EXTRAKT z české technické normy

Extrakt nenahrazuje samotnou technickou normu, je pouze informativním materiálem o normě.

ICS 35.240.60

Dopravní telematika – Elektronické vybírání poplatků (EFC) – Specifikace rozhraní pro dorozumívání mezi operátory

ČSN P ENV 14904

01 8380

Platí od 1.6.2003

35 stran

Úvod

Tato evropská norma definuje rozhraní pro clearing mezi operátory a určuje rámec společné struktury zprávy a datových prvků pro toto rozhraní. Jejím cílem je definovat přenos platby a souvisejících dat elektronického vybírání poplatků jak mezi různými platebními systémy, tak mezi různými operátory jako jsou výběrčí mýtného, operátoři clearingu nebo poskytovatelé veřejných a soukromých dopravních služeb.

Tato norma podporuje:

a) různé platební módy (např. platba před/po použití služby);

b) širokou škálu dopravní a s dopravou souvisejících služeb (mýtné, parkování, převoz/most/tunel, veřejnou hromadnou dopravu, platby za navigaci na trasu apod.);

c) služby operátora (koordinace mezi výběrčími poplatků a místy zpoplatnění apod.);

d) zabezpečení a soukromí.

Užití

Tato norma je důležitá pro operátory systémů, protože podmínky pro clearing.

Norma nestanovuje administrativní postupy a organizační struktury, ani nespecifikuje vyšší (např. panevropskou) úroveň interoperabilního platebního systému. Dále nepopisuje nepřímé (externí) účastníky jako jsou správní úřady, a z toho vyplývá, že se nezabývá obecnou ani specifickou legislativou nebo jinými národními předpisy.

Souvisící normy

Jedná se o normy definující identifikační karty (ISO 7812, 7816-5, ENV 1545-1), finanční transakce (ISO 8583) a informační technologie (ISO 8825-1, 9594, 11770-1). Norma je úzce navázána na hlavní specifikaci elektronického mýtného EN ISO 14906.

1 Předmět normy

Norma prezentuje obecné modely. Pro sestavení jednoduchého (uzavřeného) systému lze použít výběr ze sad rámce rozhraní poskytovaných touto normou.

3 Termíny a definice

Norma uvádí 21 termínů a definicí.

Termíny definující entity systému EFC:

3.4 operátor clearingu *(clearing operator)* subjekt, který vybírá a shromažďuje transakce od jednoho nebo více provozovatelů tak, aby je předal vydavateli; operátor clearingu může provádět také rozdělování mezi jednotlivé poskytovatele služeb; v bankovnictví je tento operátor shodný s nabyvatelem

3.5 agent výběru poplatků *(collection agent)* subjekt zodpovědný za prodej, distribuci a doručení platebních prostředků k uživatelům a výběr poplatků jménem vydavatele; agent výběru poplatků je oprávněn sbírat specifická data uživatelů související s aplikací

3.11 vydavatel *(issuer)* subjekt zodpovědný za platební systém a za vydávání platebních prostředků uživatelům

3.18 poskytovatel služby *(service provider)* osoba, společnost, úřad nebo abstraktní entita nabízející dopravní služby uživateli, za které uživatel musí platit poplatek (poplatky budou v některých případech nulové, např. vozidla záchranné služby)

3.21 uživatel *(user)* subjekt využívající dopravní službu poskytovanou poskytovatelem dopravní služby podle smluvních podmínek; uživatel může být popsán jako předplatitel služby EFC, vlastník vozidla a řidič v případech, kde se nejedná o stejnou osobu nebo společnost

Norma dále definuje termíny týkající se zabezpečení dat v článku 5.5:

utajení *(confidentiality)* citlivá data a informace jsou dostupná pouze oprávněným stranám (důvěrnost obsahu)

integrita *(integrity)* citlivá data, informace a posloupnosti zpráv jsou zajištěny takovým způsobem, že každá změna nebo poškození neoprávněnou stranou je detekována (integrita obsahu, integrita posloupnosti zpráv)

autentizace *(authentication)* proces, který slouží ke zjištění a ověření identity objektu. Objekt musí věrohodným způsobem dokázat, že je skutečně ten, za koho se vydává. Nejčastější způsob autentizace je zadání uživatelského jména a hesla. Výsledkem procesu je potvrzeni nebo vyvrácení identity objektu

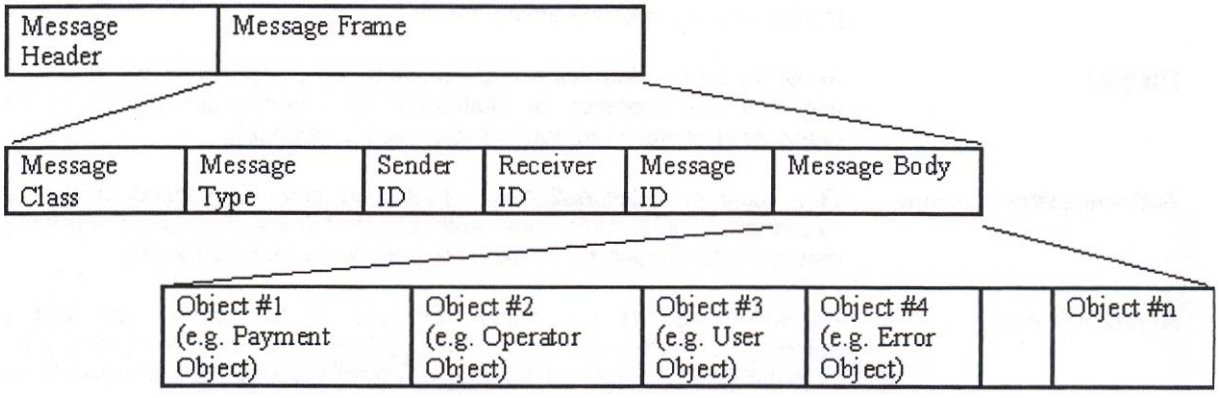
neodmítnutí *(non-repudiation)* ochrana proti popření účasti na komunikaci jednou ze stran účastnících se dané komunikace přes rozhraní

dostupnost *(availability)* data a informace jsou dostupné pro oprávněné strany

audit/kontrolovatelnost *(auditing/accountability)* vlastnost systému zajišťující, že akce libovolného objektu je sledována. K libovolné akci je tedy možné zpětně nalézt jejího původce

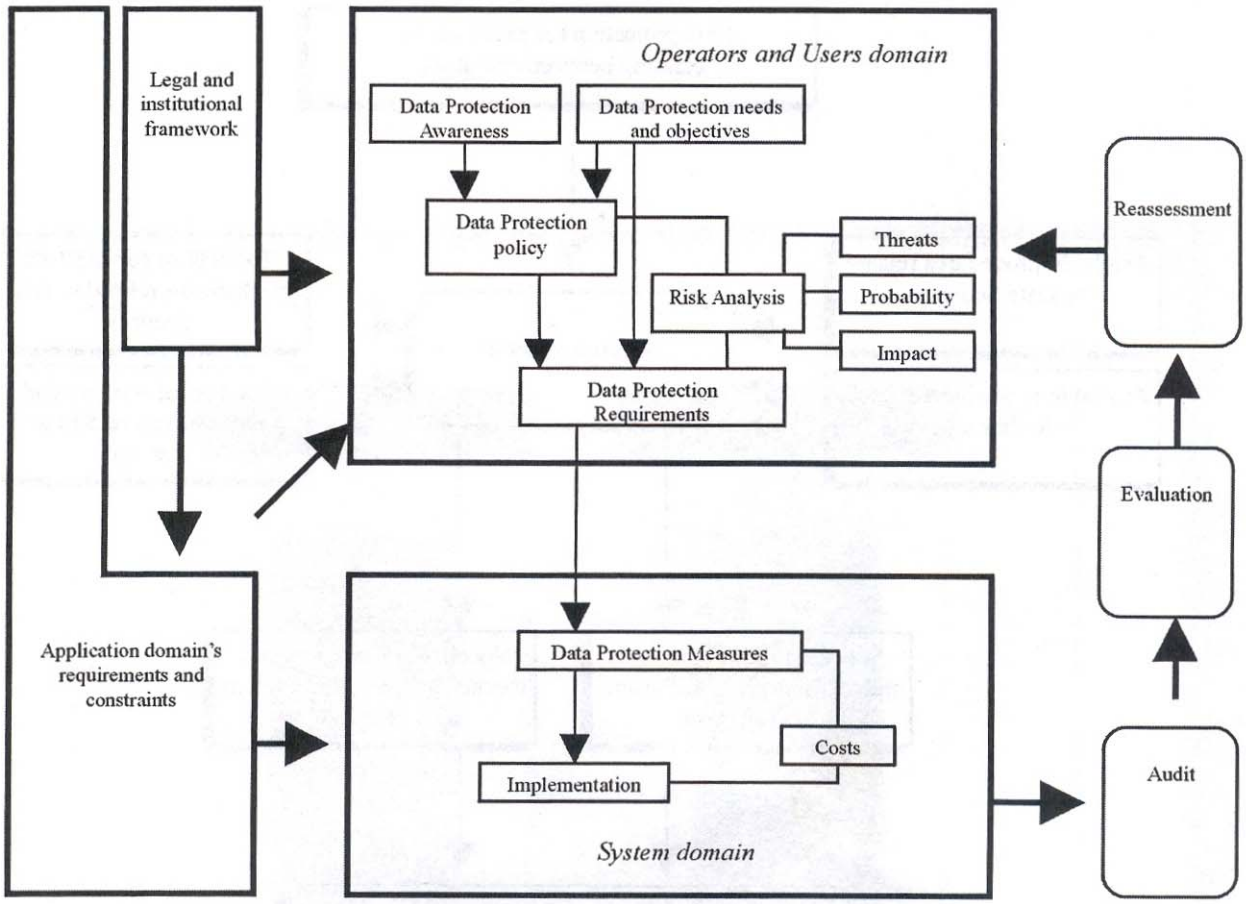
5 Rámec rozhraní

Kapitola 5 definuje společnou strukturu zprávy pro výměnu dat na jakémkoliv rozhraní mezi operátory. Příklad struktury takové zprávy s hlavičkou zprávy a rámcem zprávy je uveden na obrázku 1. Ukázka, jak lze rámec zprávy formátovat, je uvedena v příloze C.



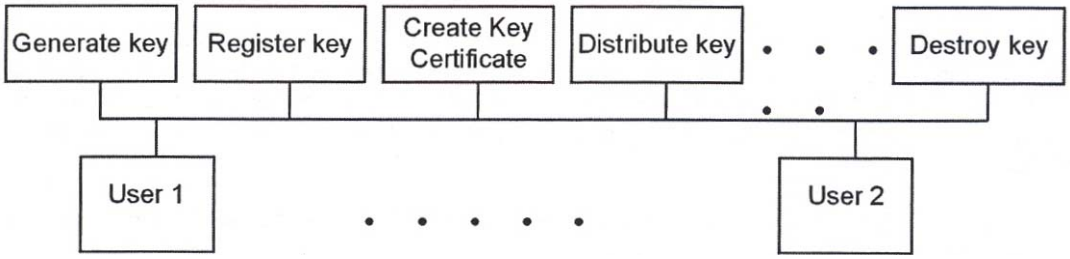
Obrázek 1 – Příklad struktury zprávy

Ochrana dat je nedílnou součástí každé transakce a tato norma rozlišuje následující aspekty zabezpečení dat: utajení, integritu, autentizaci, neodmítnutí, dostupnost a audit. Pro konkrétní specifikaci rozhraní je potřeba učinit analýzu rizik, která spočívá v posouzení možných hrozeb systémům EFC. Výsledkem jsou zaváděná opatření pro ochranu dat v systému EFC. Při definování těchto opatření je nutné vzít v úvahu i náklady spojené s jejich zavedením. Proto se posléze učiní audit a výsledky se dle něj přehodnotí, viz obrázek 2.



Obrázek 2 – Rámec ochrany dat

Norma dále uvádí obecný úvod do problematiky kryptovacích klíčů, které jsou nástrojem pro zabezpečení dat. Popisuje management takového klíče pro použití několika uživateli a jeho různé stavy, viz obrázek 5, v závislosti na použitém zabezpečení a kryptografickém systému.



Obrázek 5 – Služby managementu kryptovacího klíče

6 Metoda popisu dat

V kapitole 6 normy se stanoví metoda popisu dat. Datové typy používané v rozhraní jsou stanoveny v ASN.1, což umožňuje jejich flexibilitu a jednoznačné použití a i bezproblémové použití nových datových typů v budoucnu. Pro kódování jsou stanoveny základní kódovací pravidla (BER), ale je možné použít i jiná pravidla, pokud by tak stanovovala dohoda mezi operátory rozhraní. Popis dat zahrnuje základní datové prvky, které komunikující operátoři potřebují. Pokud je zapotřebí dodatečných dat, lze popis rozšířit na tato data. Tento komunikační protokol mohou využít i jiné strany pro jiné případy, než jsou stanoveny touto normou.

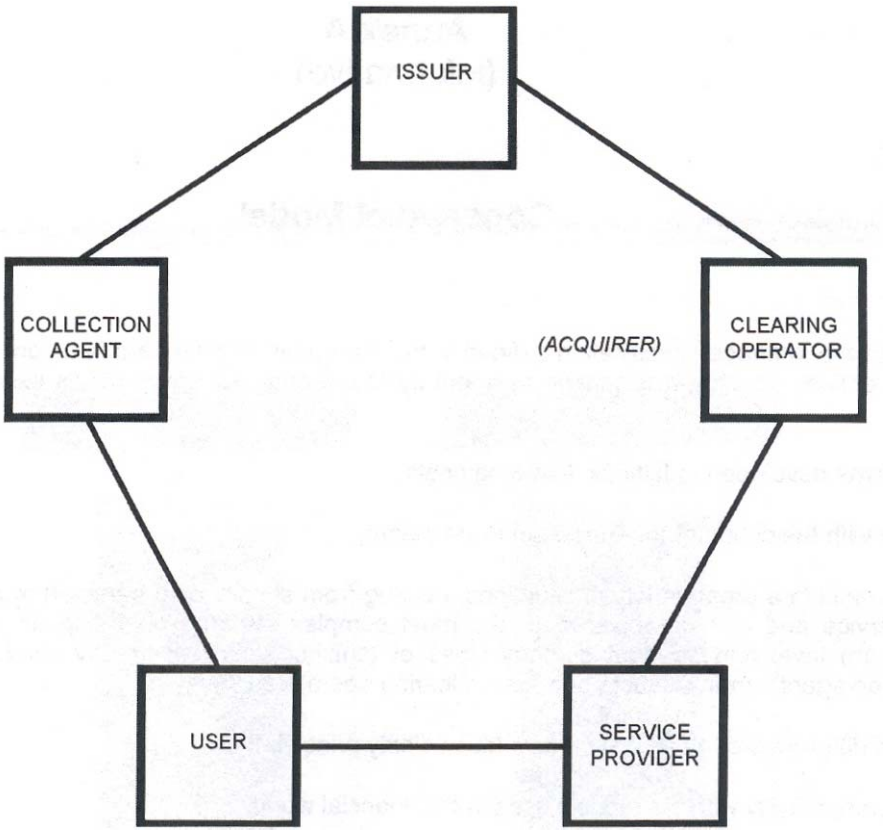
7 Zpráva

Kapitola 7 definuje zprávu. Datový typ „zpráva“ (message) popisuje úplná data přenesená mezi dvěma operátory. Dalšími typy jsou „datová jednotka protokolu“ (ProtocolDataUnit) udávající volbu mezi

dvěma typy datových struktur, dále „lokálně zabezpečená data EFC“ (locallySecuredEFCData), které jsou definovány touto normou a datový typ „externí“ (EXTERNAL), který je datovým typem definovaným jinou blíže nespecifikovanou normou. Datový typ „externí“ lze použít třeba v případě, kdy dva operátoři používají stávající standard a chtějí jej využít pro některé typy přenosu dat. Po začlenění tohoto standardu do struktury zprávy, kterou definuje tato norma, lze použít stejné komunikační spojení. Datový typ „externí“ může zahrnovat identifikátor, který označuje druh dat obsažených ve zprávě. Tato norma identifikátory nedefinuje.

Příloha A (informativní) Konceptuální model

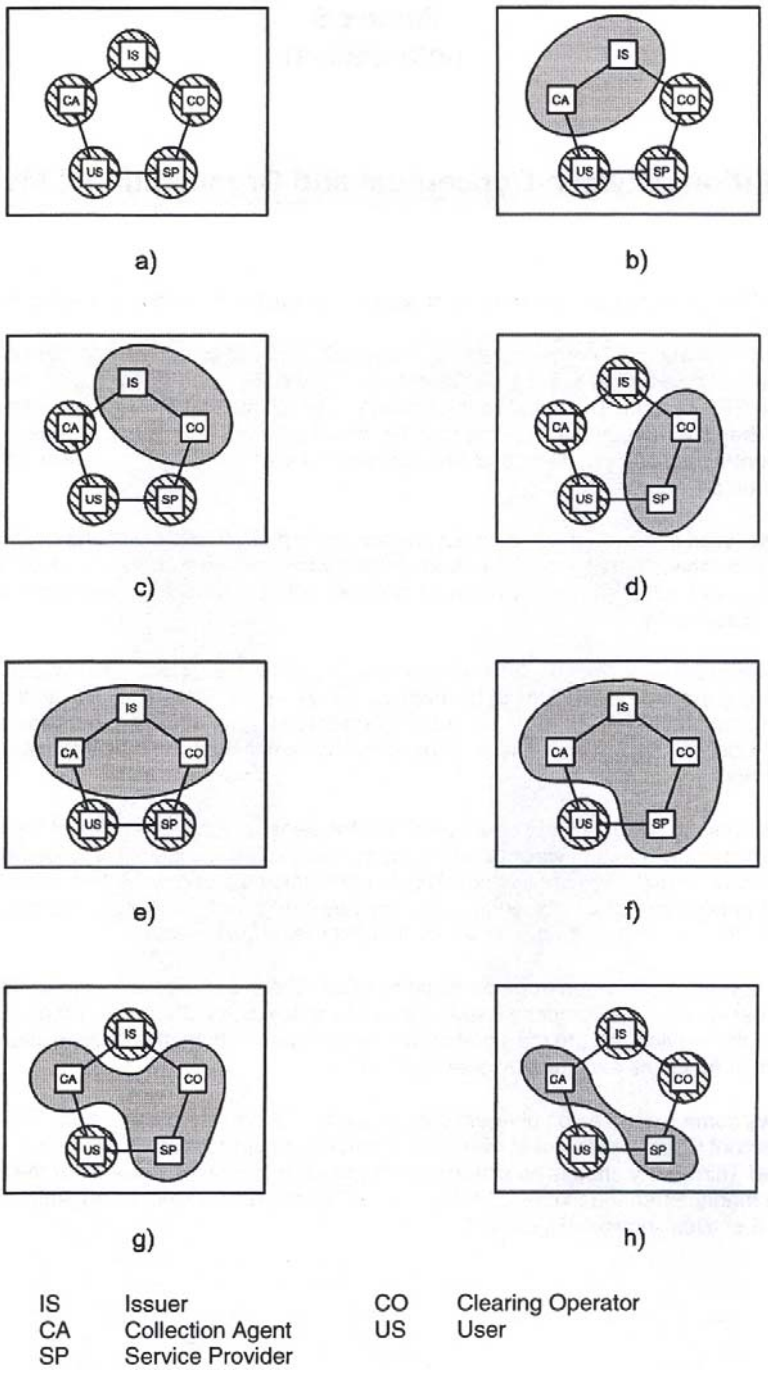
Základem specifikace rozhraní stanovené touto normou je konceptuální model, který definuje entity generického platebního systému a jejich vztahy. Na obrázku A.1 jsou uvedeny tyto entity, nejedná se však o organizace, tzn.že konceptuální model nepožaduje, aby existovala samostatná organizace pro určitou abstraktní entitu. Model odpovídá např. bankovnímu sektoru, a proto je kompatibilní s modely finančního sektoru. Využití konceptuálního modelu je podrobně popsáno v EN ISO 17573.



Obrázek A.1 – Konceptuální model

Příloha B (informativní) Vztah mezi konceptuálním a organizačním modelem

Tato příloha nabízí příklady, jak se mohou abstraktní entity promítnout (mapovat) do organizační struktury v reálném světě. Použitý přístup je striktně oddělen od technických aspektů rozhraní, které ponechává na obchodních dohodách. Lze tak kombinovat více abstraktních entit do jedné organizace, příklady uvádí obrázek B.1.



Obrázek B.1 – Příklady mapování generických abstraktních entit do organizací reálného světa

Dále norma popisuje tyto příklady a uvádí ilustraci způsobu, jakým jednotlivé platební systémy mohou vzájemně komunikovat tak, aby vytvořily integrovaný platební systém vysoké úrovně (např. panevropský).

Příloha C Formát rámce zprávy

Popisuje veškeré prvky, které rámec zprávy nazývaný také datová jednotka protokolu (PDU) obsahuje. Hlavními prvky PDU jsou: třída zprávy, typ zprávy, ID odesilatele, ID příjemce, ID zprávy a tělo zprávy.

Příloha D Datová jednotka zprávy

Uvádí příklady datové struktury prvků PDU.

Příloha E Platební objekty založené na datových prvcích definovaných v ISO 8583

Uvádí příklad datové struktury platby bankovní kartou (BankCardPayment).