Definice aplikačního rozhraní systémů EFC založených na globálním navigačním družicovém systému a celulární síti GNSS/CN

4 Definice a zkratky

4.1 Termíny z jiných norem

Tato norma používá následující definice uvedené v ISO 14904.

1) Elektronická peněženka
2) Elektronické vybírání poplatků
3) Vydatel
4) Platební prostředky
5) Metoda platby
6) Platební médium
7) Poskytovatel služby

Tato norma používá následující definice uvedené v ISO 14906.

1) Smlouva
2) Kódování
3) Integrita dat
4) Jednoduchá obsluha

Tato norma používá následující definice uvedené v ISO 17573.

1) Centrální zařízení
2) Klasifikace
3) Uživatel

4.2 Specifické termíny

Pro účely této normy platí tyto definice:

Akce *(Action)*	Operace, kterou může vyvolat aplikační obsah a která se provede v palubním zařízení vozidla
Aktoři *(Actors)*	koherentní množina pravidel, které uživatelé v Případě užití užívají při spojení s těmito Případy užití. Aktor má jednu roli pro všechny Případy užití, kterou ke spojení používá. (UML 1.3)
Centrální Účet *(Central Account)*	Účet určený pro účely EFC, který je obsluhován Poskytovatelem Služeb nebo Entitou, která pracuje v zájmu Poskytovatele Služeb.
Certifikát (Veřejný Klíč) *(Certificate (Public Key))*	Informace veřejného klíče o entitě, která je podepsána Certifikačním orgánem, a je tudíž stanovena neopomenutelnou.
Certifikační orgán	Orgán, jemuž je svěřena důvěra k vytváření a vydávání Certifikátů
Účtovací Objekt *(Charge Object)*	Geografický Objekt, který se používá v Aplikačním obsahu pro stanovení poplatků. Účtovací Objekty definované v této normě jsou Zóna, Koridor a Virtuální Portál.
Třída (informační objekt) *(Class*	Popis řady objektů, které sdílí stejné atributy, operace, metody, vztahy a sémantiku (UML 1.3)

(information object))	
Aplikační obsah (Aplikace EFC) *(Context (EFC Application))*	Část systému EFC za odpovědnosti jednoho Poskytovatele Služeb instalovaná k výběru poplatků pro specifickou část silniční infrastruktury v oblasti spojení, založená na stálé nastavení pravidel, které platí pro celou silniční infrastrukturu, která je předmětem platby
Operátor dohledového systému *(Enforcement Operator)*	Entita EFC, která je odpovědná za kontrolu, že k výběru poplatků dochází podle daných pravidel pro určitý Kontext.
Entita *(Entity)*	Držitel informace v rámci systému, který může být identifikován a adresován jinými držiteli informací z důvodu výměny informací
Událost *(Event)*	Případ zjištěný prostřednictvím OBE, který vede k Akcím.
Funkce *(Function)*	Specifické EFC použití služeb aplikační vrstvy DSRC podle ISO 14906
Geografická Doména *(Geographic Domain)*	Geografický Objekt spojený s Kontextem obklopující oblast, která je předmětem platby v tomto Kontextu.
Geografický Objekt *(Geographic object)*	Informační objekt, který umožňuje definovat kritéria pro polohu vozidla, jenž používá systém EFC, měřené jednotkou GNSS příslušného OBE. OBE porovnává souřadnice měřené jednotkou GNSS se souřadnicemi, které se nachází v rámci Geografického Objektu.
Transformační funkce *(Hash function)*	Funkce, která upravuje řetězce bitů na řetězce o stanovené délce, které splňují následující vlastnosti: Pro daná výstupní data nelze prostřednictvím počítače nalézt vstupní data, která patří k těmto výstupním datům. Pro daná vstupní data nelze prostřednictvím počítače nalézt druhá vstupní data, která patří ke stejným výstupním datům.
Klíč (šifrovací) *(Key (cryptographic))*	Posloupnost symbolů, které řídí operaci šifrovací transformace.
Zpráva s ověřovacím kódem *(Message Authetication Code)*	Řetězec bitů stanovené délky, který se odvozuje od řetězce bitů a Klíče založeném na specifickém algoritmu, splňující následující vlastnosti: Pro jakýkoliv Klíč a jakýkoliv řetězec vstupních dat lze provést výpočet účinně Pro jakýkoliv Klíč, bez upřednostnění znalosti Klíče, nelze prostřednictvím počítače vypočítat řetězec výstupních dat pro jakýkoliv nový řetězec vstupních dat, ani při znalosti řady řetězců vstupních dat a příslušných hodnot řetězců výstupních dat. Hodnotu i-tého řetězce lze zvolit po zjištění hodnoty prvních i-1 hodnot řetězců výstupních dat.
Palubní účet *(On-Board Account)*	Účet založený v OBE, který spravuje finanční prostředky, které jsou obsaženy v jízdence zaslané OBE.
Palubní zařízení *(On-Board Equipment)*	Zařízení umístěné v rámci vozidla podporující výměnu informací skrze rozhraní jeho subjednotek. Skládá se z palubního zařízení a jiných subjednotek, jejichž přítomnost musí být při provádění Transakce nepovinná.
Palubní jednotka (*(On-Board Unit)*	Entita EFC, jež je součástí palubního vybavení a která je vybavena přijímačem GNSS a komunikačním spojem CN.
Platba *(Payment)*	Informační objekt, který vykazuje schválení uhrazení definovaného poplatku za poskytnutou službu a umožňující Entitě EFC předložit tento informační objekt druhé Entitě EFC k zaplacení podle výše poplatku.
Kontrakt o platbě *(Payment contract)*	Smlouva, která se uzavírá mezi Uživatelem a Vydatelem na základě použití Platebních Prostředků pro účely EFC.
Platební scénář *(Payment Scenario)*	Metoda řízení přenosu finančních prostředků, definovaná v této normě, Poskytovateli Služeb za poplatky stanovené v procesu EFC.
Stvrzenka (*Receipt)*	Potvrzení získání příslušných dat pro výběr poplatků, vydané Poskytovatelem Služeb a poslané OBU.
Záznam *(Record)*	Informační objekt, který se ukládá v OBE a obsahuje specifické informace o určité Události.

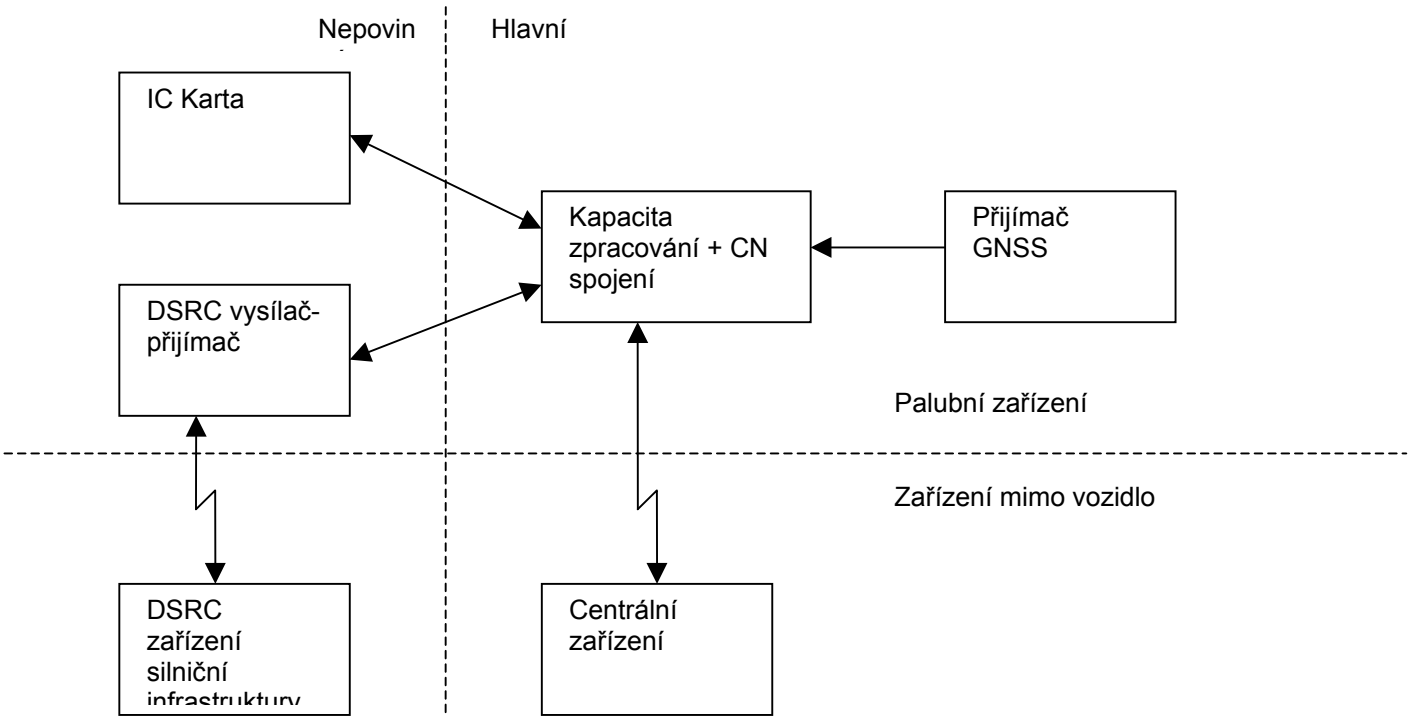
Sektor *(Sector)*	Geografický objekt, který se používá k řízení procesu nahrávání dat mýtného. Sektory se nepřekrývají a celá oblast systému EFC je pokryta Sektory. Kdykoliv se OBE používá pro výběr poplatků, musí mít k dispozici úplná a aktuální data mýtného pro Sektor, ve kterém se vozidlo nachází.
Management sektoru *(Sector Manager)*	Entita EFC, která je odpovědná za provoz a aktualizaci řízení dat EFC spojených s určitým Sektorem.
Segment *(Segment)*	Geografický objekt spojený se Sektorem a podporující proces nahrávání dat mýtného v případě, kdy se vozidlo pohybuje z jednoho Sektoru do sousedního Sektoru. Segment je umístěn kolem společné hranice těchto dvou Sektorů.
Smlouva o poskytování služby *(Service Contract)*	Smlouva uzavřená mezi Uživatelem a Poskytovatelem Služeb z důvodu použití postupů EFC v Kontextech za odpovědnosti Poskytovatele Služeb nebo Entit s ním spojených.
Podpis (elektronický) *(Signature (digital))*	Data připojená nebo zašifrovaná k datové jednotce, která umožňuje příjemci datové jednotky prokázat původ a integritu datové jednotky a poskytnout ochranu před padělaním, například ze strany příjemce.
Jízdenka *(Token)*	Informační objekt, který představuje množství finančních prostředků, jež se použijí pouze v daném Kontextu. Jízdenka se pošle OBE založené na odpovídající platbě.
Data mýtného *(Toll Data)*	Data, která OBE potřebuje pro k provedení procesů EFC podle této normy a podle nastavení Poskytovatelem Služeb.
Transakce *(Transaction)*	Posloupnost výměn informací mezi instancí Centrálního zařízení a Palubního zařízení v rámci rozhraní CN, které je nezbytné pro podporu procesu elektronického vybírání poplatků EFC. Každá taková výměna informací je částí určité Transakce.
Případ užití *(Use Case)*	Specifikace posloupnosti akcí, včetně variant, které může systém nebo jiná Entita provádět při komunikaci mezi aktory systému (UML 1.3)

5 Základní koncepty pro elektronické vybírání poplatků EFC založených na globálním navigačním družicovém systému a celulární síti GNSS/CN

5.1 Úvod

Tento článek týkající se specifikace rozhraní EFC představuje základní koncepty pro EFC založené na GNSS/CN. Připravuje cestu pro případy užití uvedených v článku architektury. Rozvíjí scénáře, které poskytují základ pro budoucí struktury jednotlivých tříd, které musí zahrnovat metody a datové prvky. Poskytuje podklady pro strukturu transakce a obsahy transakce uvedené v této normě.

Základním konceptem takového přístupu k EFC je, že palubní zařízení vozidla (OBE) musí obsahovat prostředek k sebelokalizaci v rámci silniční sítě nebo oblasti, která je předmětem platby. Tato metodika není předmětem této normy. OBE také obsahuje podrobnosti o příslušném poplatku a procesu platby a stanovuje, kdy je potřeba příslušná data nahrát, zpracovat nebo odeslat ve shodě s tímto procesem. Ukázkový příklad fyzické architektury je zobrazen na obrázku 1.



Obrázek 1 – Ukázkový příklad fyzické architektury

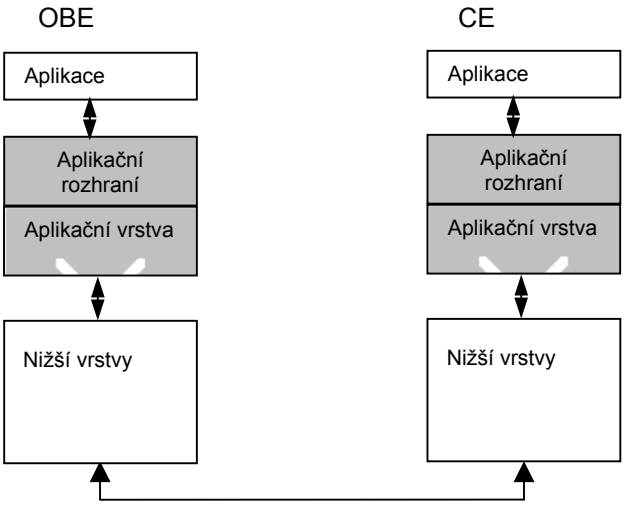
5.2 Spojení

5.2.1 Spoje celulární sítě

Tato norma se týká pouze komunikačního spoje celulární sítě (CN) mezi palubním zařízením vozidla (OBE) a centrálním zařízením (CE). Předmětem této normy nejsou ani spoje CN z OBE na OBE ani spoje mezi různými centrálními stanicemi. Spoje jsou navrženy tak, aby umožnilo (OBE) podporující určitý typ komunikačního rozhraní celulární sítě získat informace z CE, které ovlivní, změní nebo zvýší zpracovávání dat používaných v aplikaci EFC, a odeslat nasbíraná a zpracovaná data OBE k centrálnímu zařízení (CE).

Přenos dat na systém GNSS je vyloučen. Předpokládá se, že tento přenos dat vyústí v dostupnosti dat o poloze vozidla v OBE, což může ovlivnit spojení ve spoji CN.

OBE může mít rozhraní se vzdálenějšími komunikačními spoji. Tyto linky se mohou použít pro část spojení stanovené v této normě nebo se mohou využít pro dodatečná data.



Obrázek 2 – komunikační model celulární sítě

Obrázek 2 zobrazuje zásobník vrstev rozhraní celulární sítě. Tato norma se plně zabývá aplikačním rozhraním a aplikační vrstvou, včetně bezpečnostních mechanismů. Předpokládá se, že ostatní vrstvy, včetně fyzické, síťové a transportní, jsou nezávislé na aplikační vrstvě; tudíž lze normu použít s různými nosiči (nosnými médii). Definice aplikační vrstvy je pouze informativní.V případě, že nosné médium poskytuje vhodnou aplikační vrstvu, která se liší od aplikační vrstvy definované v této normě, poté lze použít i tuto aplikační vrstvu. Poté je nutné brát zřetel na získání vhodného spoje mezi aplikační vrstvou a aplikačním rozhraním.

Výměna dat mezi OBE a CE prostřednictvím spoje CN se seskupuje do transakcí následných zpráv s výměnou odesílatele a příjemce. Tato norma definuje úplný transakční model, který zahrnuje strukturu a obsah transakcí.

Většina transakcí vyžaduje spojení z bodu do bodu (point-to-point communication). Některé transakce jsou založeny na spojení z bodu do více bodů (point to multipoint communication) vysílacího spojení z CE, například všem OBE nacházejícím se v určité oblasti.

V případě spojení z bodu do bodu může být spojení budováno prostřednictvím OBE nebo CE. OBE může komunikovat s několika CE entitami s různými adresami. Adresy se ukládají v OBE nebo se posílají přes spoj CN. To samé platí pro adresy OBE v případě, že spojení buduje CE. OBE zahájí transakci v případě spouštěcí události, jak je definováno v této normě. Pro CE nejsou definovány takové události a záleží na dohodě mezi jednotlivými aktory, kdy se transakce na straně CE zahájí.

Při spojení OBE může použít data, která pocházejí z jiných zdrojů, včetně případu, kdy Řidič/Uživatel poskytuje vstupní data skrze rozhraní člověk – stroj (HMI). Proto se v některých případech při popisu základních konceptů objeví odkaz na Řidiče/Uživatele, jenž se účastní spojení. Tato účast je vždy na straně OBE skrze HMI.

5.2.2 Připojení na spoj DSRC

Jako nepovinnou charakteristiku může OBE používat komunikační spoj založený na DSRC. Spoj DSRC není součástí této normy. Pokud takový spoj existuje, předpokládá se, že součástí OBE je specifické zařízení pro spojení DSRC (viz obrázek 1) a že toto zařízení provádí výměny dat se zařízením silniční infrastruktury podle ENV ISO 14906.

Spoj DSRC a spoj CN se mohou používat jako zcela nezávislé komunikační spoje. Možností je zavedení spojení mezi spojem DSRC a spojem CN. V tomto kontextu je logické, že dochází k výměně dat stanovených touto normou podle mechanismů normy ENV ISO 14906. Tento postup je uveden v příloze B.

5.3 Aplikační obsahy EFC

5.3.1 Přehled

Systémy EFC v kontextu této normy slouží k vybírání poplatků použitím služby EFC vozidly vybavenými palubním zařízením (OBE), které poskytuje rozhraní CN stanovené touto normou. Poplatek se musí vybírat přesně definovanými procesy, včetně účtování poplatku. V kontextu této normy je aplikační obsah EFC množinou definic těchto procesů, pro které platí následující body:

- Existuje specifická část silniční infrastruktury, pro kterou jsou vybírány poplatky těmito procesy a tato část silniční infrastruktury je umístěna ve spojené oblasti, která se nazývá Geografická Doména Kontextu.
- Procesy jsou úplné ve smyslu, že definují postupy vybírání poplatků pro všechna vybavená vozidla, která projíždí Geografickou doménou a jsou předmětem poplatku.
- Existuje specifická organizační jednotka, která je odpovědná za spojení s uživateli, jenž jsou předmětem poplatku, nebo jejich zařízeními, které jsou nutné pro proces vybírání poplatků. Tato organizační jednotka se nazývá Poskytovatel Služby. Jeden Poskytovatel Služby může být odpovědný za více různých Kontextů.

Tato norma nedefinuje žádný specifický Kontext. Předpokládá, že existuje všeobecný rámec, ve kterém může být Kontext definován Poskytovateli Služeb nebo jinými organizačními jednotkami, se kterými mají vztah. Pokud definované Kontexty vyžadují transakce prostřednictvím spoje CN, musí být tyto transakce podle této normy. Tato norma definuje strukturu těchto transakcí takovým způsobem, že se Kontexty založené na všeobecném rámci mohou realizovat.

OBE nepotřebuje ukládat data o Kontextu dopředu. Všechna potřebná specifická data Kontextu se mohou poslat prostřednictvím spoje CN. To umožňuje nastavit nový Kontext a změnit existující Kontexty bez změn OBE, jakmile Kontext splňuje požadavky této normy. Podrobnosti o nahrávání dat Kontextu jsou uvedeny v článku 5.3.5.1.

Rámec je založen na pojmech Událostí a Akcí. OBE neustále sleduje parametry a stavy z různých zdrojů a porovnává je, aby nastavila hodnoty. Za specifických podmínek, které se váží na parametry, stavy a nastavené hodnoty se spustí Událost. Každá Událost vyvolá jednu nebo více Akcí v rámci OBE. Aplikační obsah definuje Seznam Událostí, které obsahují specifické Typy Událostí Kontextu s podmínkami ke spuštění Události, a s příslušnými Akcemi.

Mohou existovat specifické požadavky Kontextu na OBE a na data v něm obsažená. Při odeslání specifických dat Kontextu do OBE musí být tyto požadavky zahrnuty. Očekává se, že OBE upozorní Poskytovatele Služeb prostřednictvím spoje CN a Řidiče/Uživatele silniční infrastruktury prostřednictvím HMI na požadavky, které nejsou splněny. V tomto případě se musí použít některé výjimečné postupy řešení, které jsou mimo rámec této normy.

Pro všechna vozidla, která použijí část silniční infrastruktury, jež je předmětem poplatku, se nastaví aplikační procesy podle rámce uvedeného v této normě, který obsahuje tyto subprocesy:

- Účtování, ve kterém se všechna příslušná data udávající použití silniční infrastruktury zaznamenají, aby se stanovily příslušné poplatky.
- Platba, kterou se finanční prostředky Řidiče/Uživatele převedou k zaplacení poplatku.
- Manager uživatelských/přístupových práv, které obsahují ustanovení a aktualizaci všech smluv, jež jsou potřeba pro vykonání procesu účtování a platby.
- Systém řízení EFC, který obsahuje všechna nařízení, jež zaručují fungování procesu účtování a platby včetně monitoringu (dozoru) těchto procesů a distribuci dat potřebných jako nezbytné podmínky k jejich fungování.

Některé aplikační procesy nemusí úplně splňovat rámec uvedený v této normě. Pro tyto procesy tato norma uvádí možnost nahrání specifického softwaru z CE na OBE, který se zde nainstaluje, aktivuje a spustí aplikaci podle daného Aplikačního obsahu.

5.3.2 Proces účtování

Proces účtování je založen na specifických účtovacích událostech. Jsou pro ně zejména určeny dva typy Akcí: První spočívá ve vytvoření datového záznamu na OBE. Záznam obsahuje data a čas

spuštění Události, typ Události, Detaily Události a parametry hodnot spojené s Událostí, např. výši poplatku nebo parametry, které lze použít pro výpočet poplatku. Záznam je uložen v Seznamu Záznamů uvnitř OBE. Druhá Akce je transakcí do Centrálního zařízení prostřednictvím komunikačního spoje CN, která se nazývá Účtovací Spojení. Přenesená data mohou obsahovat vstupní data ze Seznamu Záznamů.

Podmínky ke spuštění Účtovacích Událostí obvykle zahrnuje podmínky pro Polohu. Způsob, jakým jsou začleněny v rámci této normy, v termínech Geografických Objektů, je popsán v článku 5.4, společně se seznamem účtování spojeného s typy Geografických Objektů, které jsou řazeny v článku 5.4.1.

Poplatek se vypočítá podle použití silniční infrastruktury vycházejícího ze zaznamenaných Událostí. Skládá se z výše poplatku a měny. Pokud je podle aplikačního obsahu proveden výpočet v OBE, poté musí data Kontextu (viz. článek 5.3.1) obsahovat Tarif. Poplatek je účtován v daný den a čas a účtování lze zaznamenat jako Účtovací Událost. Tarif udává poplatek a měnu jedním z následujících způsobů:

- jako paušální poplatek závisející pouze na tarifních třídách
- jako poplatek dle vzdálenosti, který může záviset na tarifních třídách, výše poplatku za jednotku vzdálenosti. Jednotka vzdálenosti je definována tarifem.
- jako poplatek dle času, který může záviset na tarifních třídách, výše poplatku za časovou jednotku. Časová jednotka je definována tarifem.
- jako poplatek dle vzdálenosti a času, který může záviset na tarifních třídách, výše poplatku za jednotku vzdálenosti a časovou jednotku. Opět jsou jednotka vzdálenosti a časová jednotka definovány tarifem.

Závislost na tarifních třídách je dána tarifním faktorem nebo jako parametr v tabulce platebních sazeb. To znamená, že se poplatek vypočítá podle této rovnice:

$$F = TF_1(TC_1) \times TF_2(TC_2) \times ... \times TF_k(TC_k) \times FRT(TC_{k+1},...,TC_n)$$

kde F je poplatek

TF_i tarifní faktor

TC_i tarifní třída

FRT tabulka platebních sazeb

Tarifní třídy jsou definovány v Tarifu a mohou obsahovat: Třídy vozidel, třídy přívěsů, časové třídy, třídy doby průjezdu, třídy polohy, rychlostní třídy a třídy účtovacích objektů.

5.3.3 Proces platby

V procesu platby jsou finanční prostředky odeslány od Řidiče/Uživatele k zaplacení poplatku Poskytovateli Služby za použití silniční infrastruktury, jak je stanoveno v procesu účtování. Proces platby může nebo nesmí být součástí Aplikačního Obsahu. Tato norma uvádí několik Platebních Scénářů, které mohou být použity Kontextem. Poskytovatel Služeb, při definování Kontextu, pevně stanoví schválené Platební Scénáře pro tento Kontext jako součást požadavků v datech Aplikačního Obsahu.(viz. článek 5.3.1).

Pro všechny Platební Scénáře potřebuje Řidič/Uživatel Platební Prostředky, které jsou poskytnuty institucí, jež se nazývá Vydatel. Platební Prostředky umožňují přesun finančních prostředků pocházejících od Řidiče/Uživatele, mezi Vydatelem a Poskytovatelem Služeb za specifických podmínek, které jsou pevně stanoveny mezi Vydatelem a Řidičem/Uživatelem, obvykle v Kontraktu o platbě (viz. článek 5.3.4). Platební Prostředky, které se mohou použít podle této normy jsou:

– Kreditní karty
– Úvěrové karty
– Elektronické peněženky

Záleží na Poskytovateli Služeb, jestli schválí nebo neschválí určitý typ Platebních Prostředků. Seznam schválených Platebních Prostředků uvede Poskytovatel Služeb jako součást požadavků v datech Aplikačního Obsahu.

Platební Scénář 1: Okamžitá platba

Ihned poté, co byl poplatek stanoven a schválen Řidičem/Uživatelem a Poskytovatelem Služeb, pošle Řidič/Uživatel Poskytovateli Služeb Povolení (Autorizaci) pro finanční transakci od Vydatele Poskytovateli Služeb a Poskytovatel Služeb pošle potvrzení o dokončení transakce formou účtenky.

Na rozdíl od tohoto jednoduchého Platebního Scénáře jsou ostatní scénáře založeny na Účtech EFC. Každému EFC Účtu je přidělena měna a Zůstatek na Účtu EFC je kdykoliv dostupný; vykazuje aktiva Řidiče/Uživatele uvedená v odpovídající měně. Pokud jsou platební scénáře založené na Účtu EFC používány v Kontextu, musí mít Řidič/Uživatel alespoň jeden Účet EFC, který je schválen Poskytovatelem Služby.

Účty EFC mohou být schváleny pouze pro jeden Kontext nebo mohou být sdíleny různými Kontexty. To je naznačeno v Doméně Účtu EFC.

Platební Scénář 2: Zpětná platba Centrálního Účtu

V tomto scénáři je Účet EFC obsluhován Poskytovatelem Služeb. Na základě Událostí zaznamenaných v procesu účtování stanoví Poskytovatel Služeb poplatky a odečte odpovídající hodnoty ze Zůstatku na Účtu EFC. Tímto způsobem může Zůstatek klesnout do záporných hodnot. Na základě některých specifických kritérií uvedených v Aplikaci pošle Poskytovatel Služeb OBE požadavek na vyrovnání stavu Účtu EFC nebo zahájí platební postup, který není založen na spojení prostřednictvím CN spoje a tudíž není předmětem této normy. Vyrovnání účtu na spoji CN se provede stejným způsobem jako platba podle Scénáře 1.

Platební Scénář 3: Předplacení Centrálního Účtu

V tomto Scénáři jako součást Inicializace předtím, než vozidlo vstoupí do Geografické Domény určitého Aplikačního Obsahu pošle Řidič/Uživatel Poskytovateli Služeb Povolení zavést Účet EFC převodem finančních prostředků odpovídající určité částce peněz, jak je definováno v Kontextu. Opět je Účet EFC obsluhován Poskytovatelem Služeb. Po dokončení převodu obdrží Řidič/Uživatel účtenku.

Poplatky stanovené podle Procesu Platby se poté odečtou ze Zůstatku na účtu a než se zůstatek dostane pod jistou mezní hodnotu, musí být účet EFC znovu zaveden stejným způsobem jako počáteční vklad. Podmínkou tohoto scénáře je vrácení Zůstatku, který na Účtu EFC zůstal po platbě, Řidiči/Uživateli poté, co opustil Geografickou Doménu tím, že je znovu převede Vydateli. Tato transakce je oznámena Řidiči/Uživateli prostřednictvím spoje CN.

Platební Scénář 4: Palubní Účet

V tomto Scénáři je Účet EFC nainstalován v OBE. Zůstatek se může změnit převodem Jízdenek. Jízdenky se skládají z hodnoty a měny. Jsou generovány Vydatelem, mohou být převedeny na Účet EFC a odtud k Poskytovateli Služeb. Jízdenky převedené na Účet EFC musí mít stejnou měnu jako Účet EFC. Pokud je Jízdenka převedena na Účet EFC, její hodnota se přičte k Zůstatku. Pokud je převedena z Účtu EFC, její hodnota se od Zůstatku odečte.

Pro každou Platební Událost (viz. článek 5.3.2) je Jízdenka převedena z Účtu EFC na Poskytovatele Služeb. Je ve stejné měně jako poplatek (což znamená, že poplatek se musí vypočítat ve stejné měně jaká se používá pro platbu z Účtu EFC) a její hodnota odpovídá výši poplatku.

Jízdenky převedené na Účet EFC se musí všechny generovat stejným Vydatelem. Řidič/Uživatel si je musí koupit od Vydatele (lze je koupit i prostřednictvím Zprostředkovatele (Loading Agent)) použitím Platebních Prostředků. Hodnota Jízdenky v odpovídající měně odpovídá ceně nákupu.

Předpokládá se, že existuje smlouva mezi Vydatelem a Poskytovatelem Služeb, která udává způsob, jakým Vydatel zaplatí Poskytovateli Služeb za Jízdenky generované Vydatelem a získané Poskytovatelem Služeb.

Řidič/Uživatel musí zaručovat, že je na jeho Účtu EFC vždy dostatečný Zůstatek, aby všechny Jízdenky požadované Procesem Účtování se mohly převést na Poskytovatele Služeb. Proto se Vydatel a Řidič/Uživatel musí dohodnout na spodní mezní hodnotě Zůstatku. V případě, že je dosaženo této mezní hodnoty, musí si Řidič/Uživatel zakoupit od Vydatele nové Jízdenky. Tuto transakci lze uskutečnit prostřednictvím spoje CN. Pokud neexistuje žádné další využití pro zbývající Jízdenky na Palubním Účtu (například z důvodu, že vozidlo opustilo Geografickou Doménu Kontextu), lze tyto Jízdenky poslat zpět Vydateli, který převede odpovídající finanční prostředky na Platební Prostředky.

Platební Scénář 5: Kombinovaný Účet

Tento Scénář kombinuje Centrální Účet (Scénáře 2 a 3) s Palubním Účtem (scénář 4). Poskytovatel Služeb použije finanční prostředky z Centrálního Účtu pro generování jízdenek a pošle je na Palubní Účet. Jako ve Scénáři 4 jsou Jízdenky podle výše poplatku zaslány zpět Poskytovateli Služeb, který vyrovná účty s Vydatelem. Nepoužité Jízdenky lze zaslat zpět Poskytovateli Služeb, což vede k odpovídajícímu navýšení Zůstatku na Centrálním Účtu.

5.3.4 Uzavření kontraktu

5.3.4.1 Přehled

V případě, že je potřeba pro Služby EFC uzavřít dohody mezi Řidičem/Uživatelem a Poskytovatelem Služeb nebo mezi Řidičem/Uživatelem a Vydatelem, uvádí tato norma možnost projednání a uzavření těchto dohod s transakcí prostřednictvím spoje CN a k ustanovení elektronické smlouvy, která tyto dohody obsahuje. Předpokládá se, že Smlouvy pro služby EFC jsou uzavřeny před tím, než se zahájí procesy účtování a platby v příslušném Aplikačním Obsahu.

Smlouvy jsou vždy uzavírány mezi dvěma stranami, jednou z nich je Řidič/Uživatel. Pro všechny typy Smluv existuje pevná struktura s určitým počtem parametrů a možností, na kterých je potřeba se dohodnout. Jedna strana zasílá seznam možností výběru a druhá strana si z tohoto seznamu zvolí parametry a možnosti. Pokud jsou určité kombinace možností a parametrů vyloučeny, jsou takové kombinace vyznačeny stranou, která seznam zasílá. Celá Smlouva je poté podepsána oběma stranami elektronickým podpisem a poslána druhé straně. Za Řidiče/Uživatele dodá podpis OBE. Tato norma nedefinuje způsob, jak je zaručeno, že Smlouvy podepsané OBE, jsou schválené Řidičem/Uživatelem, ale předpokládá se, že toto schválení je poskytnuto, jakmile je Smlouva prostřednictvím OBE podepsána.

5.3.4.2 Kontrakt o poskytování služby

Kontrakt o poskytování služby je uzavřen mezi Řidičem/Uživatelem a Poskytovatelem Služeb a dává Řidiči/Uživateli právo používat EFC pro jeden nebo několik specifických Aplikačních Obsahů při odpovědnosti Poskytovatele Služeb. Kontrakt o poskytování služby zahrnuje specifické vozidlo nebo specifické OBE. V druhém případě může být OBE přesunuto z jednoho vozidla do druhého a data spojená s vozidlem se přenesou s Inicializací Smlouvy předtím, než vozidlo vstoupí do Geografické Domény Aplikace.

5.3.4.3 Kontrakt o platbě

Kontrakt o platbě se uzavírá mezi Řidičem/Uživatelem a Vydatelem. Stanovuje podmínky použití Platebních Prostředků, které jsou vydány Vydatelem. Nutnost uzavření Kontraktu o platbě závisí na Aplikačních požadavcích spojených se zárukou platby; Platební Scénáře umožňují maximum možných výší poplatků, charakteristiky OBE a možné další faktory v rámci Aplikačního Obsahu. Kontrakt o platbě může být rozšířením stávající smlouvy týkající se Platebních Prostředků, aby se tyto Platební Prostředky staly použitelnými v rámci EFC nebo se může vytvořit nová smlouva o Platebních Prostředcích. Pokud je Kontrakt o platbě rozšířením stávající smlouvy, musí zahrnovat odkaz na tuto stávající smlouvu a předpokládá se, že zdroj finančních prostředků je stejný jako u stávající smlouvy. Pokud se jedná o smlouvu pro nové Platební Prostředky, musí být zdroj finančních prostředků specifikován Řidičem/Uživatelem.

Obvykle existuje pro Platební Prostředky Platební Médium, což je elektronické zařízení u Řidiče/Uživatele, které musí být přítomné provádění finančních transakcí založených na Platebních Prostředcích, aby Řidič/Uživatel potvrdil schválení platby. Platební Médium obsahuje data, která identifikují pravost finančních transakcí. V kontextu EFC může Platební Médium být OBU nebo karty integrovaných okruhů ICC. V případě, že Kontrakt o platbě není rozšířením stávající smlouvy, může být zdroj finančních prostředků spojen s Platebním Médiem.

Obvykle Vydatel zaručuje platby poplatků Řidičem/Uživatelem Poskytovateli Služeb Platebními Prostředky. Toto ručení může obsahovat omezení, která jsou uvedena v seznamu v Kontraktu o platbě. Tato omezení mohou zahrnovat například mezní hodnoty finančních prostředků, které jsou předmětem převodu při finančních transakcích nebo při postupech, které vyžadují potvrzení transakce a ověření pravosti.

Vydatel může od Kontraktu o platbě odstoupit v případě, že nejsou dále plněny podmínky pro použití Platebních Prostředků. Je na odpovědnosti Vydatele a Poskytovatele Služeb, aby se vyhnuli použití Platebních Prostředků u Kontraktu o platbě, od které odstoupili. Příslušné postupy nejsou součástí této normy. Ale tato norma definuje transakci, která informuje Řidiče/Uživatele o odstoupení od smlouvy.

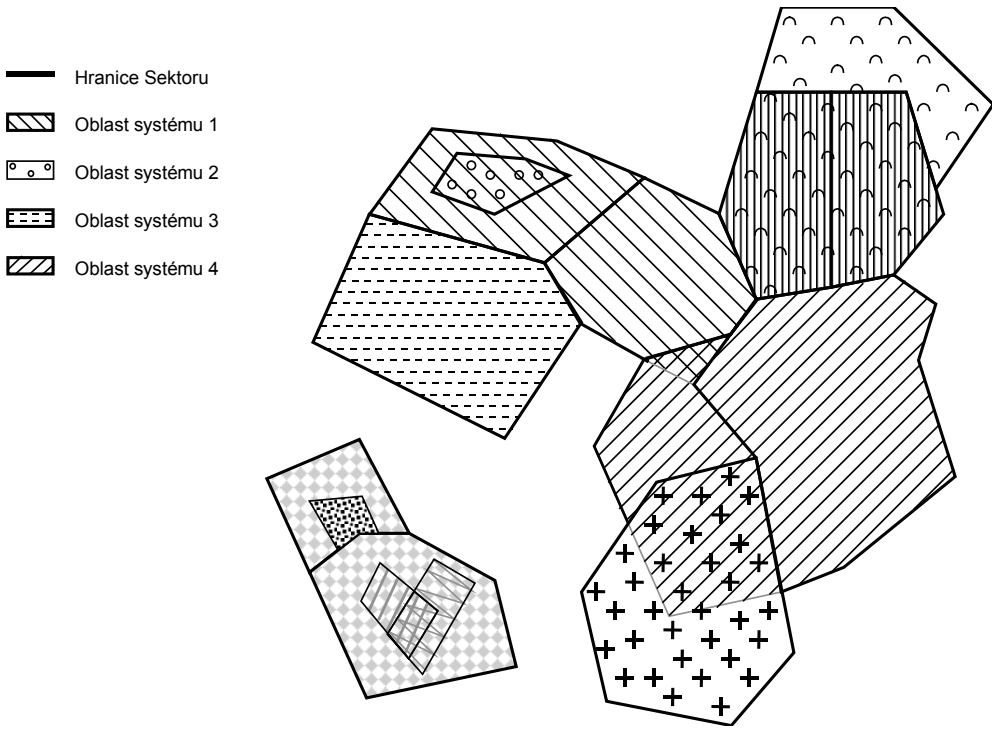
5.3.5 Systém řízení EFC

5.3.5.1 Aktualizace OBE

Všechny Aplikační obsahy potřebují specifická data určitého Kontextu, které jsou přítomné v OBE. Pro aktualizaci těchto dat lze použít Transakce Získání Dat Mýtného na spoji CN (viz. článek 6.2). Předpokládá se, že data, spojená s daným Kontextem, se musí aktualizovat předtím, než vozidlo vstoupí do Geografické Domény Kontextu. Služba pro aktualizaci dat mýtného zajištěná Transakcí Získání Dat Mýtného je založena na principu roaming, který zaručuje, že data Kontextu potřebná pro OBE lze získat včas. Proto je celá oblast, kam se vozidlo může dostat (včetně Geografických Domén a částí, které nepodléhají poplatku) rozdělena do Sektorů, jak je popsáno v článku 5.4.2. Management sektoru poskytuje službu aktualizace dat mýtného, kterou dodává data Kontextu pro takové Kontexty, jenž úplně a nebo jen z části zasahují Geografickou Doménou do daného Sektoru. Služba aktualizace dat mýtného také zahrnuje aktualizaci dat Sousedních Sektorů, aby se zajistilo, že OBE obdrží aktualizovaná data mýtného před vstupem vozidla do těchto sektorů.

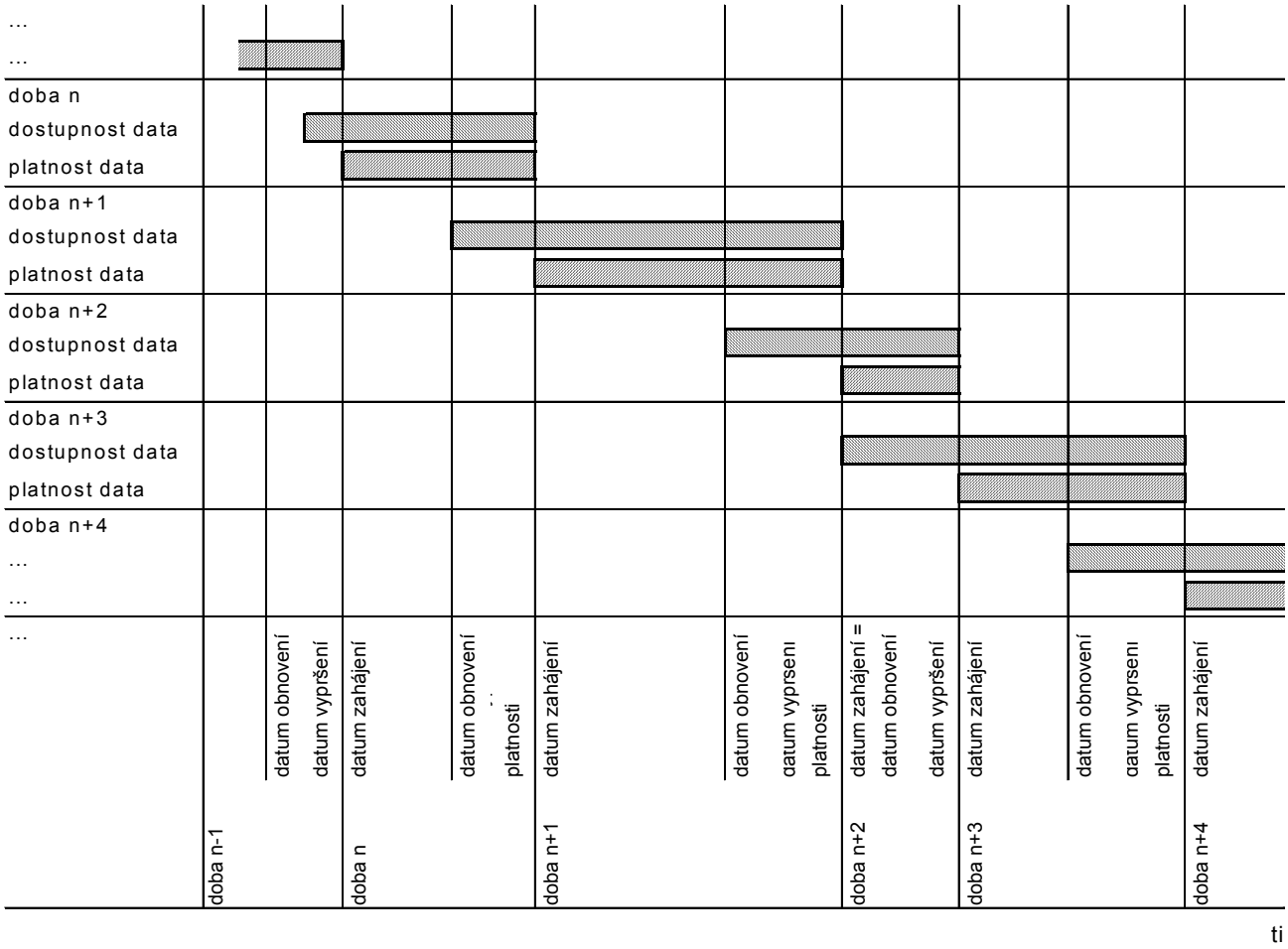
Velikosti a tvary jednotlivých sektorů se musí zvolit tak, aby se mohlo množství dat pro jednu úplnou aktualizaci přenést za rozumnou dobu a tak, aby množství dat, které se musí uložit v OBE, nepřekročilo kapacitu paměti; je nutné také brát v úvahu, že musí být možné uložit data mýtného dalších třech sousedních Sektorů najednou (viz obrázek 3). Každý Sektor nesmí obsahovat více než 4 Aplikační obsahy. Management Sektorů mohou změnit velikost a tvar Sektorů tím, že sloučí několik Sektorů dohromady a vytvoří tak jeden Sektor, nebo rozdělí jeden Sektor na několik Sektorů nebo posunou hranice mezi dvěma sousedními Sektory.

Aplikační obsah se může rozšířit na několik Sektorů. Poté data mýtného jednoho z těchto Sektorů obsahují data Obecného Kontextu takového Kontextu nebo také Účtovacích Objektů Kontextu (viz. článek 5.4.1), které jsou celé nebo jen z části uvnitř daného Sektoru. Při průjezdu do dalšího Sektoru se stejným Aplikačním Obsahem potřebuje OBE získat pouze Objekty účtování tohoto Kontextu v novém Sektoru.



Obrázek 3 – Možné rozmístění Sektorů a Geografických Domén

Změny Kontextu a dat Sektorů jsou možné pouze u předdefinovaných dat. Tato data musí být dohodnuta mezi Poskytovateli Služeb s jejich Kontexty v daných Sektorech a Managementem Sektorů. Každá verze Dat Kontextu musí být použitelná v době platnosti, která začíná Datem Zahájení, což je datum pro změny Kontextu a dat Sektoru, a končí datem vypršení platnosti, které je dalším datem pro změny a tak dále. Nová verze Kontextu a Dat Sektoru musí být dostupná předem, od data obnovení, které je před datem zahájení platnosti, až k datu vypršení platnosti tak, aby přesáhly do následující doby dostupnosti, jak je uvedeno na obrázku 4. Doby platnosti vždy začínají v 00,00 UTC data zahájení a končí v 24,00 UTC dne vypršení platnosti.



Obrázek 4 – Doby platnosti a dostupnosti dat mýtného

Management Sektorů mohou poskytovat dvě různé Služby aktualizace dat mýtného:

1. Přenos celého Sektoru a dat Kontextu na vysílací kanál;
2. Přenos všech změn do Sektoru a dat Kontextu, které jsou relevantní pro specifické OBE, v transakci z bodu do bodu do tohoto OBE.

Data Sektoru v rámci Aktualizace zahrnuje nové datum obnovení a datum vypršení platnosti. Díky tomu OBE při vstupu do Sektoru ví, jestli potřebuje provést aktualizaci Sektoru a dat Kontextu tohoto Sektoru.

Pro každou hranici mezi sousedními Sektory je definován Segment, který se skládá ze zóny o přibližně konstantní šířce na obou stranách hranice (viz. článek 5.4.2). Data Kontextu, která je třeba uložit do OBE jsou data Sektoru, ve kterém se OBE nachází, a Data Kontextu sousedního Sektoru, jakmile vozidlo dosáhne Segment ve směru do daného Sektoru. Tímto se udává maximum Dat Kontextu tří Sektorů, které se musí uložit v OBE v případě, že vozidlo je v zóně přesahu sousedních Segmentů. Ostatní Data Kontextu lze vymazat nebo uchovat pro pozdější použití.

Předpokládá se, že OBE může vykonat všechny Akce požadované Daty Kontextu. Pokud to není případ pro daný Aplikační obsah, existuje možnost, kterou Poskytovatel Služby poskytuje Aktualizační

Software prostřednictvím transakce provedené na spoji CN. Například pokud jsou Akce nebo jejich obsah rozšířeny v pozdějších verzích této normy, může být potřebný příslušný aktualizační software realizován tímto způsobem. Poskytovatel Služeb může také vyžadovat některé charakteristiky OBE, které jsou mimo rámec uvedený v této normě a může poté nabízet nahrání odpovídajícího softwaru touto transakcí.

Poznámka: Je užitečné poskytovat Aktualizační Software takovým způsobem, aby byl co nejvíce nezávislý na hardwaru a operačním systému. Na podrobnostech se musí dohodnout Poskytovatelé Služeb a výrobci OBE.

5.3.5.2 Monitoring OBE

Vzhledem k tomu, že OBE v systémech založených na GNSS/CN dokáže vykonávat Akce, které jsou čistě interního charakteru, což znamená, že ve chvíli, kdy jsou vykonávané, není zde žádné spojení s jinými částmi systému, musí být možné monitorovat správné fungování OBE. To se provádí prostřednictvím spoje CN. Tato norma stanovuje různé možnosti pro monitoring OBE:

– v případě oznamovací transakce provedené na základě žádosti může být OBE požádáno poslat Poskytovateli Služeb zprávu o současném stavu OBE nebo o záznamech nedávných potíží.

– Aplikační obsah může požádat o oznamovací transakce diagnostický systém (Watchdog), aby OBE poslalo Poskytovateli Služeb zprávu o současném stavu OBE nebo o záznamech nedávných potíží periodicky nebo v případě předdefinovaných Událostí.

– v případě prováděcí transakce provedené na základě žádosti může být OBE požádáno poslat operátorovi dohledového systému zprávu o současném stavu Aplikačního Obsahu v OBE nebo o záznamech Událostí vztahujících se na Účtování nebo Platbu.

– Aplikační obsah může obsahovat spouštěcí mechanismy pro předem nastavené prováděcí transakce, při kterých musí OBE poslat operátorovi dohledového systému zprávu o stavu nebo o záznamech Událostí vztahujících se na Účtování nebo Platbu. Spouštěcí mechanismy mohou být například udány určitou polohou vozidla.

5.4 Řízení polohy

Mnoho procesů výběrů mýtného závisí na pozici a směru jízdy vozidla, které je předmětem platby, což je v této normě nazýváno Polohou. Předpokládá se, že pro stanovení Polohy využívá přijímač GNSS část OBE. Pozice vozidla jsou neustále měřeny a srovnávány se souřadnicemi uloženými v OBE. V této sekci jsou popsány základní koncepty, které udávají, jaké souřadnice při porovnání s pozicemi vozidla jsou přenášeny prostřednictvím spoje CN a způsob, jakým jsou přenášeny.

Geografické Objekty zahrnují řadu souřadnic spojující body a možná dodatečná data související se souřadnicemi nebo s Objektem jako celkem. Tato norma definuje různé typy takových Objektů. Podle typu OBE stanoví, jestli vozidlo projelo, vstoupilo nebo opustilo daný Geografický Objekt.

Pro každý Geografický Objekt jsou souřadnice prvního bodu, tzv. Referenčního bodu, uvedeny v plné šířce a délce v systému souřadnic WGS84 (viz ISO 14821-3). Následné body jsou dány odchylkami v šířce a délce od Referenčního bodu.

Jednotlivé body Geografických Objektů se musí zvolit tak (podle daných okolností), aby se použilo nejmenší množství bodů.

Záleží na výrobci OBE, jestli začlení adekvátní algoritmy, které identifikují průjezdy, vstupy a odjezdy vozidla daným Geografickým Objektem. Tato norma definuje pouze úrovně jakosti těchto algoritmů (viz příloha xxx). Poskytovatelé Služeb se mohu poté odkazovat na tyto úrovně, pokud požadují určitou jakost Polohu v jejich Aplikačním Obsahu.

Struktura a použití Geografických Objektů je vysvětlena v následujících článcích. Souhrnná specifikace odpovídajících datových prvků je uvedena v kapitole 7.

5.4.1 Geografické Objekty spojené s Účtováním

Všechny Geografické Objekty spojené s Účtováním nebo Účtovací Objekty mají ID identitu Objektu, která je jedinečná v daném Aplikačním Obsahu.

Účtovací Objekty lze seskupovat v Řady takových Objektů. Všechny Objekty v Řadě musí být stejného typu. V případě, že je použito takových Řad Objektů, obsahuje ID identita Objektu jedinečnou ID identitu Řady a ID identitu Objektu, která je jedinečná v dané Řadě.

Kontexty mohou používat Účtovací Objekty jiných Kontextů odkazem na jejich ID identitu a identitu Aplikačního Kontextu v Kontextu, ve kterém je Účtovací Objekt jedinečně definován.

Účtovací Objekty lze vytvořit a zrušit při aktualizaci Aplikačního Obsahu. Nové Účtovací Objekty musí mít ID identitu, která se liší od ID identity všech Účtovacích Objektů, které byly zrušeny při posledních třech aktualizacích Kontextu. Změny Účtovacích Objektů nejsou možné (vyjma při simultánním zrušení a vytvoření nového Účtovacího Objektu).

Pokud je datum, které se nachází v době platnosti Dat Mýtného, v případě, kdy se musí přidat nebo odebrat některé Účtovací Objekty, známo předem, poté jsou tyto Účtovací Objekty zahrnuty v Datech Kontextu s odpovídajícím datem zahájení a ukončení platnosti.

Zóna:

Zóna se definuje souřadnicemi o posloupnosti nejméně tří bodů, začínajících číslem 0 a splňujících následující požadavky:

– Všechny body jsou jiné.

– Žádné body neleží na přímé spojnici mezi dvěma po sobě následujícími body posloupnosti, včetně spojnice mezi prvním a posledním bodem.

– Žádná spojnice mezi po sobě následujícími body posloupnosti, včetně spojnice mezi prvním a posledním bodem, se neprotíná s jinou takovou spojnicí.

– Oblast, která je vytvořena řadou spojnic mezi po sobě následujícími body posloupnosti (včetně spojnice mezi prvním a posledním bodem) a která je umístěna na pravé straně od těchto spojnic, pokud se pohlíží z jednoho bodu posloupnosti do následujícího, je menší, než oblast po levé straně.

Uzavřený polygon, který se skládá ze spojnic mezi dvěma po sobě následujícími body posloupnosti, včetně spojnice mezi prvním a posledním bodem, se nazývá hranice Zóny. Oblast na pravé straně hranice (pokud se pohlíží z jednoho bodu posloupnosti do následujícího) se nazývá vnitřní část Zóny, oblast na levé straně se nazývá vnější částí Zóny. Všechny body na hranici patří vnější části Zóny.

Zóny mohou mít vnitřní hranice. Hranice Zóny výše definované se tudíž nazývají vnější hranice. Vnitřní hranice se definují podle stejných pravidel jako vnější hranice, ale způsobem, že vnitřní část vnitřní hranice se překrývá s vnitřní částí vnější hranice, zatímco vnější část vnitřní hranice se nepřekrývá. Dále se nesmí vnější části různých vnitřních hranic překrývat. Vnitřní část Zóny je poté průsečíkem všech vnitřních částí hranic (vnějších i vnitřních), zatímco zbytek je vnější část.

V některých případech může být užitečné poskytnout vnějším částem všech Zón jejich vlastní ID identitu Zóny. Hodnota této ID identity je tudíž 0.

Následující Spouštěcí Události, které závisejí na Zóně, se definují:

– Vstup do Zóny je změnou pozice OBE z vnější části do vnitřní části.

– Výstup ze Zóny je změnou pozice OBE z vnitřní části do vnější části.

Spouštěcí Události se mohou realizovat takovým způsobem, že se použijí pouze na specifickou Zónu nebo na všechny Zóny specifické Řady Zón.

Možným Detailem o vstupech a výstupech specifické Události je Sekce, která je dána číslem prvního konečného bodu spojnice, jež se v rámci posloupnosti kříží s OBE. (Pro spojnici mezi prvním a posledním bodem posloupnosti je Sekce dána číslem posledního bodu posloupnosti. Pokud se OBE kříží spíše v bodě Zóny než ve spojnici, je Sekce dána číslem tohoto bodu.) Druhý možný Detail specifické Události je Zóna, ze které vozidlo vstupuje do specifické Zóny nebo Zóna, do které vozidlo vystupuje ze specifické Zóny (dána ID identitou Zóny, včetně 0 pro vstupy z žádných jiných Zón nebo výstupy do žádných jiných Zón).

Každý Vstup do Zóny musí být následován Výstupem z této Zóny před dalším Vstupem do Zóny a naopak. Pokud to tak není, OBE pošle chybovou zprávu prostřednictvím Oznamovací Transakce Diagnostického systému, pokud se používá.

Následující podmínky pro Polohu vozidla se s ohledem na Zónu definují:

– Vozidlo je ve vnitřní části Zóny.

– Vozidlo je mimo Zóny, což znamená, že se nachází ve vnější části všech Zón.

Tyto podmínky pro Polohu mohou být omezeny na specifické Zóny a na Zóny se specifickou Řadou.

Koridor

Koridor se definuje souřadnicemi o posloupnosti dvou po sobě následujících bodů, začínající číslem 0, které splňují následující požadavky:

– Všechny body jsou jiné.

– Žádné body neleží na (přímé) spojnici mezi dvěma po sobě následujícími body posloupnosti.

– Žádná spojnice mezi po sobě následujícími body posloupnosti se neprotíná s jinou takovou spojnicí.

Každý Koridor má dva směry. Kladný směr je udáván jako směr z prvního bodu do posledního bodu. Záporný směr je v opačném směru. Koridory se mohou definovat jako jednosměrný Koridor nebo obousměrný Koridor. Pro jednosměrné Koridory je možný jen kladný směr, zatímco pro obousměrné Koridory jsou možné oba typy – kladný i záporný směr.

První bod jednosměrného Koridoru se nazývá Vstupní Bod. Pro obousměrné Koridory jsou Vstupními body první bod i poslední bod. Jiné body Koridoru lze označit jako Vedlejší Vstupní Body. Kolem každého Vstupního bodu nebo Vedlejšího Vstupního Bodu lze definovat kruh, který je dán svým poloměrem. Poloměr může být stejný pro všechny Koridory nebo specifický pro každý Koridor.

Blízkost Vstupního Bodu nebo Vedlejšího Vstupního Bodu se definuje jako kruh na zemi s daným poloměrem kolem Vstupního Bodu (nebo Vedlejšího Vstupního Bodu).

U každého Koridoru existuje Indikátor Kritické Oblasti. Ten stanovuje spojení mezi po sobě následujícími body, které se nepoužívají pro stanovení průjezdu vozidla Koridorem (z důvodu špatného signálu GNSS, například v tunelu), a je udán ID identitami bodů před vynechanými spojnicemi.

Šířku parametrů lze zavést dvěma způsoby: pro Koridor jako celek nebo pro každou spojnici mezi dvěma po sobě následujícími body (pokud tato spojnice nepatří do kritické Oblasti).

Následující Spouštěcí Události, které závisejí na Koridoru, se definují:

– vozidlo vstoupí do Blízkosti Vstupního Bodu Koridoru.

– Vozidlo vystoupí z Blízkosti Vstupního Bodu Koridoru.

– Průjezd podél Koridoru je neidentifikován.

– Vozidlo opustí Koridor.

Spouštěcí Události se mohou realizovat takovým způsobem, že se použijí pouze na specifický Koridor nebo na všechny Koridory specifické Řady Koridorů.

Možné Detaily Události spojené s těmito Spouštěcími mechanismy jsou číslo Vstupního Bodu v případě několika Vstupních Bodů pro stejný Koridor, a směr v případě průjezdu kolem obousměrného Koridoru.

Následující podmínky pro Polohu vozidla s ohledem na Koridor se definují:

– Průjezd vozidla podél Koridoru.

– Blízkost vozidla Vstupnímu Bodu (nebo Vedlejšímu Vstupnímu Bodu).

– Vozidlo je mimo Koridor

Tyto podmínky pro Polohu mohou být omezeny na specifické Koridory a na Koridory se specifickou Řadou. Atributy spojené s těmito podmínkami pro Polohu jsou číslo Vstupního Bodu, v případě několika Vstupních Bodů pro stejný Koridor, a směr, v případě průjezdu kolem obousměrného Koridoru.

Předpokládá se, že jednotlivé body Koridoru leží na silničním spoji. Průjezd podél Koridoru musí být zaznamenán takovým způsobem, aby se zabránilo použití jiného silničního spoje než je ten, označený

Koridorem, zejména silniční spoje rovnoběžné nebo křižující spoj Koridoru. Šířka parametrů odráží blízkost dalších silničních spojů, které by mohly zasahovat do silničního spoje označeného Koridorem.

Poznámka Obvykle se Koridory rozprostírají od vstupního bodu vozovky, která je předmětem mýtného, do dalšího možného bodu výstupu. Pokud existuje několik vstupních bodů, které jsou blízko sebe a není záměrem účtovat různé poplatky, záleží na tom, který ze vstupních bodů je opravdu vstupním bodem vozidla, poté lze následující vstupní body označit jako Vedlejší Vstupní Body. V některých případech může být užitečné definovat několik Koridorů, které se rozkládají na stejné Sekci vozovky, ale mají jiné Vstupní nebo Výstupní body.

Virtuální portál

Virtuální portál se skládá z šesti odlišných bodů:

– Body 0 a 1 označují virtuální bránu.

– Body 2 a 3 společně s body 0 a 1 tvoří první čtverec.

– Body 4 a 5 společně s body 0 a 1 tvoří druhý čtverec, který leží na druhé straně virtuální brány než první čtverec.

Následující Spouštěcí Události, která závisejí na Virtuálním Portálu, se definují:

– Průjezd Virtuálním Portálem v kladném směru;

– Průjezd Virtuálním Portálem v záporném směru.

Spouštěcí Události se mohou realizovat takovým způsobem, že se použijí pouze na specifický Virtuální Portál nebo na všechny Virtuální Portály specifické Řady Virtuálních Portálů.

Kladný směr je udán směrem od prvního do druhého čtverce, záporný směr je v opačném směru. Stopa vozidla podle záznamu ze souřadnic GNSS se vypočítá jako průjezd Virtuálním Portálem pouze pokud dvě po sobě jdoucí měřené souřadnice leží ve čtvercích Virtuálního Portálu, každá v jiném. To umožňuje definovat průjezdy po silničních spojích i v případě, že se vozovky nachází částečně v tunelech. Virtuální Portál může podle nastavení bodů 0 a 1 přesahovat jeden nebo několik silničních spojů.

Následující podmínky pro Polohu vozidla se s ohledem na Virtuální Portály definují:

– Vozidlo se nachází před Virtuálním Portálem, který je umístěn v Zóně prvního čtverce.

– Vozidlo se nachází za Virtuálním Portálem, který je umístěn v Zóně druhého čtverce.

– Vozidlo se nachází mimo všechny Virtuální Portály, tudíž je mimo všechny čtverce Virtuálních Portálů.

Tyto podmínky pro Polohu mohou být omezeny na specifické Virtuální Portály a na Virtuální Portály se specifickou Řadou.

5.4.2 Jiné Geografické Objekty

Geografická Doména:

Geografické Domény se zavedly v článku 5.3.5.1. Mají stejnou strukturu jako Zóny. Každý Aplikační obsah obsahuje přesně jednu Geografickou Doménu. Geografická Doména se definuje tak, že:

– všechny jiné Geografické Objekty Kontextu spojené s Účtováním jsou vnitřní částí Geografické Domény;

– Geografická Doména nepokrývá více než oblast potřebnou pro splnění podmínek uvedených výše, vyhnout se nadměrnému množství bodů potřebných k definici jejího tvaru a zaručit fungování Aplikačního Obsahu.

OBE provádí pouze specifické události Kontextu Aplikačního Obsahu pokud se nachází v Kontextu dané Geografické Domény.

Sektor

Sektory se zavedly v článku 5.3.5.1. Mají stejnou strukturu jako Zóny. Řada všech Sektorů se zvolí tak, že

– Sektory se nikdy nepřekrývají;

– celá oblast je pokryta sektory;

– neexistují rohy s více než třemi sousedními Sektory;

– minimální vzdálenost mezi rohy je 500 metrů.

Z těchto podmínek vyplývá, že sousední Sektory mají společnou část jejich hranic s minimální délkou 500 metrů.

Každý Sektor má ID identitu Sektoru, která je jedinečná v rámci celé silniční infrastruktury, již mohou vozidla dosáhnout. Pokud se vytvoří nové Sektory, musí mít ID identitu, jež se liší od ID identity všech Sektorů, které byly zrušeny v posledních třech aktualizacích těchto dat Sektorů.

Pokud vozidlo vstoupí do určitého Sektoru a Kontext a data Sektoru nejsou OBE dostupná, musí OBE zobrazit příslušnou chybovou zprávu Řidiči/Uživateli prostřednictvím HMI.

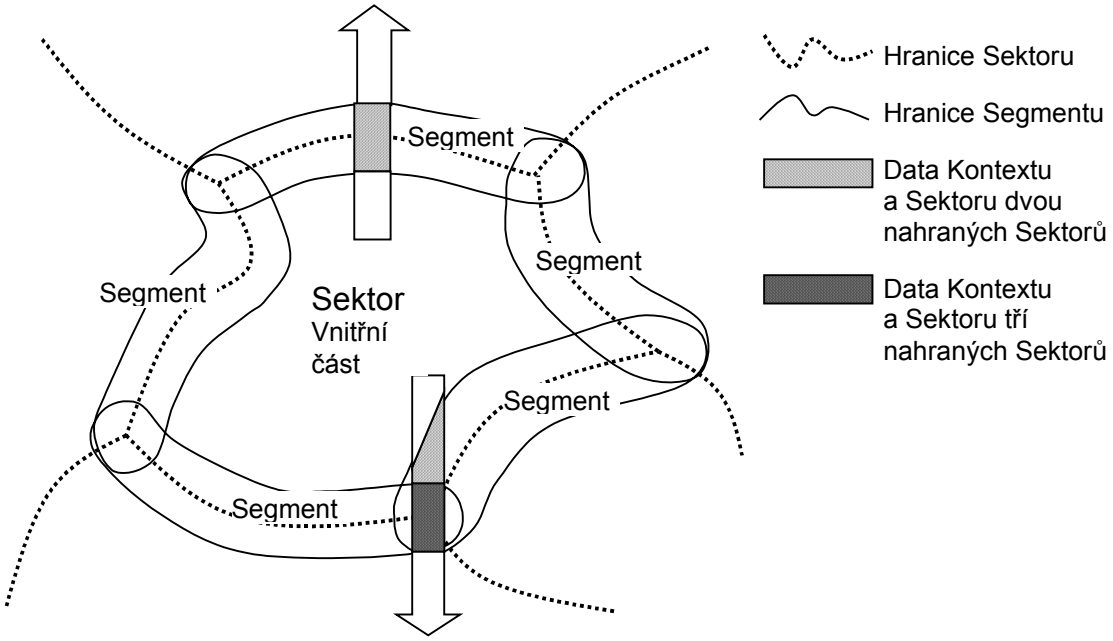
Segment:

Segmenty mají stejnou strukturu jako Zóny. Pro každou dvojici sousedících Sektorů se definuje Segment způsobem, že

– společná část hranice mezi dvěma Sektory je uvnitř daného Segmentu;

– vzdálenost mezi hranicemi Segmentu a společnou částí hranic sousedících Sektorů se nachází přibližně mezi 300 a 500 metry.

Segmenty jsou druhem tranzitních oblastí mezi Sektory a zajišťují, aby Kontext a data Sektoru byly dostupné před tím, než vozidlo vstoupí do daného Sektoru. Nahrávání těchto dat Sousedního Sektoru se zahájí, jakmile vozidlo dosáhne Segmentu směrem do daného Sektoru. Segmenty se identifikují ID identitami těchto dvou Sektorů, ke kterým náleží.



Obrázek 5: Sektory, Segmenty a nahrání Kontextu a dat Sektoru

5.5 Bezpečnost

5.5.1 Úkoly Bezpečnosti

Bezpečnost je prioritou pro všechny vzájemně součinné (interoperable) EFC systémy, aby fungovaly účinně a spolehlivě. Bezpečnostní opatření musí poskytovat prostředky pro následující úkoly bezpečnosti:

– zaručení funkční integrity fyzických komponentů OBE. Tato záruka musí být navržena, aby zajišťovala Poskytovateli Služeb, že se OBE ve vozidle od zahraničního výrobce OBE bude chovat způsobem, který Poskytovatel Služeb vyžaduje;

– zaručení operační integrity běžících Aplikací OBE. Tato záruka musí být navržena, aby zajišťovala všem aktorům jako jsou Poskytovatel Služeb a Řidič/Uživatel, že Aplikace, které byla jednou poskytnuta specifická data a parametry, provede výpočet požadovaných výsledků;

– zaručení integrity dat vyměněných mezi OBE a CE a dále použité jako základ pro účtování poplatku;

– zaručení integrity způsobů platby zvolených pro určité vozidlo v Aplikačním Obsahu.

Pro každé z těchto opatření se musí definovat bezpečnostní cíle, a to opatřeními, které jsou odpovědné za OBE, Aplikační obsah a Platebními Systémy. Na základě těchto cílů se stanovují a realizují bezpečnostní opatření. Tato norma podporuje tato opatření následujícími způsoby:

– definuje Úrovně Bezpečnosti pro OBE a návody k zaručení těchto úrovní (viz Služba Ověřování Entity, článek 5.5.3.1);

– poskytuje ochranu pro přenášená data na spoji CN proti následujícím hrozbám:

  - **Maskování**, při němž třetí strana pošle data, která předstírají, že pocházejí od důvěryhodné entity;
  - **Odmítnutí**, při němž jedna z entit účastnících se přenosu dat posléze popře, že vytvořila přenesená data;
  - **Manipulace**, v níž třetí strana změní data přenesená mezi důvěryhodnými stranami;
  - **Odposlouchávání**, v němž třetí strana obdrží data poslaná mezi důvěryhodnými stranami; informace, které nemá právo vlastnit;
  - **Přehrávání**, v němž třetí strana pošle opětovně data, která již byla v minulosti mezi důvěryhodnými stranami přenesena, a předstírá, že jsou nová.

5.5.2 Bezpečnostní rámec

Bezpečnostní opatření, která se zavedou podle této normy, závisí na Typu Transakce a dalších Parametrech. Pravidla pro zavedení jsou uvedena v článku 9.3 (není součástí překladu pozn. překl.). Předpokládá se, že se opatření zavedou do obecného bezpečnostního rámce, jak je uvedeno v této sekci. Toho lze dosáhnout použitím příslušného výběru možností a parametrů v rámci určitých zpráv, jak se definuje v této normě. V jakékoliv případě se předpokládá, že všechny entity zainteresované v Transakcích podle této normy jsou schopné podpořit bezpečnostní rámec a bezpečnostní služby zde definované.

Šifrovací metody se používají k zaručení bezpečnosti dat na spoji CN. Tyto metody jsou zavedeny takovým způsobem, aby se mohly snadno rozšířit do dalších komunikačních spojů, a tudíž se mohly použít ve všeobecné komunikační síti. Bezpečnosti dat se dosáhne jako bezpečnosti z jednoho konce na druhý (end-to-end security), což znamená, že se bezpečnostní služby zavedou zadáním požadavků pouze pro odesílatele a příjemce dat, ale ne pro cestu spojení. To znamená, že se nevylučují žádné hrozby pro bezpečnost dat kromě odposlouchávání, ale všechny ostatní hrozby lze detekovat předtím, než jsou data přenosu použita příjemcem včetně toho, že šifrovací klíče odesílatele a příjemce nejsou ohroženy.

Vyžaduje se, aby Entity účastnící se v transakcích byly schopny získat dvojici odpovídajících si šifrovacích klíčů, Veřejný klíč a Soukromý klíč. Veřejný klíč se používá k šifrování dat asymetrickou šifrovací metodou; tato data lze dešifrovat použitím odpovídajícího Soukromého klíče a dešifrovací částí stejného asymetrického algoritmu. Soukromý klíč se musí uložit entitou, která jej získala způsobem, jenž umožňuje použití pro opakované dešifrování dat. Proces dešifrování, uložení a přenosu Soukromého klíče musí být chráněn způsobem, kdy Soukromý klíč zůstane tajným pro entity, které nemají oprávnění k jeho použití, od okamžiku, kdy se vygeneruje, a jakmile se použije entitou, která jej získala. Veřejný klíč je volně přístupný pro všechny entity.

Pro některé bezpečnostní služby uvedené v článku 5.5.3 se používají symetrické klíče. Stejný klíč lze poté použít pro šifrování i dešifrování a tento klíč musí být tudíž k dispozici odesilateli i příjemci dat, která jsou předmětem ochrany. Klíč je generován odesílatelem a přenesen příjemci použitím asymetrického šifrování pro ochranu proti odposlouchávání. Symetrické šifrování je méně náročné na

dobu výpočtu a objem paměti a minimální velikost balíku šifrovaných dat je mnohem menší než při asymetrickém šifrování. Symetrické šifrování nelze použít u některých bezpečnostních služeb.

Tato norma nedefinuje nebo nepředepisuje specifické šifrovací algoritmy nebo požadavky na šifrovací klíče (délku klíče, generující proces klíče), ale definuje postupy, jak mohou entity, které jsou zahrnuty v přenosu tajných dat, stanovit tyto položky výměnou odpovídajících parametrů. Operátoři systému EFC založeném na této normě se potřebují dohodnout na minimálním řadě algoritmů a povolené délce klíčů, které musí podporovat veškerá zařízení.

Pro splnění všeobecných bezpečnostních požadavků má každý šifrovací klíč omezenou životnost. Postup generování nových klíčů není předmětem této normy, ale norma definuje postupy pro oznámení potřeby nového klíče a postupy pro distribuci těchto klíčů na spoji CN.

5.5.3 Bezpečnostní služby

Ochrana dat přenesených v rámci transakcí vyžadovaných bezpečnostními opatřeními je zaručena použitím bezpečnostních služeb. V těchto službách, před posláním dat, jsou tyto služby změněny nebo jsou přidány nové bezpečnostní prvky se specifickými daty. Postupy jsou popsány v následujících článcích na obecné úrovni. Pro technické podrobnosti o realizaci těchto postupů je nutné použít jiné normy, které mohou obsahovat podrobnější popis. Následující normy spojené s bezpečností jsou pro takový účel vhodné:

ISO 9594-1

ISO 9594-6

ISO 9594-8

ISO 14821-5

Návrh ISO 15764

5.5.3.1 Prověření Entity

Pro každou entitu, která je zahrnuta do komunikace na spoji CN založené na této normě se definuje následující:

- Identifikátor Entit je řetězcem dat, který je jedinečný v celém systému EFC v každém případě;
- Hodnoty Parametru Použití, které stanovují přijaté Kategorie Dat ve dvou případech: pokud entita přijímá data, musí se zkontrolovat, zda-li odpovídají Kategoriím Dat stanovených v Hodnotách Parametru Použití odesilatele předtím, než jsou použity dále, a pokud entita zamýšlí poslat data jiné entitě, musí se zkontrolovat, zda-li Kategorie Dat těchto dat odpovídají Hodnotám Parametru Použití Entity, jež zamýšlí jejich přijetí předtím, než jsou poslány. Parametr Použití odpovídá syntaxi předepsané ISO xxx pro Schéma Entity a musí se předložit k registraci Identifikátoru Objektu v rámci ISO.

Software OBE a CE musí zaručit, že nelze používat data, která pochází od entity, jež nevlastní odpovídající Hodnoty Parametrů Použití a že se žádná data neposílají entitě, která nevlastní žádné Hodnoty Parametru Použití, jež jsou pro tento účel potřebné.

Služba Prověření Entit se používá k zaručení, že entita, jež udává, že vlastní určitý Identifikátor Entit, Hodnoty Parametru Použití a Veřejný klíč, je důvěryhodná; to znamená, že data podle těchto Hodnot lze s touto entitou vyměnit a její Veřejný klíč lze použít v jiných bezpečnostních službách jako Veřejný klíč Entity s tímto identifikátorem.

Poznámka Služba Prověření Entit se nepoužívá pro Veřejný klíč určité entity jako její identifikátor, ale pro oddělený identifikátor entity. To platí ze dvou důvodů: I když existuje jen malá pravděpodobnost, že dvě entity mají stejný Veřejný klíč, není tato možnost teoreticky vyloučena. Také by nebyla zaručena jedinečnost. Druhým důvodem je to, že Veřejný klíč se musí čas od času vyměnit. Identifikátor Entity zaručuje kontinuitu určité identity entity.

Služba Prověření Entit se zakládá na certifikovaném postupu pro zúčastněné entity. Tento postup je proveden Certifikačním orgánem. Certifikační orgán kontroluje, že:

- Identifikátor Entity, jež je schválen pro tuto entitu, která je předmětem certifikace, je jedinečný v celém systému EFC;

- Entita, která je předmětem certifikace, splňuje požadavky pro Hodnoty Parametru Použití, jež jsou pro tento účel schválené;
- Veřejný klíč patří entitě, která je předmětem certifikace; to znamená, že tato entita získala nebo vygenerovala odpovídající Soukromý klíč;
- Entita, která je předmětem certifikace, vlastní Identifikátor Entit a Veřejný klíč Certifikačního orgánu, a tyto prostředky jsou chráněny proti nahrazení jinými bez povolení (autorizace).

Pokud všechny tyto body kontroly jsou kladné, poté Certifikační orgán vydá Certifikáty, které obsahují Identifikátor Entit Entity, která je předmětem certifikace, její Hodnoty Parametru Použití, její Veřejný klíč, Identifikátor Entit Certifikačního orgánu, jeho Veřejný klíč a Dobu Platnosti tohoto Certifikátu. Tento Certifikát je chráněn podpisem Certifikačního orgánu (viz. článek 5.5.3.2).

Certifikáty jsou veřejně přístupné bez jakýchkoliv omezení. Jsou zhotoveny pro certifikovanou entitu a tato entita může prokázat své prověření jiným entitám, které vlastní určitý Certifikát od stejného Certifikačního orgánu, zasláním takového Certifikátu. Tyto entity poté důvěřují takové entitě, používají její Veřejný klíč a aplikují její Hodnoty Parametru Použití pouze poté, co si ověřily Podpis na Certifikátu, jak je popsáno v článku 5.5.3.2 a po potvrzení, že Doba Platnosti není překročena. Tato norma stanovuje postupy posílání Certifikátů jiným entitám.

Poznámka V mnoha případech je užitečné začlenit určitý centrální Certifikační server jako součást CE, který obsahuje všechny Certifikáty jednoho nebo více Certifikačních orgánů v rámci systému EFC. Výměna dat mezi takovými Certifikačními servery není předmětem této normy. Pro tento účel existují jiné mezinárodní normy (například ISO xxx).

Pro možnost použití více Certifikačních orgánů v situacích v rámci systému EFC podporuje tato norma řetězení certifikátů. To znamená, že jeden Certifikační orgán vydá Certifikát pro jiný Certifikační orgán a tímto úkonem schválí všechny Certifikáty vydané tímto jiným Certifikačním orgánem. Na úrovni certifikovaných entit vyvolá tento úkon dva důsledky:

- Určitá entita certifikovaná Certifikačním orgánem, která obdržela Certifikát od tohoto Certifikačního orgánu pro jiný Certifikační orgán, může získat Identifikátor Entit a Veřejný klíč tohoto jiného Certifikačního orgánu a používat jej k ověření Podpisů na Certifikátu stejným způsobem, jako Identifikátor Entity a Veřejný klíč svého vlastního Certifikačního orgánu, jakmile se Certifikát svého vlastního Certifikačního orgánu pro jiný Certifikačním orgán stane platným.
- Určitá entita certifikovaná Certifikačním orgánem, která obdržela Certifikát pro svůj vlastní Certifikační orgán od jiného Certifikačního orgánu, může prokázat svou autenticitu posláním obou Certifikátů. Takový řetězec Certifikátů je ověřen nejdříve ověřením druhého Certifikátu a použitím Veřejného klíče certifikovaného Certifikačního orgánu a poté se ověří první Certifikát.

Mnohonásobné řetězení Certifikátů se nevylučuje, ale musí se zaznamenat, že cestu Certifikátů přes několik Certifikačních orgánů, mezi dvěma entitami s odlišnými Certifikačními orgány, lze obecně nalézt pouze v případě, že existuje hierarchická struktura Certifikačních orgánů.

V postupných popisech, pokud existuje zmínka o Certifikátu, lze také do ní zahrnout řetězení Certifikátu. Podle doby platnosti se Certifikáty musí čas od času vyměnit, neboť s nárůstem doby použití Soukromého klíče vzrůstá nebezpečí ohrožení. Nový Certifikát pro entitu musí obsahovat stejný Identifikátor entit jako používal předchozí Certifikát a nový Veřejný klíč. Hodnoty Parametru Použití lze použít po zjištění, že odpovídající požadavky jsou splněny. Nové Certifikáty se musí vydat stejným Certifikačním orgánem nebo Certifikačním orgánem, který byl tímto Certifikačním orgánem certifikován. V případě, že nový Certifikát vydá jiný Certifikační orgán, poté se nový Certifikační orgán stane „výchozím“ Certifikačním orgánem této entity a Veřejný klíč předchozího Certifikačního orgánu lze použít pouze k ověření Certifikátů, pokud existuje platný Certifikát nového Certifikačního orgánu pro předchozí Certifikační orgán. Certifikáty pro stejnou entitu, jejichž doby platnosti se překrývají, jsou povoleny. V takovém případě při poslání Certifikátu se musí poslat vždy Certifikát, jehož doba vypršení platnosti je delší.

Tato norma podporuje zrušení Certifikátů v případě, že je Soukromý klíč certifikované entity shledán ohrožen nebo se Hodnoty Parametru Použití staly neplatnými. Existuje seznam zrušení pro OBE a jiný seznam zrušení pro entity CE. Seznam zrušení pro OBE, poněvadž se nepoužívá žádné přímé spojení OBE v systému EFC, se pouze vymění mezi entitami CE a netvoří součást spoje CN mezi OBE a CE specifikovaných v této normě. Seznam zrušení entit CE je dostupný OBE, Managementem Sektoru pro všechny entity CE, které se zúčastňují Transakcí v jeho Sektoru a pro Management

Sektorů, (kteří jsou sami entitami) sousedních Sektorů. Je na odpovědnosti každé entity, která má v úmyslu se účastnit v zabezpečených transakcích, se rozhodnout, zda-li potřebuje zkontrolovat, že Certifikát druhé zúčastněné entity není zrušen.

Všechny entity musí čas od času vyměnit Veřejný a Soukromý klíč Certifikačního orgánu. To se musí provést tak, aby žádný Certifikát vydaný Certifikačním orgánem nepřekročil dobu platnosti přes dobu platnosti klíčů Cerfikačního orgánu. Z tohoto důvodu se musí stanovit překrývání dob platnosti klíčů Certifikačního orgánu. Certifikační orgán vydá Certifikát pro svůj nový Veřejný klíč, který je podepsán použitím předchozího Soukromého klíče. Postup pro nahrazení Certifikátu určeného pro entitu certifikovanou Certifikačním orgánem novými klíči je popsán v případě, že předchozí a nový Certifikační orgán jsou ve skutečnosti identickými orgány a že jsou spojené prostřednictvím Certifikátu vydaného pro tento Certifikační orgán.

5.5.3.2 Značení zpráv

Služba značení zpráv se používá pro následující účely:

- Zaručuje, že data přenesená při transakci pocházejí od entity s daným Veřejným klíčem, který je znám příjemci těchto dat. Tato služba se používá v případě, že hrozí maskování nebo odmítnutí.
- Chrání proti manipulaci, což zaručuje, že data přenesená od jedné entity k druhé entitě zůstanou nezměněna při své cestě komunikační sítí.
- Chrání proti přehrávání, což zaručuje, že přenesená data se pošlou entitě příjemci poprvé.

Postup Služby značení zpráv je následující: původce dat, která jsou předmětem ochrany, přidá k nim podpis, což je realizováno použitím Transformační Funkce na data, která jsou předmětem ochrany, a dešifrováním výsledného řetězce dat použitím Soukromého klíče původce. Příjemce těchto dat, která jsou předmětem ochrany, ověří Podpis použitím stejné Transformační Funkce na data a porovná výsledný řetězec dat s Podpisem, zašifrovaným použitím Veřejného klíče entity, která se vydává za původce. Přijmutí dat od této entity závisí na shodnosti těchto dvou datových řetězců.

Možný útočník snažící se poslat data, která vydává za data pocházející od této entity, není schopen vytvořit platný Podpis, protože nemá přístup k Soukromému klíči. Takto jsou data ochráněna proti maskování. Pouze entita, která vlastní Soukromý klíč, je schopna vytvořit platný Podpis. Dokonce i pokud jiná entita by chtěla získat data s platným Podpisem této entity a snažila by se nalézt jiná data, pro která je Podpis také platným, nebylo by to možné z důvodu vlastností Transformační Funkce. Takto je prokázáno, že podepsaná data pocházejí od entity s Veřejným klíčem, který byl úspěšný při ověření podpisu, a tudíž vylučuje odmítnutí.

V případě, že entita příjemce ověřující Podpis změnila data, tato změna vyvolá odlišnou Transformaci a Podpis nebude shledán platným. Takto se chrání proti manipulaci.

Ochrana proti přehrávání je následující: v první zprávě Transakce se Identifikátor entity odesílatele, zamýšlený příjemce a Číslo Relace zahrnou do dat, která jsou předmětem ochrany (tzn. Data, na která se použije Transformační Funkce), a do všech následujících zpráv Transakce se zahrne Číslo Relace a Číslo Zprávy. Číslo Relace je jedinečné pro všechny transakce mezi odesilatelem a příjemcem a Číslo Zprávy je číslem, které se zvyšuje po jedné pro každou následující zprávu v rámci této Transakce. Tudíž může příjemce první zprávy zkontrolovat prostřednictvím identity odesilatele a příslušného Čísla Relace, že zpráva je nová, a příjemci následujících zpráv mohou udělat to samé na základě Čísla Relace a Čísla Zprávy. Změna těchto identifikátorů a čísel ve zprávě, jež by vedla k jejich přehrávání, se detekuje příjemcem, v případě změny Podpisu, neboť tím se změní Transformace.

Tato norma nedefinuje nebo nepředepisuje specifickou Transformační Funkci, ale definuje postupy, jak mohou entity používající Službu Značení zpráv v Transakci stanovit Transformační Funkci výměnou odpovídajících parametrů. Operátoři systémů EFC založených na této normě se potřebují dohodnout na minimální řadě Transformačních Funkcí, která musí být podpořena všemi zainteresovanými entitami. Kombinací Značení zpráv a Službou Prověření Entit se zaručuje, že zprávy pocházející od entity, která vlastní stejný Identifikátor entit jako se udává ve zprávě a stejné Hodnoty Parametru Použití stanovené v odpovídajícím Certifikátu, zůstanou nezměněny na cestě k entitě příjemce. Toto je obvykle nutné, neboť použití Služby Značení zpráv bez Služby Prověření Entit obecně nevede k efektivní ochraně.

Jedním z použití Služby Značení zpráv je Podpis Certifikátů ve Službě Prověření Entit.

5.5.3.3 Prověření zpráv

Služba Prověření zpráv se používá:

- k zaručení, že data pocházejí od entity, která zná symetrický klíč, jenž se používá ve Službě, a v tomto smyslu ochraňuje před maskováním třetími stranami, které symetrický klíč neznají;
- k ochraně před manipulací ve smyslu, že třetí strana bez znalosti symetrického klíče změní data, což lze detekovat entitou příjemce;
- k ochraně před přehráváním, což zaručuje, že jsou přenesená data poslána entitě příjemci poprvé.

Pro tuto službu musí být symetrický klíč oběma entitám dostupný. Používá se k vytvoření Autentizačního Kódu Zprávy (MAC) následujícím způsobem: Určitá Transformační Funkce se použije na soubor dat, jak je popsáno v článku 5.5.3.2, a výsledný řetězec dat se zašifruje symetrickým klíčem. Výsledný MAC se připojí k souboru dat, který je předmětem ochrany. Příjemce zkontroluje přijatý soubor dat tím, že dešifruje MAC symetrickým klíčem a porovná jej se stejnou Transformací použitou na soubor dat.

Útočník, který nezná symetrický klíč, nemůže vygenerovat platný MAC. Tudíž tyto postupy chrání před maskováním. Také pro Službu Značení zpráv není možné změnit data bez toho, aniž by se MAC stal neplatným, a tudíž je zaručena integrita dat.

Ochrana proti přehrávání se provede stejným způsobem jako při Službě Značení zpráv.

Služba Prověření zpráv neposkytuje ochranu proti odmítnutí, protože entita, která poslala data, může posléze tvrdit, že entita příjemce je vygenerovala a vytvořila MAC. Toto nelze vyloučit, protože příjemce dat zná symetrický klíč potřebný pro generování MAC.

Při Službě Značení zpráv vede pouze kombinace Ověření Zprávy se Službou Prověření Entit k účinné ochraně. Pro spojení těchto Služeb se vygeneruje symetrický klíč jednou z těchto dvou entit a pošle se druhé entitě zašifrovaný Veřejným klíčem, který je obsažen v Certifikátu této entity (viz článek 5.5.3.1).

5.5.3.4 Šifrování

Služba šifrování se používá proti odposlouchávání zobrazením dat, jenž je nesmyslné pro ty, kteří je zachycují, a nemají povolení k tomu, aby rozuměli jejich obsahu.

Služba šifrování se provádí použitím asymetrického nebo symetrického klíče na data, která jsou předmětem ochrany.

Jak je zmíněno v článku 5.5.2 jedním z použití Služby šifrování založené na asymetrickém šifrování je přenos symetrických klíčů.

6 Scénáře Transakcí

Není účelem této normy definovat všechny případy užití systému EFC. Případy užití systému EFC, které zahrnují pouze aktora na straně CE, nejsou popsány do podrobností a existuje o nich zmínka pouze, pokud je to třeba v obecném popise. Případy užití systému EFC, které se týkají strany OBE, jsou pouze popisovány nepřímým způsobem podle možnosti ovlivnění alespoň z části jinými případy užití za účasti obou stran CE a OBE. Například detekce použití části silniční infrastruktury, která je předmětem platby, v rámci platebního procesu (viz. článek 5.3.2), se celá odehrává v OBE komunikujícím s Řidičem/Uživatelem, a je ponechána na výrobci OBE. Je ale ovlivněna Aktualizacemi Dat Kontextu (viz 5.3.5.1), a tudíž jsou výrobci omezeni tím, že při navrhování softwaru OBE musí brát v úvahu Aktualizace Dat Kontextu specifikované v této normě.

Tato norma definuje rámec pro začlenění těchto případů užití, které zahrnují obě strany CE a OBE a jsou založeny na spojení prostřednictvím spoje CN. Rámec se udává v termínech Scénářů Transakcí. Komunikační spoj CN se používá ve třech hlavních scénářích:

- Manager uživatelských/přístupových práv;
- Řízení účtování;
- Řízení systému EFC.

Každý případ užití odpovídající takovému scénáři se skládá z několika jiných případů užití, jak je vysvětleno v tomto článku v diagramech případu užití. V každém z těchto scénářů se může vyskytovat několik typů výměn zpráv nebo Transakcí, které zajišťují základní funkce systému EFC.

To vede k hierarchické struktuře Transakce uvedené na obrázku 6. Každá specifická transakce je zahájena OBE nebo CE, jak je uvedeno na obrázku. Transakce zahájené CE mohou být vysílány nebo spojeny z bodu do bodu.

Obrázek 6 Přehled Transakcí (Transaction Overview) je uveden na poslední straně překladu. (pozn. překl.)

Diagramy případu užití ukazují zainteresování následujících aktorů:

- **Řidič/Uživatel:** Tento aktor používá spolu s vozidlem i část silniční infrastruktury, která je předmětem platby, a hodlá zaplatit za tuto službu na základě dat přenesených v systému EFC. Předpokládá se, že účast Řidiče/Uživatele v systému EFC je zajištěna prostřednictvím OBE ve vozidle. Přímé kontakty s jinými aktory bez použití OBE a jeho komunikačních spojů nejsou součástí systému EFC, jak je definováno v této normě. V případě, že některé z těchto Transakcí definovaných touto normou jsou nahrazeny takovými přímými kontakty, musí se to zaznamenat.

  Dvě specifické části OBE jsou zavedeny pro jednání v zastoupení Řidiče/Uživatele: OBU a Platební Médium. OBU zahrnuje část OBE, která obsahuje jedinečný identifikátor hlavní části zařízení (viz. článek 5.1). Platební Médium je nepovinné a může být vloženo do zařízení jako OBU nebo ICC, a je tudíž spojené komunikačním spojem CN.

  Spojení mezi Řidičem/Uživatelem a OBE se předpokládá prostřednictvím HMI nebo ICC. Toto rozhraní není definováno touto normou, ale některé požadavky na toto rozhraní mohou být odvozeny podle některých datových prvků, které jsou přímo spojeny s Řidičem/Uživatelem.

  Vždy existuje vozidlo na straně Řidiče/Uživatele účastnící se systému EFC. Toto vozidlo není zavedeno jako aktor, protože je vůči systému EFC zcela pasivní. Tato norma nedefinuje způsob, jak jsou vozidlo a OBE spojeny, ale poskytuje různé možnosti pro toto spojení v Kontraktu o poskytování služby. Předpokládá se, že data o vozidle potřebná v systému EFC jsou dostupná v OBE.

  Řidič/Uživatel jedná v rámci této normy jako smluvní strana Kontraktu o poskytování služby a Kontraktu o platbě, která tyto smlouvy podepisuje jako aktor odpovědný za akce, jež probíhají na straně OBE, a jako vlastník vozidla. Mohou existovat různé osoby nebo instituce, které se účastní systému EFC v těchto rolích. Při popisu Scénářů Transakcí se termín Řidič/Uživatel používá pro všechny tyto zmíněné možnosti a podle situace bude jasně určeno, o jakou roli se jedná.

- **Poskytovatel Služeb:** aktor odpovědný za Aplikační obsah se nazývá Poskytovatel Služeb. Je stranou, která se účastní v kontraktech o poskytování služby s Řidiči/Uživateli. Jak je naznačeno v článku 5.3 mohou za různé Aplikační obsahy odpovídat různí Poskytovatelé Služeb a stejná entita může být Poskytovatelem Služeb pro různé Kontexty.

- **Vydatel metody platby**, někdy nazývaný pouze Vydatel: aktor poskytující Platební Prostředky Řidiči/Uživateli, které mu umožňují zaplatit poplatky v rámci systému EFC. Je stranou, která se účastní v Kontraktech o platbě s Řidiči/Uživateli. Stejný Vydatel může poskytovat různé Platební Prostředky. Předpokládá se, že Vydatelé sjednali dohody s Poskytovateli Služeb o použití Platebních Prostředků v rámci Aplikačních Obsahů a o přenosu finančních prostředků.

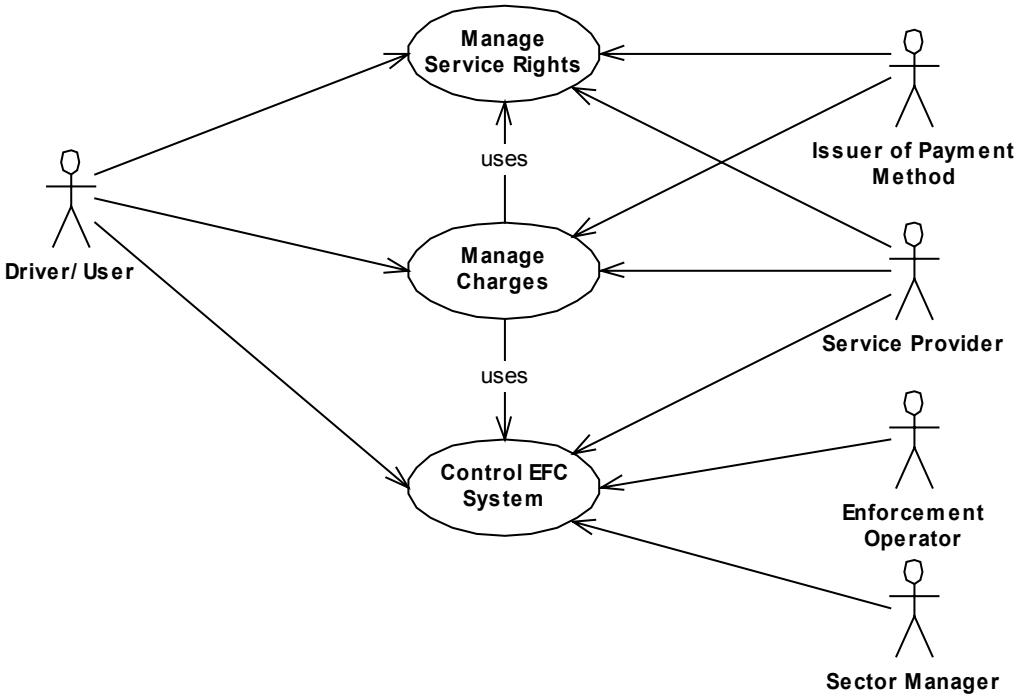
- **Operátor dohledového systému:** Tento aktor má za úkol kontrolovat, zda-li jsou v určitém Aplikačním Obsahu prováděny procesy účtování a platby správně, a proto potřebuje data z OBE. Stejný Operátor dohledového systému může být odpovědný za Dozor různých Kontextů.

  Operátor dohledového systému nesmí být přítomen na spoji CN ve všech Kontextech, může například používat DSRC jako komunikační médium vůči OBE.

  Předpokládá se, že k provedení takového úkolu může Operátor dohledového systému získat data od Poskytovatele Služeb, ale tento případ není předmětem této normy.

- **Management Sektoru:** Je odpovědný za jeden nebo více Sektorů, což znamená, že poskytuje Data Kontextu a Data Sektoru pro tyto Sektory. Předpokládá se, že získá Data Kontextu o Aplikačních Obsazích s Geografickou Doménou v jeho Sektoru od příslušných Poskytovatelů Služeb.

Poskytovatel Služeb, Vydatel metody platby, Operátor dohledového systému a Management Sektoru se účastní Transakcí na straně CE, což znamená, že jsou odpovědni za příslušné části CE (které mohou být rozděleny nebo umístěny v různých oblastech, s odlišnými adresami na spoji CN) a mají s nimi rozhraní. Je možné, že stejná osoba nebo instituce hraje roli několika takových aktorů. Poskytovatel Služeb může být například Vydatelem specifické metody platby pro svůj Aplikační obsah, nebo může být identický s Operátorem dohledového systému, nebo může být Managementem Sektoru a to Sektoru, ve kterém má jeho Kontext svou Geografickou Doménu. Tato norma poskytuje možnost přidělit různé adresy entitám podle různých typů aktorů. Výrobce OBE se nepovažuje za aktora v rámci systému EFC. Jeho účast je pouze skrze vlastnosti OBE, a protože jsou tyto vlastnosti statické, neexistuje na spoji CN pro výrobce žádné spojení s OBE.



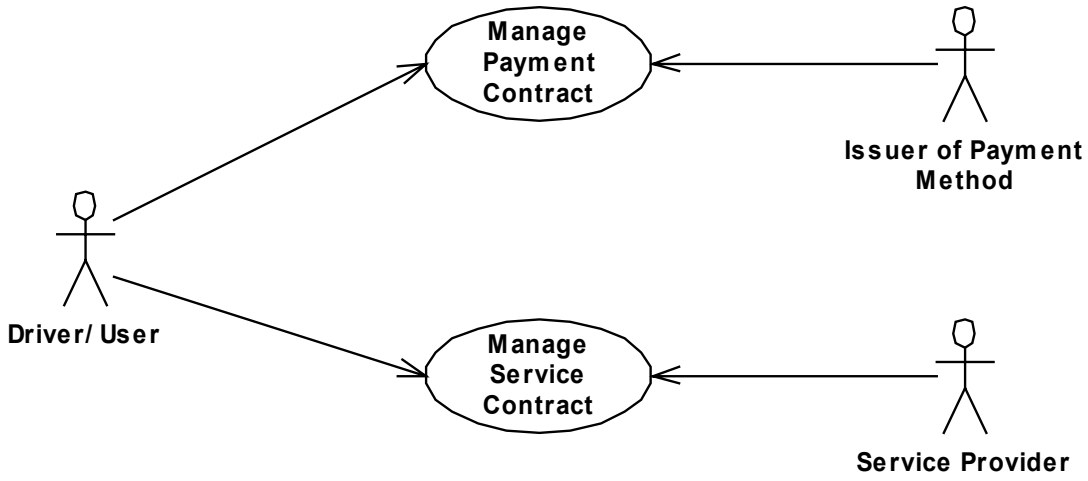
Legenda
Driver/User – **Řidič/Uživatel**
Manage service rights – **Manager uživatelských/přístupových práv**
Manage charges – **Řízení Účtování**
Control EFC System – **Řídicí Systém EFC**
Issuer of the payment method – **Vydatel metody platby**
Service Provider – **Poskytovatel Služby**
Enforcement Operator – **Operátor dohledového systému**
Sector Manager – **Management Sektoru**

Obrázek 7 – Přehled Transakcí na nejvyšší úrovni

Případy užití Řízení Účtování zahrnuje proces účtování a, pokud je součástí systému EFC, i proces platby, jak je popsáno ve článku 5.3.3. Proto používá informace stanovené ve Smlouvách o případu užití Managera uživatelských/přístupových práv. Navíc používá informace o datech mýtného získané od případu užití Řídicího Systému EFC a poskytuje informace o tomto případě užití pro monitorování OBE.

6.1 Scénáře Managera uživatelských/přístupových práv

Manager uživatelských/přístupových práv zahrnuje řízení Kontraktu o poskytování služby a řízení Kontraktu o platbě.



Legenda
Driver/User – **Řidič/Uživatel**
Manage Payment Contract – **Uzavření kontraktu o platbě**
Manage Service Contract – **Uzavření kontraktu o poskytování služby**
Issuer of the payment method – **Vydatel metody platby**
Service Provider – **Poskytovatel Služby**

Obrázek 8 – Případ užití Managera uživatelských/přístupových práv

Kontrakt o poskytování služby a Kontrakt o platbě jsou nezávislé. Jsou spojené pouze prostřednictvím Platebních Prostředků následujícím způsobem: každý Aplikační obsah umožňuje použití jistých Platebních Prostředků. Příslušná informace je obsažena v Kontraktu o poskytování služby přiložené ke Smlouvě nebo v Datech Kontextu (viz. článek 5.3). Každý Kontrakt o platbě umožňuje použití jednoho Platebního Prostředku. Pro Platební proces (viz. článek 5.3.3), který se začlení do rámce Aplikačního Obsahu, je nutný alespoň jeden Platební Prostředek, který je podporován Kontextem i Kontraktem o platbě.

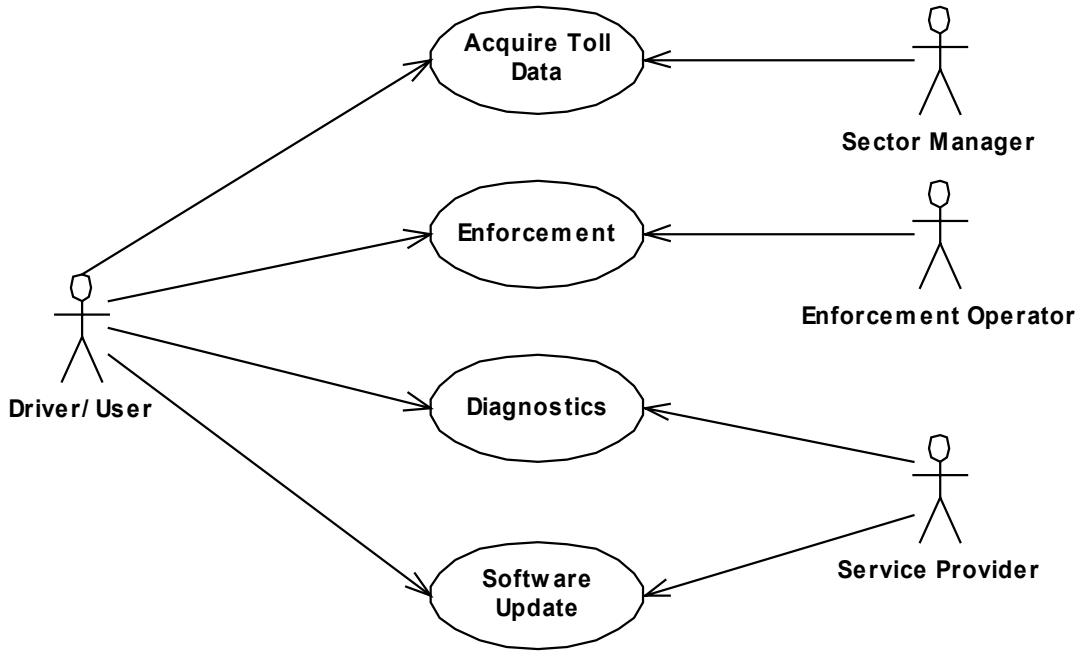
Řízení smluv na spoji CN je pouze nepovinné. Lze sjednat smlouvy použitelné v systému EFC založeném na spojení, které není předmětem této normy.

6.2 Scénáře řízení systému EFC

Případ užití řízení systému EFC zahrnuje následující typy Transakcí:

- Získání Dat Kontextu;
- Aktualizaci Softwaru;
- Diagnostiku;
- Dozor.

Oba scénáře Získání Dat Kontextu i Aktualizace Softwaru existují v módu z bodu do bodu a v módu vysílání.



Legenda
Driver/User – **Řidič/Uživatel**
Acquire Toll Data – **Získání Dat Mýtného**
Enforcement – **Dozor**
Diagnostics – **Diagnostika**
Software Update – **Aktualizace Softwaru**
Enforcement Operator – **Operátor dohledového systému**
Service Provider – **Poskytovatel Služby**
Sector Manager – **Management Sektoru**

Obrázek 9 – Případ užití řízení systému EFC

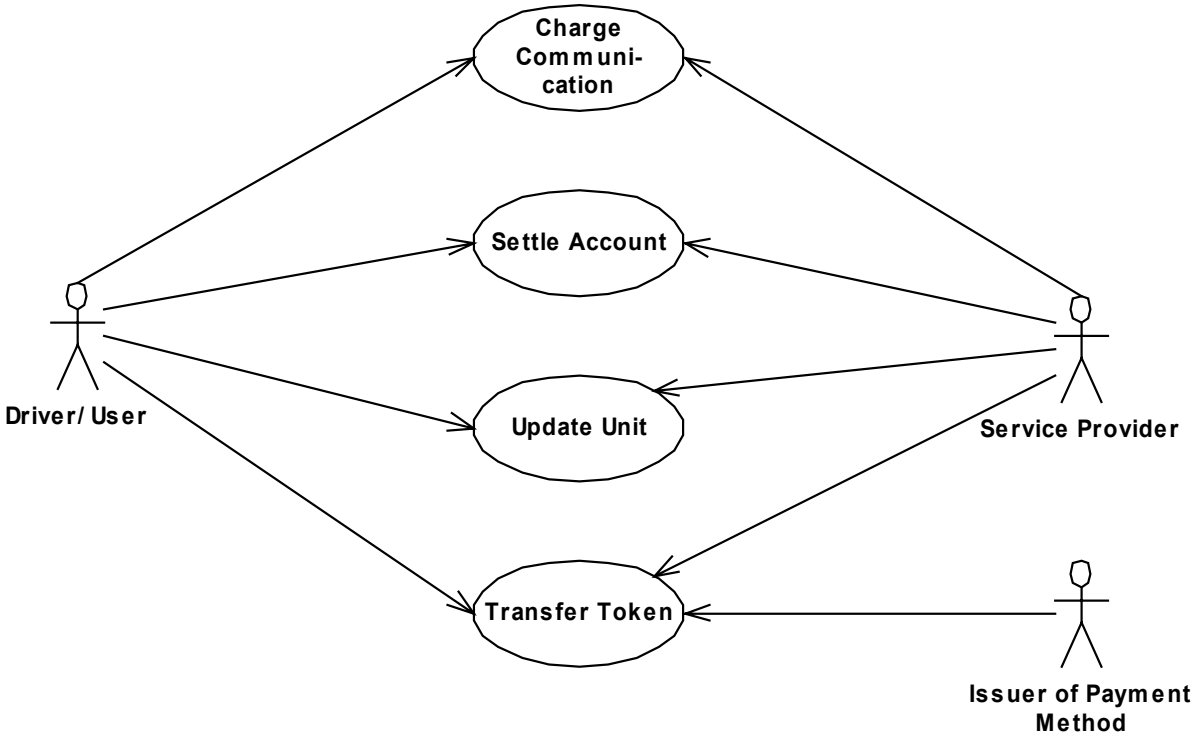
Aktualizaci Softwaru je nutné dokončit předtím, než Vozidlo vstoupí do Geografické Domény Aplikačního Obsahu, kde je aktualizovaný software potřebný. Informace pro všechny případy, kdy lze nebo je nutné provést Aktualizaci Softwaru, je přenesena do OBE v Transakcích Získání Dat Kontextu.

Transakce Diagnostiky jsou nepovinné a může je Poskytovatel Služby použít pro kontrolu, zda-li OBE řádně pracuje, zatímco se vozidlo vyskytuje v Geografické Doméně jeho Aplikačního Obsahu.

6.3 Scénáře řízení účtování

Případ užití řízení účtování zahrnuje následující typy Transakcí:

- Účtovací Spojení;
- Vyrovnání stavu Účtu;
- Aktualizace jednotky;
- Přenos Jízdenky.

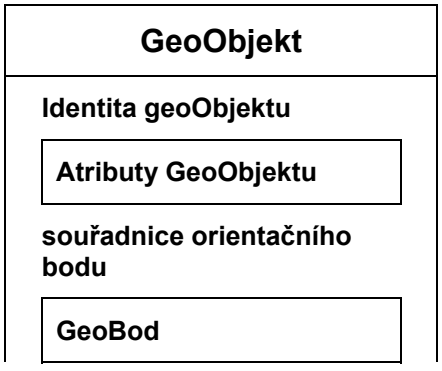


Legenda
Driver/User – **Řidič/Uživatel**
Charge Communication – **Účtovací Spojení**
Settle Account – **Vyrovnání stavu Účtu**
Update Unit – **Jednotka pro Aktualizaci**
Transfer Token **– Přenos Jízdenky**
Service Provider – **Poskytovatel Služby**
Issuer of the payment method – **Vydatel metody platby**

Obrázek 10 – Případ užití řízení účtování

7.1 GeoObjekt

Třída GeoObjekt obsahuje parametry dat Geografických Objektů, jak je popsáno v článku 5.4. Jedná se o zobecnění různých typů Geografických Objektů. Struktura takové třídy GeoObjekt v termínech atributů je uvedena na obrázku 12.



Obrázek 12 – Atributy třídy GeoObjekt a jeho podtřídy

Identita GeoObjektu umožňuje jedinečný odkaz na určitý Geografický Objekt.

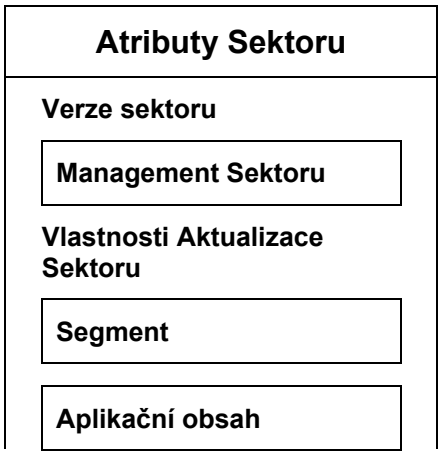
Atributy GeoObjektu obsahují specifické parametry Geografických Objektů různých typů.

Atribut souřadnic orientačního (výchozího) bodu obsahuje geografické souřadnice orientačního bodu a je nepovinný. Pokud takový atribut existuje, stanoví se souřadnice ostatních bodů Geografického

Objektu podle souřadnic orientačního bodu. Tento způsob může pomoci omezit množství dat, které musí být přeneseny, když se GeoObjekt nahrává do OBE.

7.1.1 Sektor

Podtřída GeoObjektu, Sektor, obsahuje všechny parametry spojené se Sektorem, jak je definováno v článku 5.3.5.1 a článku 5.4.2. Identita GeoObjektu pro určitý Sektor je jedinečná v rámci všech existujících Sektorů. Specifické parametry Sektoru jsou obsaženy v atributu Atributy GeoObjektu. Jejich seznam je uveden na obrázku 13.



Obrázek 13 – Specifické Atributy GeoObjektu pro Sektor a jeho podtřídy

Verze atributu udává verzi dat Sektoru. Po provedení Transakce Získání Dat Mýtného musí OBE mít aktuální verzi s datem vypršení platnosti udaným atributem aktuální Verze Data Vypršení Platnosti, a navíc může obsahovat příští verzi, pokud je již dostupná. Atribut Nové Datum udává datum, kdy lze aktualizovat nejnovější dostupnou verzi (viz. článek 5.3.5.1). Pro každý Sektor existuje jeden Management Sektoru, který je specifikován v podtřídě Management Sektoru. Tato podtřída je typu Entity EFC.

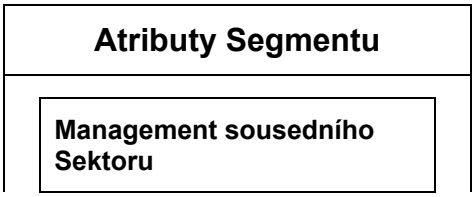
Pro každý Sektor existuje jeden nebo více Segmentů specifikovaných v podtřídě Segment (viz. článek 7.1.2)

Všechny Aplikační obsahy obsahující úplně nebo částečně Geografickou Doménu jsou uvedeny v seznamu podtříd Aplikačního Obsahu.

7.1.2 Segment

Podtřída GeoObjektu, Segment, obsahuje parametry dat spojené se sousedním Sektorem Sektoru, jehož je daný Segment součástí, ve směru Segmentu.

Identita GeoObjektu pro daný Segment je jedinečná v rámci Sektoru, jehož je Segment součástí. Specifické Atributy GeoObjektu pro daný Segment jsou uvedeny na obrázku 14.



Obrázek 14 – Specifické Atributy GeoObjektu pro Segment a jeho podtřídy

Podtřída Management Sousedního Sektoru poskytuje Managementu Sektoru informace o sousedním Sektoru na straně Segmentu hranice Sektoru.

7.1.3 Geografická Doména

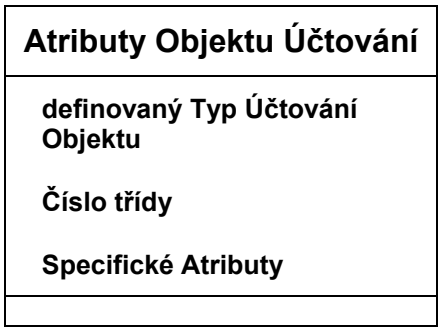
Podtřída Geografické Domény neobsahuje žádné specifické atributy.

7.1.4 Objekt Účtování

Podtřída Objekt Účtování třídy GeoObjektu je součástí třídy Aplikační obsah a obsahuje specifické parametry dat Zón, Koridorů a Virtuálních Portálů obsažené v Aplikačním Obsahu. Atribut Typ GeoObjektu udává, zda-li je Objekt Účtování Zóna, Koridor nebo Virtuální Portál.

Existuje možnost seskupovat Objekty Účtování specifického typu do Řad Objektů Účtování s charakteristickými vlastnostmi (jako například vlastnosti spojené s tarifem). Pokud si Poskytovatel Služby odpovědný za daný Aplikační obsah zvolí tuto možnost, je atribut Identita GeoObjektu Objektu Účtování jedinečný v rámci řady daného Objektu Účtování. V jiném případě je atribut jedinečný v rámci Aplikačního obsahu.

Obrázek 15 udává Objekt Účtování specifických Atributů GeoObjektu.



Obrázek 15 – Objekt Účtování specifických Atributů GeoObjektu

Definovaný Typ Účtování Objektu udává, zda-li je Objekt Účtování Zóna, Koridor nebo Virtuální Portál.

Atribut čísla třídy udává tarifní třídu Objektu Účtování, který se používá pro výpočet poplatku založeném na tarifu stanoveném v daném Aplikačním obsahu.

Specifické Atributy daného Objektu Účtování jsou přítomny pouze v případě, jedná-li se o Koridor, a udávají, jestli je Koridor jednosměrný nebo obousměrný, jeho šířku, šířku oddělující směry v případě obousměrného Koridoru a délku Koridoru.

Obrázek 6 – Přehled Transakcí