EXTRAKT z mezinárodní normy

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

ICS: 03.220.01; 35.240.60

Veřejná doprava osob – Interoperabilní systém managementu sběru jízdného – Část 3: Doplňkové koncepty k části 1 ohledně interoperability v prostředí s více aplikacemi

TNI CEN ISO/TR 24014–3

01 8240

39 stran

Obecná charakteristika

Tato technická normalizační informace popisuje, jak implementovat interoperabilní aplikace managementu sběru (IFM) v prostředí s více aplikacemi a dodatečně vzniklé role a případy použití.

Multiaplikační média otevřou nové možnosti pro samostatné zabezpečené aplikace IFM, aby byly na jednom médiu nahrány a provozovány odděleně. To umožní zajištění spotřebitelsky orientované obchodní interoperability s možností spotřebitele používat stejné médium v různých systémech řízení poplatků, nezávisle na místních způsobech zpoplatnění a specifických systémech a bez potřeby společných obchodních zásad.

Poznámka: Extrakt přejímá původní číslování kapitol.

Užití

Tato technická zpráva popisuje, jak implementovat IFM v multiaplikačním prostředí s více aplikacemi, dodatečně vzniklé role a případy jejich užití.

Je součástí skupiny norem, které jsou řešeny v rámci WG3 ve vztahu k managementu sběru jízdného a navazuje na 1 část, která definuje základní prvky systému managementu jízdného a jeho architektury a 2 část, která doplňuje předchozí část o obchodní modely managementu sběru jízdného.

Pro orgány státní správy je tato technická zpráva zdrojem informací jak implementovat interoperabilní aplikace managementu sběru jízdného.

Pro výrobce telematických zařízení a jejich provozovatele je tato technická zpráva důležitá, protože informuje výrobce a provozovatele o požadavcích na interoperabilitu v prostředí s více aplikacemi. Dále uvádí, že právě implementací standardů do této oblasti veřejní dopravy umožní prosperitu z multiaplikačního prostředí.

Související normy

ISO 24014-1:2007 zavedena v ČSN EN ISO 24014-1:2007 (01 8240) Interoperabilní systém managementu jízdného – Část 1: Architektura

ISO/TR 24014-2 nezavedena

1 Předmět normy

Tato technická zpráva nejprve popisuje cíle a požadavky na multiaplikační řízení, jež jsou kompatibilní s druhy aplikací, popsanými v případech užití v ISO 24014-1, které vyžadují vysokou úroveň bezpečnosti a v multiaplikačním kontextu musí být bezpečně ochráněny před jinými aplikacemi

3 Termíny a definice

Pro účely tohoto dokumentu byly použity termíny a definice z ISO 24014-1, ISO/TR 24014-2

Kapitola obsahuje 6 termínů a definic souvisejících s touto normou.

médium (media)

zařízení obsahující nejméně jeden zabezpečený prvek

uživatelská média (Customer Media)

zařízení obsahující zabezpečený prvek inicializovaný s jednou nebo více aplikacemi

zabezpečený prvek (Secure Element) SE

fyzický prvek jakéhokoliv provedení (zabudovaný, ne/přenosný), který lze nainstalovat do média, aby mohly být aplikace spuštěny v zabezpečeném prostředí

specifikace zabezpečeného prvku (SE) (SE Specification)

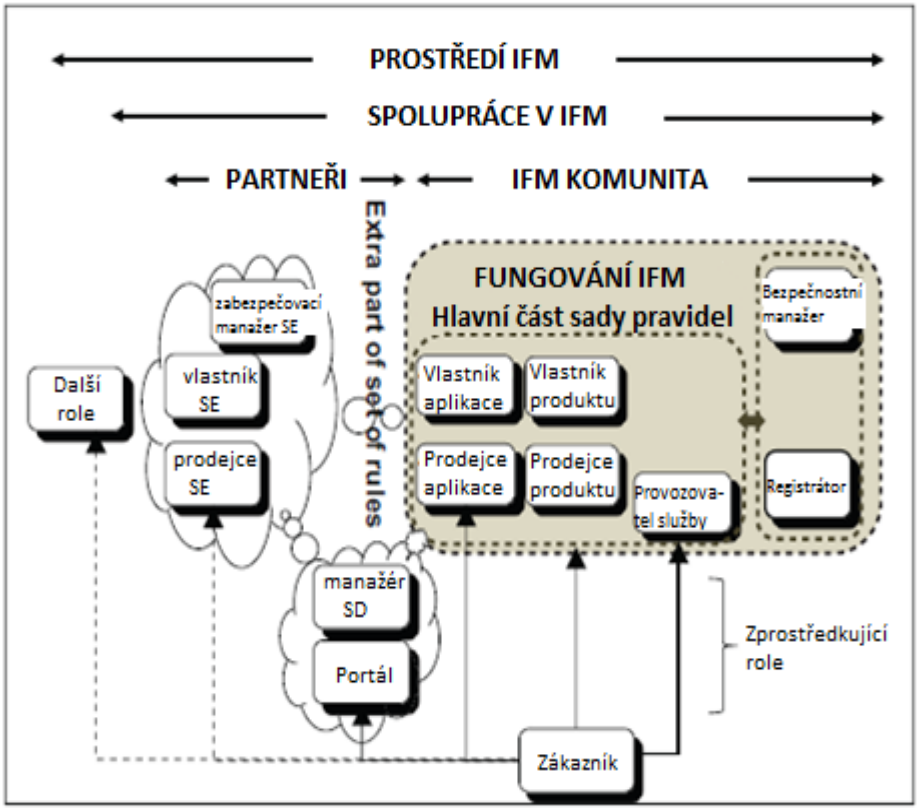
sada specifikací pro instalaci, výběr, chod a smazání aplikací v zabezpečeném prvku

zabezpečený kanál (Secure Channel)

mechanismus pro komunikaci z jakéhokoliv zdroje do zabezpečeného prvku, který poskytuje požadovanou úroveň zabezpečení

zabezpečená doména (Security Domain) SD

softwarová jednotka, která slouží ke kontrole, k zabezpečení a zadání požadavků na sdělení určitou rolí, např. prodejcem aplikace



Obrázek 1 – Hlavní termíny a definice zobrazené ve funkčním modelu

4 Značky a zkratky termínů

GP globální platforma *(GlobalPlatform)*

IFM interoperabilní management jízdného *(Interoperable Fare Management)*

IFMS interoperabilní systém managementu jízdného *(Interoperable Fare Management System)*

NFC bezdrátová komunikace (viz ISO/IEC 18092) *(Near Field Communication (refer to ISO/IEC 18092))*

PT veřejná doprava *(Public Transport)*

PTA dopravní úřad *(Public Transport Authority)*

PTO provozovatel veřejné dopravy *(Public Transport Operator)*

SCP protokol zabezpečeného kanálu *(Secure Channel Protocol)*

SE zabezpečený prvek *(Secure Element)*

SD zabezpečená doména *(Security Domain)*

POZNÁMKA V této technické zprávě může být použit i obvyklý termín „SD karta“, v tom případě se jedná o konkrétní typ komponentu.

5 Obecný koncept a limity

Tato kapitola poskytuje úvodní informace, které vysvětlují možnosti multiaplikační media, která jsou obsahem této technické zprávy. Uvádí, že multiaplikační média otevřou nové možnosti pro samostatné zabezpečené aplikace interoperabilního systému managementu sběru jízdného (dále jen IFM), aby byly na jednom médiu nahrány a provozovány odděleně. To umožní spotřebiteli zajistit obchodní interoperabilitu s tím, že bude možné používat stejné médium v různých systémech sběru jízdného nezávisle na místních způsobech zpoplatnění a specifikacích systému bez potřeby společných obchodních zásad.

Bližší specifikace jsou uvedeny v kapitolách 6 a 7.

V obecném konceptu je definováno že, globální platforma je považována za jedinou známou otevřenou normu, která je v současnosti k dispozici a splňuje zde definované cíle a požadavky. Z tohoto důvodu byla navržena jako aktuální řešení normalizačního procesu. Interní bezpečnostní procesy aplikací nadále zůstávají závislé pouze na jejich bezpečnostních koncepcích. Existují rovněž patentované materiály a metody, jež je možno zvolit pro vypořádání se s lokálními potřebami zpětné kompatibility, jakožto obchodní alternativu či odpověď na specifickou poptávku spotřebitelů, a to navzdory nejistotě ohledně aktualizací. Jiné typy architektur, založené především na přímých platbách či systémech soustředěných okolo back-office, využívajících médií pro ID management, mají odlišné potřeby a nejsou předmětem této technické zprávy.

Technická zpráva poté popisuje rozšíření funkčního modelu z ISO 24014-1 takovým způsobem, aby byl schopen zohlednit další role, nezbytné k provozu aplikací v novém kontextu, nezávisle na faktoru formy médií či na jeho zabezpečovacím prvku toto je blíže popsáno v kapitole 8.

Podrobnosti o využití multiaplikací v jednotlivých podobách mobilního odbavování prostřednictvím uzavřených dohod o partnerství, které mohou být mezi provozovateli mobilních sítí a provozovateli dopravních systémů vyžadovány, nejsou popsány v této technické zprávě, také se tato zpráva nezabývá finančními procesy souvisejícími se systémy správy jízdného.

Nejsou zde popsány způsoby, kterým systémy správy jízdného přistupuje k různým způsobům plateb, např. prostřednictvím kreditních nebo debetních karet, debetních účtů, věrnostních programů, bankovních převodů či jakýchkoli účtů s řízeným přístupem.

Rovněž nejsou popsány způsoby, kterými mohou sloužit jednotlivým provozovatelům služeb prostřednictvím zúčtovacích institucí.

Případy užití, uvedené v závěru této technické zprávy, se omezují na ty případy, kdy za instalaci a aktualizaci sady aplikací, instalovaných na multiaplikační média v souladu s poptávkou objednavatele, nese odpovědnost organizace, která s tímto objednavatelem není totožná.

O případech užití, které povolují správu médií ve vlastní režii, je pojednání v kapitole 9.

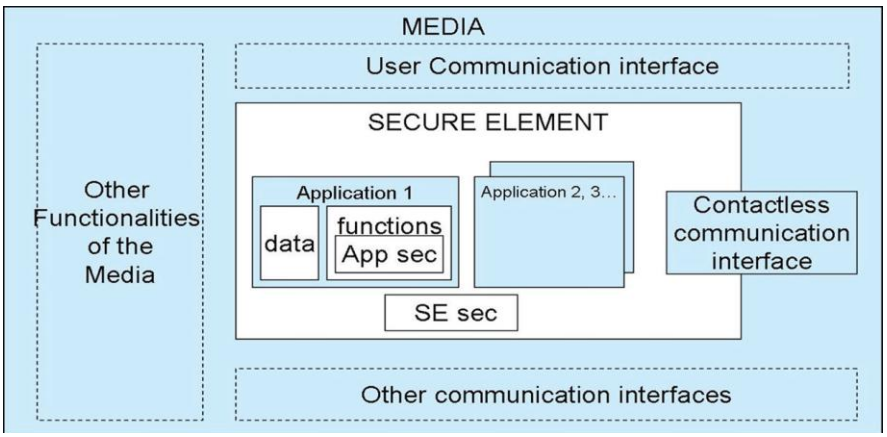
6 Média

6.1 Multiaplikace

V kontextu této technické zprávy jsou definovány pro toto prostředí jako zabezpečovací prvek (SE) s následujícími charakteristikami, definovanými v normě ISO/IEC 7816-13 pro karty.

6.2 Funkční model média

Funkční architektura média obsaženého v této technické zprávě je zobrazena na obrázku níže. Médium je vybaveno komunikačními rozhraními a používá různé protokoly a komunikační sítě: USB, 3G/GSM mobilní sítě, Bluetooth, eSATA. Funkční architektura je v této kapitole dále blíže uvedena.



Obrázek 2 – Funkční architektura média

7 Požadavky veřejné dopravy na multiaplikační uživatelská média

7.1 Obchodní požadavky

Tato kapitola navrhuje řešení, která nevyžadují zásadní změny stávajících systémů IFM.

Týká se druhů aplikací, popsaných v ISO 24014-1.

Multiaplikační média proto musí, bez ohledu na jejich formu, aplikaci umožnit, aby komunikovala jako běžná čipová karta

- alespoň při prezentaci u bezkontaktní čtečky v dopravě, například u průchodu validační branou,
- volitelně při využití jiných komunikačních kanálů.

Média musí v bezkontaktním režimu podporovat komunikaci na krátkou vzdálenost bez ohledu na ostatní rozhraní, která závisejí na jejich formě.

7.1.2 Bezpečnost

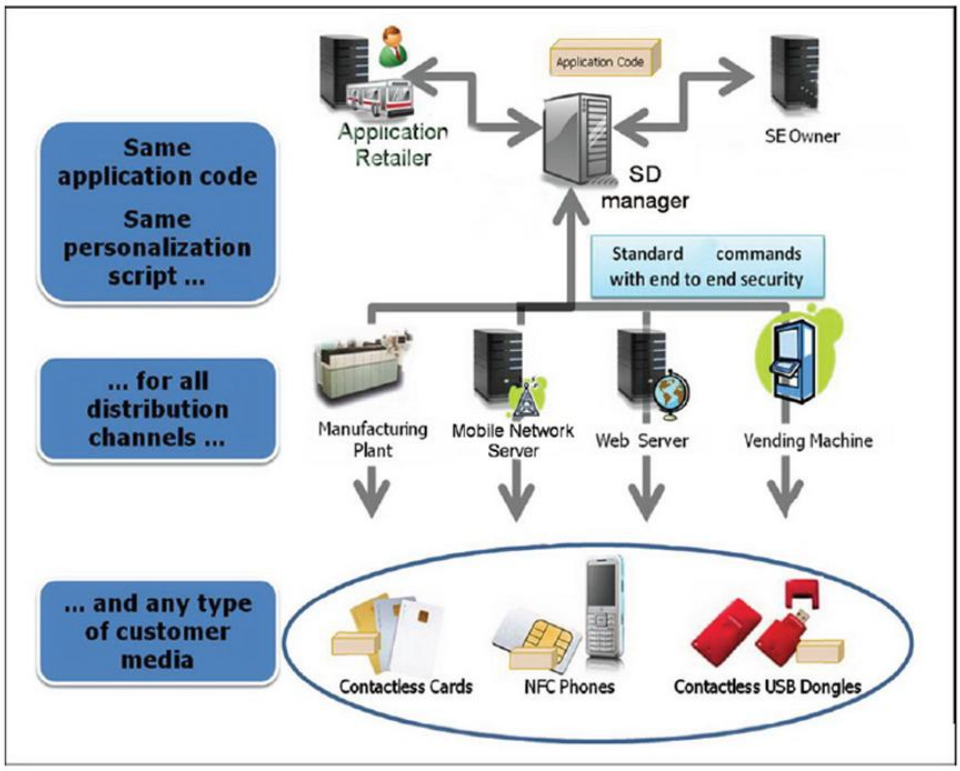
Zvažované aplikace IFM vyžadují vysokou úroveň zabezpečení a rovněž jejich správa musí v multiaplikačním kontextu probíhat bezpečně.

7.1.3.1 Univerzálnost komunikačních vrstev

Pro naplnění univerzálnosti médií je potřeba naplnit očekávané požadavky na komunikační vrstvy a je potřeba umožnit přístup bezkontaktním kartám IFM i platebním médiím přes mobilní telefon.

7.1.3.2 Správa aplikací

Multiaplikační model musí být otevřený pro všechny druhy médií a schopný nahrát, obnovit a smazat aplikace médií.



Obrázek 3 – Univerzálnost použití aplikačního managementu

Na obrázku 3 je ilustrována skutečnost, že téhož procesu se používá k zacházení s aplikacemi bez ohledu na komunikační kanál

7.2 Všeobecné požadavky na funkčnost

V této podkapitole se uvádějí požadavky, které se vztahují na média a zabezpečovací prvek, uvažované společně jako jediné zařízení bez ohledu na to, zda jsou požadované funkce implementované uvnitř zabezpečovacího prvku či nikoli

7.3 Bezpečnostní prvky

4 doporučení popisují vlastnosti bezpečnostních prvků,

7.5 Unikátnost

7.5.1 Obecné

Unikátnost vyžaduje standardní procesy a protokoly pro:

- kontaktní a bezkontaktní rozhraní;

- správu aplikací;

- výběr aplikací;

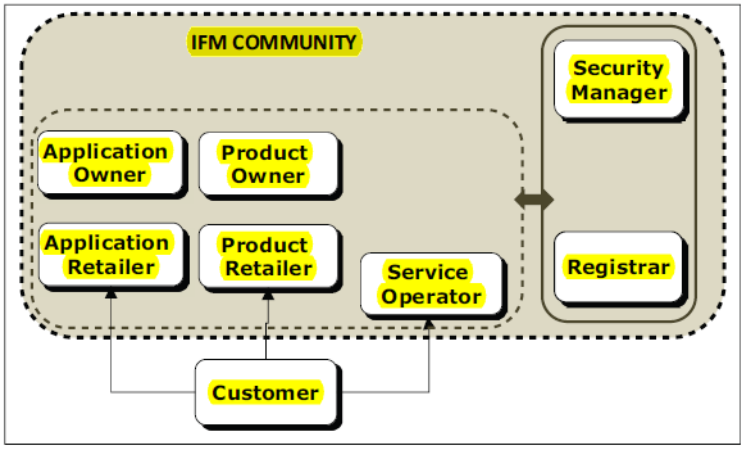
- provoz aplikací.

Dopravci veřejné dopravy, kteří mají proprietární technologie si musejí být vědomi toho, že tento způsob může být překážkou interoperability s jinými systémy IFM nebo s jinými dopravci.

8 Zasazení funkčního modelu IFM do multiaplikačního kontextu

8.1 Obecně

Základní funkční model v rámci komunity IFM, popsaný v ISO 24014-1, lze načrtnout jako na obrázku níže



Obrázek 4 – Základní funkční model v komunitě IFM

Pro zvážení možností implementace funkčního modelu ISO/TR 24014-2 zavádí koncepty partnerů IFM v podobě rolí, které nepodléhají koncepci IFM, ale přímo souvisí komunitou IFM a tudíž s ní sdílejí dodatečný soubor pravidel.

Provozování multiaplikačních zařízení, popsaných v předchozích kapitolách, umožnilo vznik funkčního modelu, popsaného v kapitole praxe při multiaplikacích.
Role, které spravují životní cyklus médií, se nedostávají do přímé interakce s komunitou IFM, nejsou tedy partnery IFM. Jejich popis lze nalézt v kapitole 8.2.
Role, které spravují životní cyklus zabezpečovacích prvků, se do přímé interakce dostávají a jsou tedy partnery IFM. Jejich popis lze nalézt v odstavci 8.3.
O aplikace uvnitř zabezpečovacích prvků (SE) se starají „zprostředkující role“ mezi komunitou IFM a komunitou SE. Jejich popis lze nalézt v odstavci 8.4.
Pro ilustraci multiaplikačního kontextu samotné veřejné dopravy jsou ukázány různé komunity IFM.
Podniky mimo oblast dopravy mohou mít na partnery IFM podobné vazby a nejsou zde zastoupeny.
Podobně několik tečkovaných linií okolo komunity SE (Bezpečnostní manager SE, Vlastník SE, Prodejce SE) znázorňují skutečnost, že lze využívat nejen jediný, ale vícero zabezpečovacích prvků.
Příčné role mohou být u všech dvojic [IFM a SE] odděleny.

9 Případové studie

Kapitola popisuje pouze nové případy užití, vzniklé díky procesům stahování aplikací a díky novým možnostem přístupu k aplikacím prostřednictvím jiných komunikačních kanálů, než je bezkontaktní přenos na krátkou vzdálenost.
Podmínky využívání portálů či prodejen s aplikacemi nebo možnosti zákazníků zvolit konkrétní aplikaci nejsou zmiňovány, neboť závisí na jednotlivých implementacích či zařízeních.

10 Praxe při implementaci multiaplikací

Tato kapitola přináší několik praktických příkladů a doporučení pro využívání multiaplikačního prostředí.
Využívání multiaplikačních zařízení lze považovat nejen za ekonomickou příležitost, jak se vyhnout správě výhradně dopravních médií a jak prosadit interoperabilní média pro zákazníky, která budou spolupracovat s různými tarifními systémy.
Také se může jednat o příležitost, jak zvýšit součinnost mezi stávajícími IFM v dané oblasti sledováním migračních tras, jak uvádí ISO/TR 24014-2.