu by mohla být dále přenášena (např. pomocí rádia) na zodpovědná místa, které by tak mohly na poruchu kryptografického modulu velmi rychle reagovat.

Jelikož mikroprocesor XC167CI nemá integrované USB rozhraní je potřeba využít konvertorů. Jako vhodný konvertor může sloužit zařízení FT232BL od firmy Future Technology Devices International (FTDI) [17]. FT232BL je kompatibilní s USB 1.1 a USB 2.0. Napájen je 4,35V až 5,25V. MTBF je 247 484 hodin. Schéma zapojení FT232BL je uvedeno na obrázku 5.4. Toto zařízení konvertuje USB rozhraní na sériové UART rozhraní, kterým již je mikroprocesor XC167CI vybaven. USB rozhraní slouží kryptografickému modulu ke komunikaci s KMC (offline metoda). Aby byla umožněna offline komunikace mezi KMC a ETCS entitou, musí být kryptografický modul schopen načítat a ukládat soubory z/na přenositelné médium. Způsob uložení klíčové management žádosti (např. instalace transportních klíčů) a klíčové management oznamující zprávy na přenosném médiu je popsán v [9].



Obr. 5.4 Schéma zapojení FT232BL

Pro zajištění vyšší spolehlivosti jsem do kryptografického modulu umístil dva USB porty a konvertory. Oba konvertory jsou připojeny k hlavnímu mikroprocesoru. Hlavní mikroprocesor zpracovává přijaté žádosti z přenosného zařízení a také je posílá do záložní jednotky po druhé IIC sběrnici. Dále hlavní mikroprocesor vyhodnocuje oznamující zprávy od záložní jednotky s těmi, které vygeneruje sám a ukládá je zpět na přenosné zařízení. Ukládány jsou méně úspěšné oznamující zprávy z obou dvou mikroprocesorů.

Při online komunikaci jsou žádosti od KMC přijaty nadřazenou jednotkou a přes IIC sběrnici jsou odeslány jak do hlavního mikroprocesoru tak do záložního. Oba mikroprocesory provedou potřebné operace a odešlou oznamující zprávy, které jsou porovnány nadřazenou jednotkou. Nadřazená jednotka opět odešle do KMC méně úspěšné oznamující zprávy z obou dvou mikroprocesorů.

5.4.4 Fyzická ochrana kryptografického modulu

Celý kryptografický modul je umístěn do stíněné krabičky, která je kompletně uzavřena bez odnímatelných krytů. Z krabičky jsou vyvedeny 2 USB porty, IIC sběrnice, 4 napájecí vodiče a 2 stavové vodiče. Kryt může být dále opatřen pečetí, aby bylo možno identifikovat otevření kryptografického modulu. Rozměry půdorysu krabičky jsou 150 x 100mm.

5.4.5 Generátor pseudonáhodného čísla

Jedná se o efektivní deterministický program, který generuje posloupnost čísel, která je pokud možno nerozlišitelná od posloupnosti náhodných čísel. Pseudonáhodné generátory jsou klíčovým prostředkem moderní kryptografie. Vstupními daty pro pseudonáhodné generátory jsou náhodné posloupnosti zvané „random seed“, které jednoznačně určují další běh generátoru. V důsledku deterministočnosti těchto programů, jsou nevyhnutelně periodické. Tato perioda může být velmi dlouhá, tudíž téměř nedetekovatelná.

Statistické testování generátoru pseudonáhodného čísla

Statistický test generátoru pseudonáhodných čísel provádí následující statistické testy náhodnosti. Jeden bitový tok 20 000 po sobě jdoucích bitů vystupujících z generátoru pseudonáhodného čísla má být podroben následujícím čtyřem testům. Monobit test, poker test, test běhu, test dlouhého běhu.[10]

Monobit test:

1) Spočítat počet jedniček v 20 000 bitovém toku. Označíme toto množství X.
2) Test je úspěšný pokud: 9 725 < X < 10 275.

Poker test:

1) Rozdělí se 20 000 bitový tok do 4 po sobě jdoucích segmentů, každý po 5 000 bitech. Spočítá se a uloží počet výskytů stejných 4 bitových hodnot z 16 možných. f(i) se označí počet všech 4 bitových hodnot i, kde $0 \leq i \leq 15$.
2) Vyhodnotí se rovnice (5.3):

$$X = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000 \tag{5.3}$$

3) Test je úspěšný, jestliže 2,16 < X < 46,17.

Test běhu:

1) Běh je definován jako maximální posloupnost po sobě jdoucích bitů, buď jedniček nebo nul, které jsou součástí 20 000 bitového vzorkového toku. Výskyty běhu (jak po sobě jdoucích jedniček, tak po sobě jdoucích nul) všech délek (≥1) ve vzorku toku mají být ukládány a počítány.
2) Test je úspěšný, když výskyty běhu jsou v rámci rozsahu příslušného intervalu uvedeného v tabulce níže. Toto musí platit pro nuly i jedničky (všech 12 počítání musí ležet v zadaném intervalu). Pro účely této zkoušky jsou běhy delší než 6 počítány do délky 6.

Tab. 5.2 Požadované intervaly pro test běhu

Délka běhu	Požadovaný interval
1	2 315 - 2 685
2	1 114 - 1 386
3	527 - 723
4	240 - 384
5	103 - 209
6+	103 - 209

Test dlouhého běhu:

1) Dlouhý běh je definován jako běh o délce 26 nebo více (nul i jedniček)
2) Test je úspěšný, pokud na vzorku 20 000 bitů neexistují žádné dlouhé běhy.

Průběžný test generátoru pseudonáhodného čísla:

Generátor produkuje bloky o 64 bitech, první 64-bitový blok generovaný po zapnutí, nebo inicializaci nemá být použit, ale má být uložen pro porovnání s dalším 64-bitovým blokem, který bude generován. Každý následující generovaný 64-bitový blok má být porovnán s dříve vytvořeným blokem. Test je neúspěšný, pokud jsou 64-bitové bloky shodné.

Schválený generátor pseudonáhodného čísla:

Následující generátor pseudonáhodného čísla využívá 3DES šifrovací algoritmus a je schválený NIST. [18]

$$I = ede*K(Dat) \tag{5.4}$$

$$R = ede*K(I \text{ XOR } V) \tag{5.5}$$

Nový V je generován podle rovnice (5.6):

$$V = ede*K(R \text{ XOR } I) \tag{5.6}$$

ede*X(Y) – představuje použití 3DES šifrovacího algoritmu s klíčem *X na data Y.

*K – představuje 3DES klíč, 3 x 64 bitů.

V – je 64 bitová semínková hodnota, která je také držena v tajnosti.

Dat – je datum/časový vektor (64 bitů), který je aktualizován pro každé použití.

R – je požadované 64bitové pseudonáhodné číslo.

5.4.6 3DES šifrovací algoritmus

Jedná se o symetrický šifrovací algoritmus, to znamená, že používá stejné kryptografické klíče pro šifrování na jedné straně a dešifrování na straně druhé. Mezi hlavní výhody symetrické kryptografie patří rychlost a mezi nevýhody patří složitější distribuce klíčů. 3DES algoritmus nahradil nedostačující 56 bitový DES algoritmus. Vylepšení 3DES

oproti DES algoritmu spočívá v tom, že se použije DES algoritmus 3x za sebou. To má za následek snížení celkové rychlosti procesu, ale zvýšení celkové bezpečnosti. 3DES algoritmus může používat pouze 2 různé klíče, potom se jedná o 112 bitovou variantu, nebo může použít tři různé klíče, potom se jedná o 168 bitovou variantu. V protokolu EURORADIO se používá 168 bitová varianta. [19, 20]

Mód provozu 3DES algoritmu použitý v protokolu EURORADIO je ECB (Electronic CodeBook mode). V ECB módu je pro šifrování i dešifrování použit datový blok přímo jako vstup 3DES algoritmu. Znamená to, že vždy když vstoupí stejný blok dat, dostanu i stejný výstupní blok dat, pokud bude použit stejný kryptografický klíč. [21]

Testování kryptografického algoritmu:

Testování kryptografického algoritmu se provádí pomocí známé odpovědi a má být prováděn pro všechny módy (šifrování, dešifrování). Test známou odpovědí se provádí na datech, pro které je správný výstup již známý a porovnává se vypočtený výstup s původně vytvořeným výstupem (známou odpovědí). Pokud vypočtená hodnota výstupu se nerovná známé odpovědi, test je neúspěšný.

Závěr

Hlavním úkolem této práce bylo popsat vlastnosti protokolu EURORADIO a navrhnou vhodné hardwarové a softwarové řešení úložiště kryptografických klíčů protokolu EURORADIO s ohledem na bezpečnostní požadavky.

V prvních dvou bodech je popsáno, kde se protokol EURORADIO používá a je zde uveden popis jeho vlastností. Hlavní popis je soustředěn na vytváření, udržování a ukončování bezpečného spojení. Ve třetím bodě je popsán klíčový management protokolu EURORADIO. Popisuje se zde jak se pracuje s kryptografickými klíči, bez kterých není možno navazovat bezpečné spojení. Ve čtvrtém bodě jsou popsány základní bezpečnostní požadavky, které jsou kladeny na kryptografické moduly podle normy FIPS 1402.

Poslední bod se zabývá návrhem kryptografického modulu pro protokol EURORADIO. Je zde popsána koncepce kryptografického modulu, která zahrnuje použití kryptografického modulu a popisuje pracovní prostředí, ve kterém se bude používat. Dále jsou zde uvedeny požadavky, které má kryptografický modul splňovat. Nakonec je proveden návrh jednotlivých částí kryptografického modulu s ohledem na požadavky, které byly uvedeny dříve.

Jako senzory pro detekci průniku jsem zvolil fototranzistory, ale je možné je nahradit i jinými systémy. Další možným řešením je např. elektrický odvod, který je přímo spojený s vodivým krytem. Odejmutí krytu naruší tento obvod a tím je informován mikroprocesor.

Pro ukládání kryptografických klíčů jsem navrhl použít SRAM paměť. Pokud bych nahradil SRAM paměť pamětí DRAM, nemusel bych kontrolovat přísun elektrické energie, jelikož při přerušení by se všechna data na DRAM automaticky vymazala. Tím by odpadla potřeba zálohovacího kondenzátoru a Schottkyho diody. Hlavní nevýhodou DRAM paměti je mnohem vyšší spotřeba a až o řád nižší spolehlivost oproti SRAM paměti.

Schéma zapojení hlavního mikroprocesoru kryptografického modulu a návrh desky plošných spojů jsou uvedeny v příloze. Cena navrhovaného kryptografického modulu se pohybuje okolo 800Kč.

Možným vylepšením protokolu EURORADIO je nahrazení 3DES algoritmu algoritmem AES. AES algoritmus je novější symetrický algoritmus, který narozdíl od 3DES algoritmu velmi zrychluje celý proces šifrování/dešifrování a zvyšuje i celkovou bezpečnost šifry. Velikost klíče může být 128, 192, nebo 256 bitů. Takovýto přechod na nový šifrovací algoritmus musí být proveden v celém ETCS L2 systému, aby byly zařízení vzájemně kompatibilní. [22]

Po konzultaci byla diplomová práce omezena pouze na návrh hardwaru, kvůli rozsahu práce. Přesto jsou v práci uvedeny požadavky na software a možné řešení některých částí softwaru např. generátor náhodného čísla. Zbylé části zadání diplomové práce jsou splněny v celém rozsahu.

Seznam literatury a informačních zdrojů

[1] Jaroslav Vašátko: Strategie rozvoje projektu ERTMS v České republice v letech 2007 – 2013, Vědeckotechnický sborník ČD č. 21/2006

[2] Jaroslav Čermák: Využití sítě GSM-R pro standardní telekomunikační služby: Diplomová práce, Plzeň, ZČU, 2007

[3] Petr Varadinov: Pilotní projekt ETCS L2 v České republice, Vědeckotechnický sborník ČD č. 28/2009

[4] Fabio Senesi – Enzo Marzilli: European Train Control System Development and implementation in Italy, CIFI, 2007

[5] Václav Chudáček – Libor Lochman: Vlakový zabezpečovací systém ERTMS/ETCS, Vědeckotechnický sborník ČD č. 5/1998

[6] EURORADIO FIS, SUBSET 037, UIC 2005 http://www.era.europe.eu/Core-Activities/ERTMS/Pages/ListofMandatorySpecification.aspx, 10/2011

[7] ČSN EN 50159: Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Komunikace v přenosových zabezpečovacích systémech, Český normalizační institut, Praha, 2011

[8] Off-line Key Management FIS, SUBSET 038, UIC 2011, http://www.era.europa.eu/Core-Activities/ERTMS/Pages/ListOfMandatorySpecifications.aspx, 10/2011

[9] KMC-ETCS Entity offline KM FIS, SUBSET 114, UIC 2011

[10] Federal Information Processing Standards Publication 1402, Security requirements for Cryptographic modules, National Institute of Standards and Technology, 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, 2/2012

[11] Václav Chudáček a kolektiv, Železniční zabezpečovací technika, Praha 2005

[12] ČSN EN 50126: Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS), Český normalizační institut, Praha, 2001

[13] Katalogové listy společnosti Infineon, XC167CI, http://www.keil.com/dd/docs/datashts/infineon/xc167ci_ds.pdf, 4/2012

[14] J. M. Irazabal, S. Blozis: AN10216-01 I^2C MANUAL, Philips Semiconductors, 2003, http://www.nxp.com/documents/application_note/AN10216.pdf, 4/2012

[15] JTAG, Wikipedie, http://cs.wikipedia.org/wiki/Joint_Test_Action_Group, 4/2012

[16] Katalogové listy společnosti ON Semiconductor, N01L83W2A, http://www.onsemi.com/pub_link/Collateral/N01L83W2A-D.PDF, 4/2012

[17] Katalogové listy společnosti Future Technology Devices International, FT232BL, http://www.ftdichip.com/Support/Documents/DataSheets/ICs/DS_FT232BL_BQ.pdf, 4/2012

[18] NIST – Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, National Institute of Standards and Technology, 2005, http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf, 4/2012

[19] National Institute of Standards and Technology Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, National Institute of Standards and Technology, 2008, http://csrc.nist.gov/publications/nistpubs/800-20/800-67.pdf, 2/2012

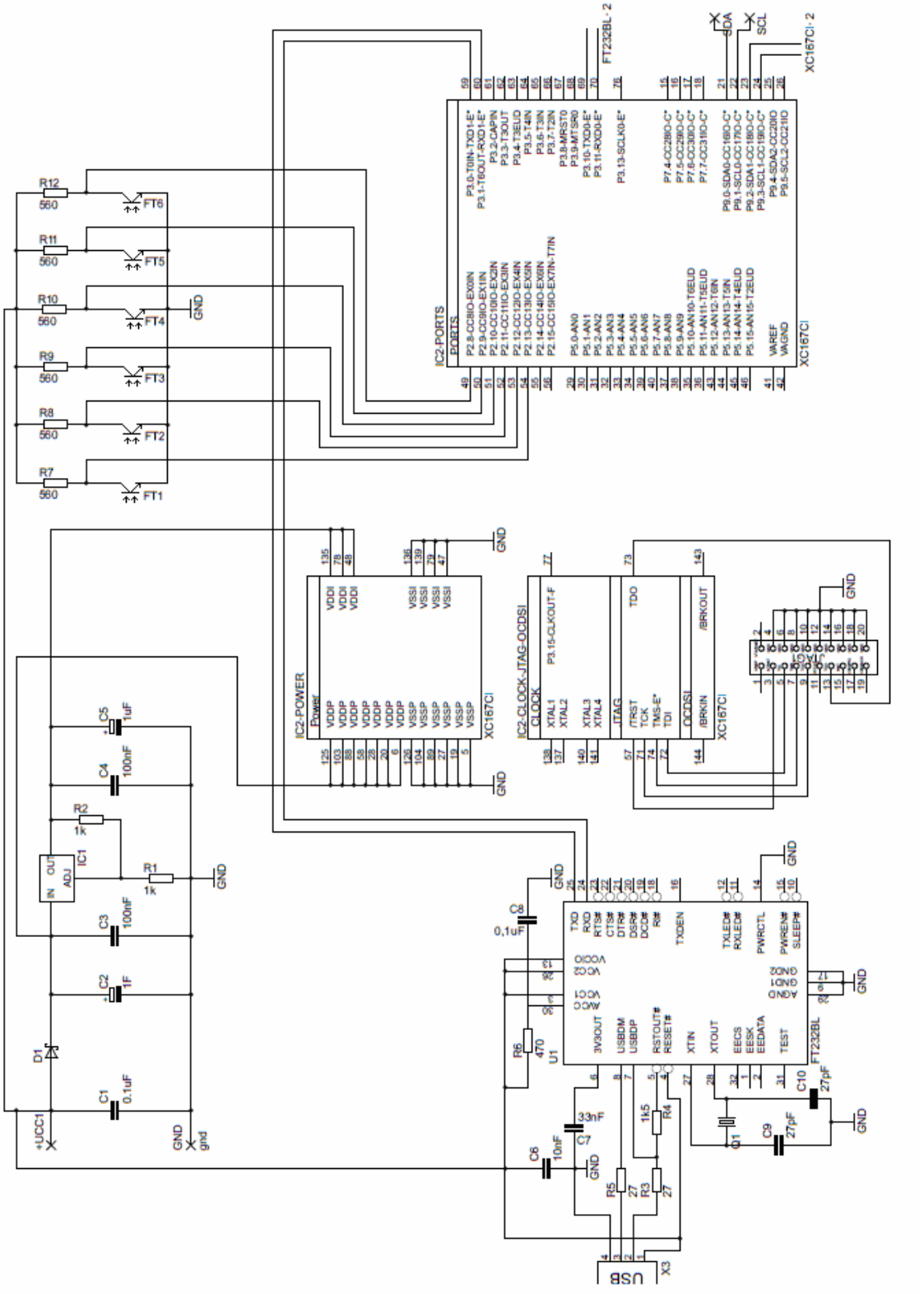
[20] Federal Information Processing Standards Publication 46-3, Data Encryption Standard, National Institute of Standards and Technology, 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 2/2012

[21] National Institute of Standards and Technology Special Publication 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm, National Institute of Standards and Technology, 2000, http://csrc.nist.gov/publications/nistpubs/800-20/800-20.pdf, 2/2012

[22] Federal Information Processing Standards Publication 197, Advanced Encryption Standard, National Institute of Standards and Technology, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2/2012

Přílohy

Příloha A – Schéma zapojení kryptografického modulu



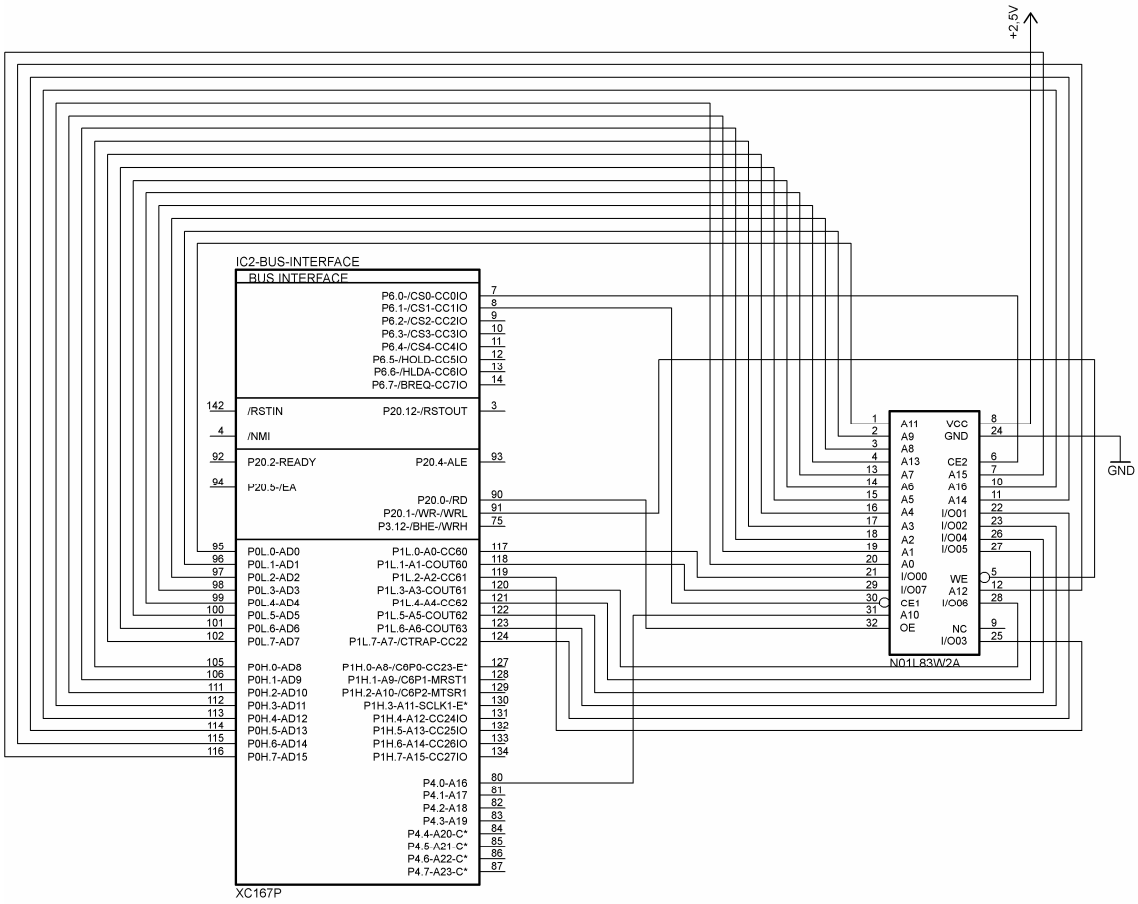
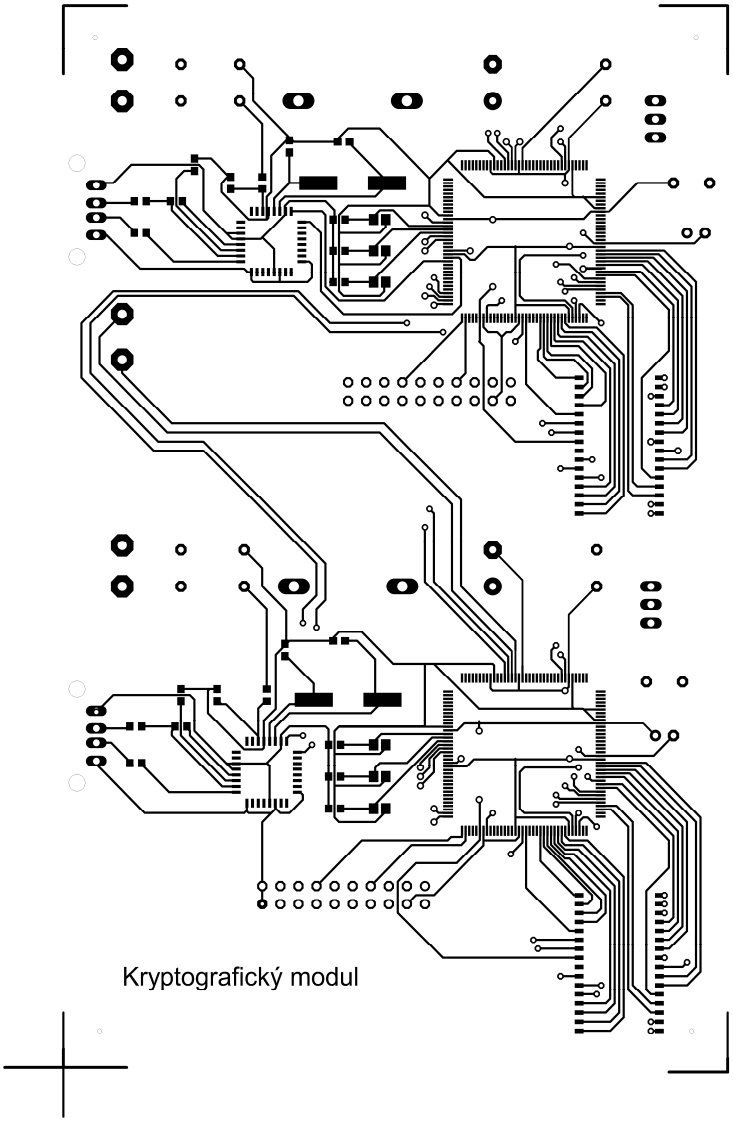
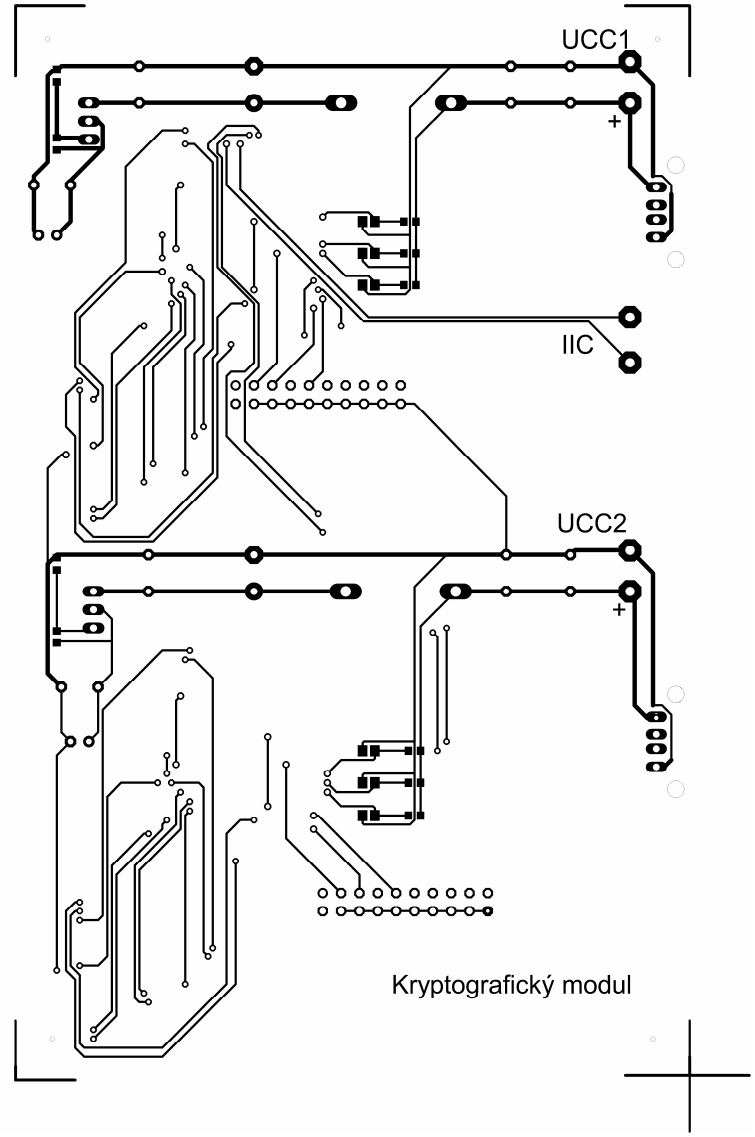


Schéma zapojení SRAM paměti a mikroprocesoru

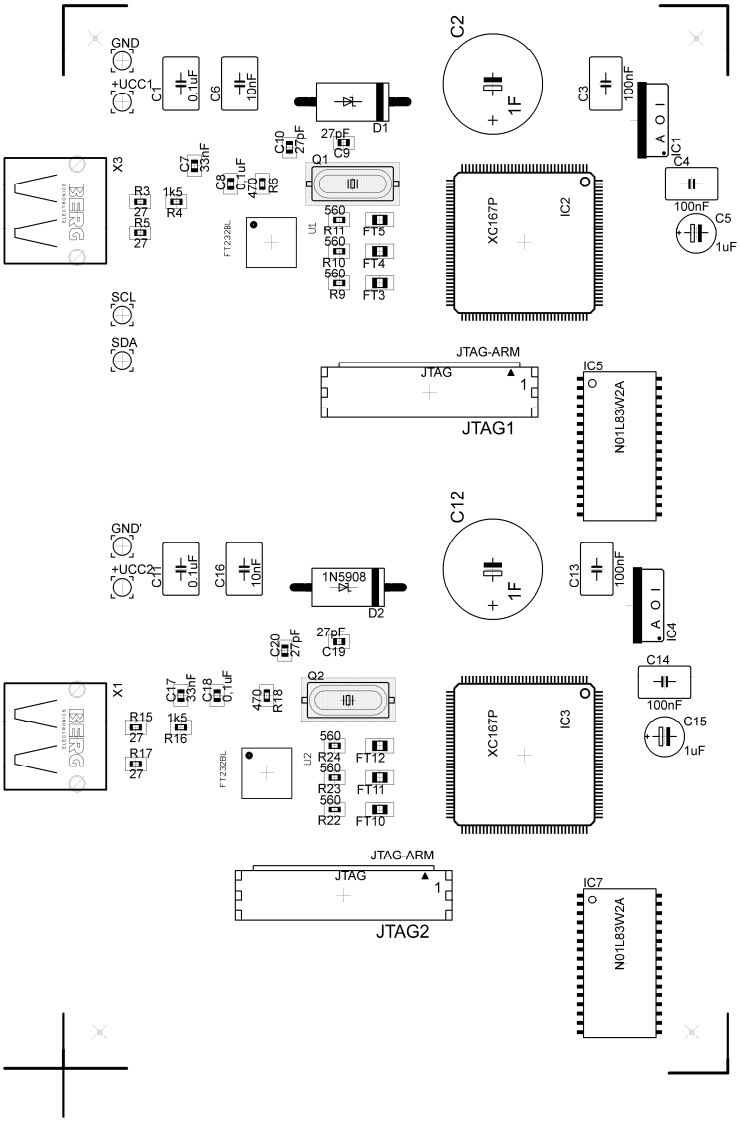
Příloha B – Návrh desky plošných spojů



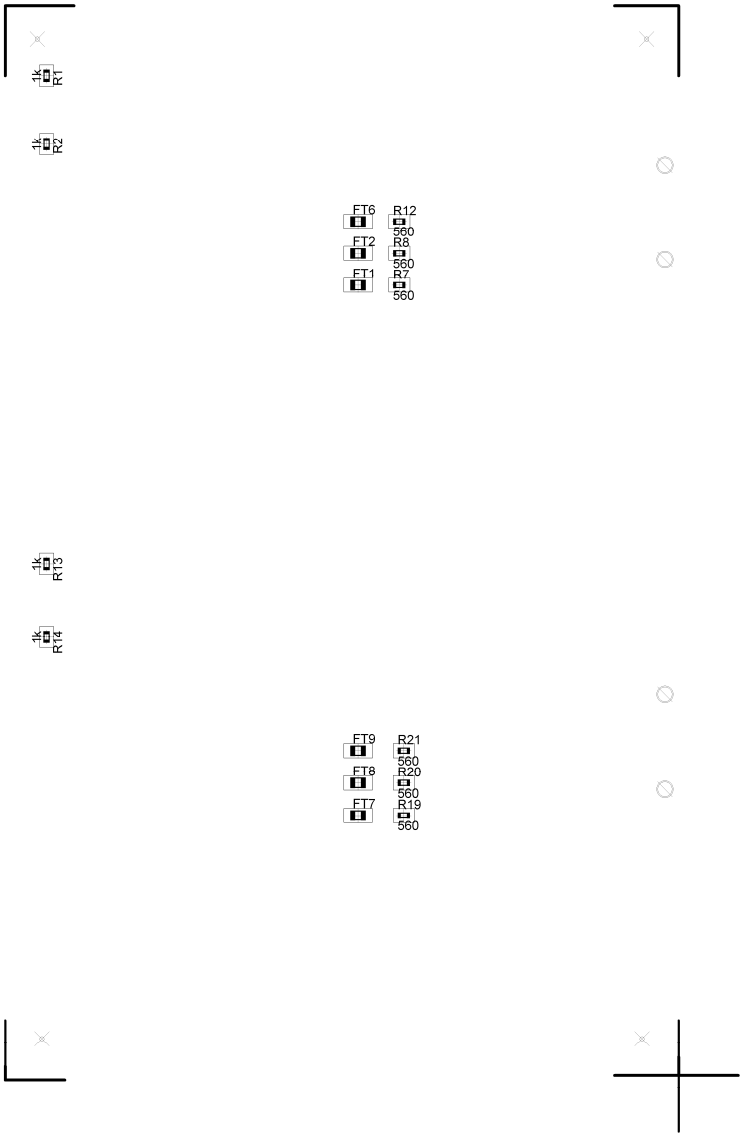
Vrchní vrstva plošného spoje (bez rozlité mědi)



Spodní vrstva plošného spoje (bez rozlité mědi)



Osazení součástek na vrchní vrstvě



Osazení součástek na spodní vrstvě