CEN TS 16439 - **Electronic fee collection – Security framework**

Application Area: Electronic Fee Collection (EFC)

Publication Year, Number of Pages: Published 2014, 141 pages

Zavedení normy do ČSN: převzetím originálu

Extract Creation Year: 2014

Introduction

Elektronické mýtné systémy se skládají z několika subjektů, které si mezi sebou elektronicky předávají informace. Pro správnou funkci takového systému je nutné zajistit, že předávaná data nemohou být nikým narušena, podvržena nebo zcizena. Vzájemná důvěra mezi subjekty je postavena na přijetí a dodržování bezpečnostních pravidel komunikace.

Poznámka: Extrakt přejímá původní číslování kapitol

Application

Technická specifikace CEN/TS 16439 analyzuje možné útoky na elektronický mýtný systém a definuje bezpečnostní opatření a požadavky na jednotlivé komponenty, které omezí rizika plynoucí z použité elektronické komunikace. Je primárně určena **pro odborníky navrhující mýtné systémy** (systémové architekty), ale díky podrobné analýze možných útoků může být cenným materiálem i pro **pracovníky státní správy** hodnotící rizika spojená s elektronickými mýtnými systémy.

1. Scope

Technická specifikace CEN/TS 16439 **popisuje** následující aspekty bezpečnosti v systémech elektronického mýta: obecné informace o cílech bezpečnosti zainteresovaných stran, analýza bezpečnostních hrozeb, definice modelu vzájemné důvěry, bezpečnostní požadavky, bezpečnostní opatření a protiopatření, specifikace bezpečného rozhraní, správa klíčů, bezpečnostní pravidla, ochrana osobních údajů.

Popisovaná technická specifikace **se nezabývá** analýzou rizik kompletního systému elektronického mýta, bezpečnostními riziky aplikací běžících na OBU ve vozidlech, rozhraním subjektu správce interoperability, technickými opatřeními zajišťujícími důvěru mezi poskytovatelem mýtné služby a uživatelem, kompletním popisem všech potřebných bezpečnostních opatření řešících všechny popsané hrozby, konkrétním popisem implementace bezpečnostních opatření pro konkrétní systém, např. EETS, detailním popisem ochrany osobních údajů.

2. Associated Standards

Norma souvisí s širokým spektrem norem pro EFC, např. EN 15509, ISO 17573, CEN ISO/TS 17575-1, CEN ISO/TS 12813, CEN ISO/TS 13141 a EN ISO 12855, dále s normami souvisejícími s bezpečnostními technikami jako ISO/IEC 9797-1, ISO/IEC 10118-3, ISO/IEC 11770-1, ISO/IEC 14888-2, ISO/IEC 18033-2, ISO/IEC 19790, poslední skupinou souvisejících dokumentů jsou RFC (Request for Comments) vydávané Komisí techniky Internetu (IETF) např. RFC4301, RFC4347, RFC4648, RFC5035, RFC5246, RFC5280, RFC5746.

3. Terms and Definitions

Tato technická specifikace definuje 55 termínů, například:

majetek *(asset)*
cokoliv, co má pro zainteresovaný subjekt v rámci EFC systému nějakou hodnotu

útok *(attack)*
pokus o zničení, odhalení, změnu, zablokování, zcizení, získání neautorizovaného přístupu nebo zneužití majetku

zabezpečení informací *(information security)*
zachování tajnosti, integrity a dostupnosti informací

mimořádná bezpečnostní událost *(information security incident)*
jednotlivý případ nebo série případů nechtěných nebo neočekávaných událostí, které s významnou pravděpodobností kompromitují provoz společnosti nebo ohrožují zabezpečení informací

integrita *(integrity)*
neporušenost a kompletnost dat

zranitelnost *(vulnerability)*
slabina daného majetku nebo procesu, která může být využita k jejímu ohrožení

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

4. Abbreviations

Tato technická specifikace definuje 49 zkratek, například:

ISMS Systém- řízení bezpečnosti informací *(Information Security management system)*

PKI- Infrastruktura pro správu a distribuci veřejných klíčů *(Public Key Infrastructure)*

TTP- Důvěryhodná třetí strana *(Trusted Third Party)*

Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology (www.ITSterminology.org).

5 Model vzájemné důvěry

Tato kapitola popisuje možnosti navázání vzájemné důvěry mezi subjekty zastávajícími v rámci EFC role výběrčího, poskytovatele mýtné služby, uživatele a subjektu pro správu interoperability. Vysvětluje, které z těchto subjektů musí používat bezpečné komunikační kanály a jak tyto komunikační kanály vytvořit pomocí veřejných certifikátů podle ISO/IEC 9594-8 (X.509). Popisuje rozdíly mezi hierarchickými důvěryhodnými certifikáty, kde důvěra vychází z centrální certifikační autority, a navázáním důvěry způsobem "každý s každým".

Dále jsou zde popsány doporučené způsoby odvolávání certifikátů, nastavování doby jejich platnosti a doporučené použití několika různých privátních klíčů pro různé účely.

6 Požadavky na zabezpečení

Tato kapitola obsahuje základní sadu bezpečnostních požadavků, které by měly ochránit data v EFC systému. Požadavky vycházejí z analýzy hrozeb EFC systému, která je uvedena v příloze D. Požadavky jsou seskupeny do tzv. profilů, které jsou závazné pro splnění daného profilu.

Kapitola je tématicky rozdělena na podčásti, které popisují požadavky na zabezpečení a příslušné profily pro konkrétní komponenty EFC systému. Jedná se například o komunikační rozhraní, uchovávání dat, systém výběrčího, systém poskytovatele mýtné služby, uživatele a správce interoperability. Příklad požadavků pro obecné rozhraní je uveden v tabulce 1.

Tabulka 1 — Požadavky na obecné rozhraní (tabulka 3 normy)

Číslo	Požadavek
RQ.IF.01	Výměna dat se provádí pomocí ověřeného komunikačního kanálu, který zajistí integritu dat, důvěrnost a nepopir (doklad o původu a doručení).
RQ.IF.02	Výměna dat se provádí pomocí spolehlivého (dostupného) přenosového kanálu.
RQ.IF.10	Výměna dat zajistí důvěrnost údajů.
RQ.IF.11	Výměna dat zajistí integritu dat.
RQ.IF.12	Výměna dat zaručí autenticitu dat původce.
RQ.IF.13	Výměna dat zaručí nepopiratelnost s dokladem o původu.

RQ.IF.14	Výměna dat zaručí nepopiratelnost s dokladem o doručení.
RQ.IF.20	Výměna dat se provádí pouze mezi ověřenými subjekty.
RQ.IF.21	Výměna dat se provádí pomocí ověřeného kanálu, který zajistí integritu dat a důvěrnost.
RQ.IF.30	Výměna dat musí umožňovat detekci znovu zaslaných zpráv (ochrana proti "replay atacks").

Dále tato kapitola popisuje rizika ze kterých vychází požadavky na bezpečnost. Níže je uveden příklad hodnocení rizik DSRC profilu a navržených protiopatřeních:

- Transakce pro navýšení finančního zůstatku OBE obdržená prostřednictvím RSE obsahuje všechny povinné informace požadavku o platbu (payment claim). Přečtení dat z OBE falešným RSE je možné bez předchozího upozornění uživatele. Proto je vyžadována autentizace RSE.
- Manipulace s těmito údaji a/nebo přehrávání zaznamenané komunikace z falešného OBE je v zásadě jednoduchá, i když technicky náročná. Proto je vyžadována autentizace OBE i RSE. Je také požadován doklad o integritě zprávy.
- Uživatel může zapřít použití určitého silničního úseku (účtování nebo CCC). K tomu může využít falešnou LAC zprávu, kterou potvrdí, že daným úsekem neprojel. Podvržení nebo zapření dat bez ochrany je jednoduché. Proto je nutné použít zabezpečení s nepopiratelností a dokladem o původu.
- Odposlech komunikace je technicky obtížný, protože vyžaduje přítomnost v těsné blízkosti OBE nebo RSE, přitom útočník nezíská nové informace o uživateli, vozidlu nebo RSE, které by nešly získat i jinak. Zabezpečení proto není nutné.

Z výše uvedených hodnocení rizik a navržených protiopatřeních vychází povinné a doporučované požadavky profilu, které přímo zmiňují navržené požadavky z tabulky 3:

Povinné RQ.IF.11 + RQ.IF.12 + RQ.IF.13 + RQ.IF.30

Doporučené (žádné)

7 Bezpečnostní opatření a protiopatření

Tato kapitola popisuje doporučená bezpečnostní opatření a protiopatření na základě bezpečnostních požadavků popsaných v kapitole 6. Příklad zápisu je uveden v tabulce 12.

Tabulka 2 — Požadavky na obecné rozhraní (tabulka 12 normy)

Číslo	Bezpečnostní opatření	Splňuj požada
SM210	RSE si vyžádá od OBE výpočet zabezpečení zprávy pomocí DSRC autentizačního kódu zprávy pro výběrčího (MAC_TC) minimálně z položky PaymentMeans, pomocí klíče, který zná výběrčí a poskytovatel mýtné služby.	RQ.IF.11 RQ.IF.12 RQ.TSP.19

8 Specifikace zabezpečení interoperabilního rozhraní

Tato část obsahuje detailní technický popis zabezpečení, splňující bezpečnostní opatření definovaná v kapitole 7. Jsou zde popsány typy šifer, délky klíčů a formáty dat, většinou pomocí odkazu na příslušné normy. V případě, že odkazovaná norma připouští více možností, je zde specifikována konkrétní varianta.

9 Správa kryptografických klíčů

Tato kapitola definuje zásady pro skladování kryptografických klíčů a práci s nimi. Věnuje se nejen asymetrickému šifrování, ale také symetrickým šifrám používaným především u DSRC.

Příloha A (normativní) Specifikace datových typů

Příloha A definuje použité datové typy pomocí ASN.1.

Příloha B (normativní) Proforma prohlášení o shodě implementace (ICS)

Tato příloha obsahuje formulář Prohlášení o shodě implementace (ICS).

Příloha C (informativní) Cíle a obecné požadavky zainteresovaných stran

Informativní příloha C popisuje obecné požadavky a základní cíle subjektů tvořících EFC systém. Jsou zde popsány obecné požadavky jednotlivých skupin jako například:

Hlavní zájem uživatelů je 1) být ochráněni proti nesprávnému výběru poplatku, 2) všechny osobní údaje o uživateli, které mýtný systém uchovává, musí být chráněny proti neoprávněnému užití.

Příloha D (informativní) Analýza hrozeb

Tato příloha obsahuje velmi podrobnou analýzu možných hrozeb pro mýtný systém. Hrozby jsou rozděleny podle rozhraní/komponenty na kterou je útok směrován a podle efektu, který má útok přinést.

Příloha E (informativní) Bezpečností zásady

Příloha E definuje bezpečnostní zásady ve formě obecných principů, které lze převzít do vnitrofiremních nařízení.

Příklad:

EFC-PS-10 Nařízení informační bezpečnosti by měla být revidována v pravidelných intervalech nebo při výskytu události související s informační bezpečností.

Příloha F (informativní) Příklad bezpečnostních zásad pro EETS

Příloha F obsahuje příklad bezpečnostních zásad pro EETS. V této krátké příloze jsou uvedeny odkazy na bezpečnostní zásady z přílohy E s dodatkem konkrétních dokumentů, které dané bezpečnostní zásady v rámci EETS naplňují.

Příloha G (informativní) Požadavky na ochranu soukromí

Příloha G obsahuje základní principy návrhu EFC systému se zaměřením na ochranu soukromí. Jsou zde uvedeny konkrétní dokumenty, např. směrnice EU 95/46/EC, a zásady které z těchto dokumentů vyplývají.

Associated Terms

- vulnerability
- threat agent

- accountability
- HTTP over Secure socket
- HyperText Transfer Protocol
- XML Encoding Rules
- Advanced Encryption Standard
- non-repudiation
- toll system
- Wide Area Network
- processing of personal data
- Internet Protocol Security
- Virtual Private Network
- service user; user
- attack
- Rivest, Shamir and Adleman
- certificate revocation list
- interoperability management
- elliptic curve cryptography
- secure hash algorithm
- foreign power
- security measure (countermeasure)
- information security
- authenticity
- threat analysis
- activist
- Datagram Transport Layer Security
- enforcement
- impact
- Internet Engineering Task Force
- message authentication code
- Simple Mail Transfer Protocol
- hacker
- policy
- electronic fee collection
- trusted third party