Základní technické parametry systémů pro elektronické odbavení cestujících ve veřejné dopravě v ČR

Tento dokument byl zpracován v návaznosti na nařízení vlády č. 295/2010 Sb. o stanovení požadavků a postupů pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících (EOC) účinném od 1.11.2010 a na poziční dokument SDT k problematice „Rozvoje elektronických odbavovacích systémů pro cestující ve veřejné dopravě v ČR" ze dne 4.11.2010.

Cílem dokumentu je definovat základní technické parametry elektronického odbavení cestujících ve veřejné dopravě (dále jen ZTP EOC) nutné pro zajištění vzájemné interoperability dílčích systémů a doporučit minimální požadavky na systémy EOC, technické nosiče dat a zařízení pro odbavení cestujících. Navrhované ZTP mají omezenou platnost do okamžiku, kdy bude vytvořen a vstoupí v platnost národní „Standard EOC". Vznik Standardu požaduje poziční dokument SDT. Základní technické parametry elektronického odbavení cestujících ve veřejné dopravě navržení v tomto dokumentu jsou ve shodě s mezinárodními normami ISO 14443 a EN ISO 24014. Pro naplnění stanovených cílů ZTP EOC je nezbytné definovat požadavky v těchto oblastech:

a) požadavky na technický nosič dat (dále jen TND),

b) požadavky na datovou struktury TND,

c) požadavky na bezkontaktní terminály a prvky Security Access Module (dále jen SAM),

d) požadavky na generování, správu a ochranu kryptografických klíčů TND a dalších zařízení systému,

e) bezpečnost,
bezpečnostní politika a zajištění bezpečnosti systému TND včetně procesů a organizace systému pro řízení bezpečnosti (ISMS) v souladu s normou ISO/IEC 27001 a 27002).

Výklad pojmů

Bezpečné úložiště je zařízení splňující jednu z podmínek:

a) kritéria FIPS 140-1 - Level 3 nebo FIPS 140-2 - Level 3 nebo vyšší,

b) kritéria ISO/IEC 15408 (Common Criteria) EAL 4+ nebo vyšší,

c) kryptografický prostředek certifikovaný NBÚ podle zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění.

Citlivá operace je operace, která provádí změnu systémovou, bezpečnostní, personální a finanční na technickém nosiči dat (např. manipulace s datovou strukturou technického nosiče dat, změna bezpečnostního nastavení, změna osobních údajů, nabití elektronické peněženky).

Digitální podpis slouží k verifikaci zapsaných dat na technickém nosiči dat (TND).

Hardware Security Module (HSM) je bezpečnostní modul sloužící pro bezpečné uložení kryptografických klíčů v centrálním systému.

Information and Communications Technology (ICT) představuje technologie, nástroje a postupy, které lidé používají ke sběru, distribuci a sdílení informací a ke komunikaci mezi sebou prostřednictvím počítačů propojených počítačovými sítěmi.

Integrovaná dopravní aplikace (IDA) je aplikace sloužící k odbavování cestujících uložená na TND v souladu s definovanou datovou strukturou.

Integrovaný dopravní systém (IDS) – jedná se o dopravní systém zajišťující vzájemně propojené dopravní služby ve vymezené územní oblasti s jednotnou informační službou, systémem jízdného a jízdním řádem.

Secure Access Module (SAM) je modul určený pro potřeby bezpečného úložiště klíčů a provádění kryptografických operací, který je umístěn v akceptačním zařízení.

Standard elektronického odbavení cestujících ve veřejné dopravě (Standard EOC) je standard, který definuje podmínky interoperability odbavovacích systémů v národním prostředí. Standard EOC pro ČR dosud neexistuje, vznik tohoto standardu a jeho účinnost požaduje SDT.

Technický nosič dat (TND) je datový nosič (např. bezkontaktní čipová karta nebo zařízení s rozhraním NFC – Near Field Communication) obsahující informace pro odbavení cestujících.

Unique Identifier String (UID) je řetězec znaků, které globálně, jednoznačně a časově nezávisle identifikují objekty.

Základní technické parametry elektronického odbavení cestujících ve veřejné dopravě (ZTP EOC) je technická specifikace minimálních požadavků na EOC ve veřejné dopravě. Definice ZTP EOC je obsahem tohoto dokumentu.

Požadavky na technický nosič dat (TND)

ZTP EOC uvádí pro technický nosič dat (TND) následující požadavky:

a) komunikace musí být řešena ve shodě s ISO 14443 A definující bezkontaktní interface, čímž výsledné řešení zajistí technologickou interoperabilitu plošně všem uživatelům,

b) operační systém TND musí oddělit ve své paměti několik datových prostorů tak, aby TND umožňoval práci s nezávislými aplikacemi,

c) pokud to umožňuje TND, musí být přístup k odděleným datovým prostorům řízen podle typu operací. Typem operace se rozumí přesně popsané operace s TND popsané v normě ISO 14443 A.

d) operační systém a autentizační mechanismy TND musí být nastaveny tak, aby umožňovaly jednomu subjektu v rámci obslužného SW vykonávat správu obsahu TND bez možnosti přístupu k datům a klíčům uvnitř jednotlivých aplikací, tj. nahrávat dopravní aplikace jejich správu i vymazání takovým způsobem, že neoprávněné subjekty nejsou schopny zjistit ani ovlivnit jejich obsah,

e) TND musí nabízet vlastní nativní bezpečnostní prvky - šifrování komunikace a řízení přístupu pomocí kryptografických klíčů,

f) TND musí umožnit zavedení dodatečné bezpečnostní vrstvy pomocí prostředků, které jsou na nativních bezpečnostních mechanismech TND nezávislé,

g) na provozních zařízeních pracujících s TND musí být možné obnovovat bezpečným způsobem kryptografické klíče použité pro ochrany TND a jejich aplikací (v některých případech lze očekávat, že systém EOC toto umožní za podmínky vykonávání těchto operací v prostředí s definovanými bezpečnostními parametry),

h) musí být možné bezpečným způsobem zapisovat na TND nové aplikace, popř. je vymazávat nebo jiným způsobem odstranit (v některých případech lze očekávat, že systém EOC toto umožní za podmínky vykonávání těchto operací v prostředí s definovanými bezpečnostními parametry),

i) doporučuje se, aby TND měla bezpečnostní certifikaci podle ISO/IEC 15408 (Common Criteria) EAL 4+ nebo vyšší. Datové struktury musí být zpracované na základě standardu pro běžně používané technologie.

Požadavky na datovou struktury TND

Pro zajištění interoperability užití TND v systémech EOC musí datová struktura TND obsahovat:

a) integrovanou dopravní aplikaci (IDA),

b) platební aplikaci.

Datová struktura jednotné IDA na TND musí vzájemně akceptovat jednotné jízdní doklady uložené v IDA TND.

Požadavky na bezkontaktní terminály a prvky SAM

Rozhraní čtecích terminálů dle ZTP EOC musí být řešeno ve shodě s ISO 14443 A definující bezkontaktní interface. Bude-li použita technologie NFC, musí být čtecí terminály v souladu se standardem ISO 18092:2004. Terminály musí umožnit použití alespoň dvou modulů SAM. Minimální funkční požadavky na SAM jsou tyto:

a) **Správa SAM**:

   i. všechny SAM moduly musí být centrálně evidované a spravované (správu SAM zpravidla zajišťuje a evidenci zadává/řídí objednatel dopravy),

   ii. musí poskytnout všem subjektům informaci o stavu tohoto modulu (stav aktivace, inicializován, v provozu, dočasně zablokován, trvale zrušen, apod.),

   iii. každý SAM modul musí být jednoznačně označen identifikačním číslem UID, které bude snadno zjistitelné a nezměnitelné.

b) **Aktivace SAM** - po zapnutí je nutné u odbavovacího zařízení aktivovat SAM tak, aby pouze oprávněné zařízení nebo osoba mohla funkce SAM využívat. Pro stavy zařízení on-line a off-line jsou definovány tyto požadavky:

   i. On-line zařízení (nebo s možností krátkého připojení) – je preferována aktivace SAM pomocí centrálních HSM modulů nebo jiného bezpečného úložiště za předpokladu bezpečné komunikace.

   ii. Off-line zařízení – lze provádět aktivaci SAM pomocí centrálních HSM modulů nebo jiného bezpečného úložiště. V případě, že nejsou prováděny citlivé operace, je možné aktivovat SAM pouze na základě přihlášení obsluhy. Citlivou off-line operací je např. nabití TND, pro které by, v případě aktivace SAM přihlášením obsluhy, měla být stanovena zvláštní pravidla.

c) **Klíče pro citlivé operace** - klíče pro citlivé operace (rozumí se manipulace s datovou strukturou TND a bezpečnostní nastavení) nesmí být trvale uloženy v paměti akceptačního

zařízení nebo SAM. Klíče pro citlivé operace jsou zejména master klíč aplikací a master klíč TND, případně také další dle předmětné bezpečnostní politiky provozovatele systému EOC.

d) **Utajení komunikace** - Komunikace mezi HSM a sítí akceptačních zařízení s moduly SAM musí být šifrovaná, protože se v ní budou přenášet citlivá data. Šifrování je požadováno minimálně na síťové úrovni (VPN, SSL) mezi serverem s HSM a čtecí terminál, preferuje se ovšem end to end aplikační šifrování mezi HSM a SAM.

e) **Upgrade aplikace a klíčů** - systém EOC musí umožnit bezpečné předání nových klíčů i aplikačních kódů do paměti SAM modulů. Je požadováno využití HSM nebo jiného bezpečného úložiště.

Požadavky na generování, správu a ochranu kryptografických klíčů

ZTP EOC kromě využití nativních bezpečnostních prvků TND (přístup k datům TND se autorizuje kryptografickým klíčem, komunikace s kartou je zašifrovaná atd.) vyžadují využití další aplikační bezpečnostní vrstvy nezávislé na technologii TND:

a) pro zajištění integrity citlivých dat a principu nepopiratelnosti se vyžaduje digitální podpis,

b) pro utajení zvláště citlivých dat (např. osobní údaje) se vyžaduje dodatečné šifrování pomocí asymetrické kryptografie (preferovány eliptické křivky).

Technicko-bezpečnostním jádrem systému musí být HSM moduly, SAM moduly a jejich spolupráce. SAM moduly v terminálech a čtečkách musí sloužit jako úložiště klíčů k jednotlivým aplikacím. Jejich nahrání do SAM musí být zajištěno prostřednictvím zabezpečené komunikace s HSM. Pro SAM moduly se doporučuje použití flexibilních čipů s operačním systémem v souladu s obecně rozšířenými a používanými standardy GlobalPlatform a JavaCard, které umožňují v bezpečném prostředí čipu uchovávat data, klíče i aplikační kódy.

Bezpečnostní infrastruktura musí uchovávat kryptografické klíče v bezpečnostních modulech HSM. Systém EOC by měl upravovat:

a) požadavky na HSM (např. certifikace, stupeň bezpečnosti),

b) rozdělení kompetencí HSM (např. provozní, root, personalizační),

c) požadavky na použití HSM jiných subjektů (jako úložiště hesel).

Požadavky na systémy EOC

Základem systému EOC v rámci IDS musí být infrastruktura, ve které se shromažďují informace o veškerých uskutečněných transakcích. Komunikace s okolními systémy musí probíhat zabezpečeně pomocí kryptografie tak, aby byla zaručena důvěryhodnost, integrita a nepopiratelnost přenášených dat. Sběr a správa transakcí musí zabezpečit evidenci všech dopravních transakcí od jednotlivých držitelů TND respektive poskytovatelů hromadné dopravy. Technické požadavky na systém EOC jsou následující:

a. systém EOC musí být přizpůsobitelný možným změnám rozsahu sítě a to dočasným i trvalým. (např. vznik/zánik dopravce, vznik nových tarifů, vznik nových dopravních linek),

b. veškerá citlivá datová komunikace mezi prvky systému EOC musí probíhat šifrovaně,

c. každá dopravní transakce musí být jednoznačně přiřazena právě jednomu TND a o každé operaci musí existovat auditovatelný záznam,

d. systém správy TND musí být schopen generovat pravidelné i ad-hoc seznamy blokovaných karet a případně SAM modulů,

e. v systému musí TND umožňovat multifunkční použití, tj. souběžné umístění, užívání a správu aplikací různých subjektů,

f. systém EOC musí umožnit exportování transakčních historií pro jednotlivé dopravce ve stanoveném časovém rozsahu,

g. veškeré transakce a události (definované předmětnou bezpečnostní politikou) musí být logovány a archivovány pro potřeby auditu,

h. systém EOC musí umožňovat souběh více technologií odbavení u jediného dopravce.

Z hlediska interoperability jsou základní bezpečnostní požadavky na systém správy TND tyto:

a. bezpečná komunikace - komunikace, která musí probíhat mezi jednotlivými subsystémy systému správy TND a komunikace s okolními systémy musí být realizována zabezpečeným kanálem.

b. autentizace - proces ověření (prokázání) identity vzdáleného prvku systému či subsystému při požadavku na využití TND, SAM a HSM,

c. autorizace - proces řízení přístupových oprávnění k aplikačním zdrojům po úspěšném ověření identity (autentizaci),

d. monitorování a audit - uživatel/systém pohybující se v systému správy TND musí být na základě definovaných operací monitorován a následně auditován.

Odkazy

Nařízením vlády č. 295/2010, požadavky a postupy pro zajištění propojitelnosti elektronických systémů plateb a odbavení cestujících;

Rozvoj elektronických odbavovacích systémů pro cestující ve veřejné dopravě v ČR. Poziční dokument Sdružení pro dopravní telematiku ze dne 4.11.2010.

ČSN ISO/IEC 14443, Identifikační karty, Bezkontaktní karty s integrovanými obvody, Karty s vazbou na blízko;

ČSN EN ISO 24014, Interoperabilní systém managementu jízdného;

ISO/IEC 27001, Systém řízení bezpečnosti informací – ISMS, Požadavky;

ISO/IEC 27002, Systém řízení bezpečnosti informací – ISMS, Soubor postupů pro řízení informační bezpečnosti;

NIST FIPS 140-1, Standard pro hodnocení bezpečnosti kryptografických modulů;

NIST FIPS 140-2, Standard pro hodnocení bezpečnosti kryptografických modulů, aktualizace verze 140-1;

ČSN ISO/IEC 15408, Bezpečnostní techniky, Kritéria pro hodnocení bezpečnosti IT;

ČSN ETSI EN 302 190 V1.1.1 (ISO/IEC 18092:2004), Komunikace v blízkém poli - Rozhraní a protokol (NFCIP-1);

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších změn.

V Praze dne 14.12.2010
Sdružení pro dopravní telematiku, Bartolomějská 11 (Konviktská 24), 110 00 Praha 1
www.sdt.cz.