EN ISO 19299 - **Elektronický výběr poplatků (EFC) – Bezpečnostní rámec**

Application Area: Electronic Fee Collection (EFC)

Publication Year, Number of Pages: Published 2020, 129 pages

Extract Creation Year: 2023

Standard Topic Group: Zabezpečení a kontrola

Standard Topic: Model důvěry

Topic Description: Metodické kroky k vytvoření důvěryhodného vztahu mezi jednotlivými entitami v rámci systému EFC

Introduction, Explanation of Starting Points

Description of Architecture, Hierarchies, Roles, and Object Relationships

Definice modelu důvěry mezi jednotlivými entitami mýtného systému.

Description of Process / Function / Method of Use

Specifikace metodiky vedoucí k vytvoření bezpečného modelu důvěry.

Description of Interfaces / APIs / System Structure

Specifikace požadavků týkající se bezpečnosti pro interoperabilní rozhraní.

Protocol / Algorithm / Computation Definition

Specifikace bezpečnostních profilů týkající se komunikace a uložení dat.

Definition of Data Representation / Physical Meaning

Definition of Constants / Ranges / Restrictions

Introduction

Tato technická norma (dále rovněž “popisovaný dokument”) definuje bezpečnostní rámec pro všechny organizační a technické jednotky architektury EFC a související rozhraní založené na sadě technických norem ISO 17573. Popisovaný dokument popisuje sadu bezpečnostních požadavků a souvisejících bezpečnostních opatření, dále identifikuje seznam potenciálních hrozeb pro systémy EFC a jejich možný vztah k definovaným bezpečnostním požadavkům.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Application

Popisovaný dokument definuje bezpečností rámec architektury EFC, a tudíž je určený pro všechny role, tj. výběrčího mýtného, poskytovatele mýtných služeb, výrobce zařízení na infrastruktuře i palubních zařízení. Bezpečnostní hrozby identifikované v popisovaném dokumentu lze použít pro definici příslušných bezpečnostních požadavků systému EFC, na jejichž základě je pak možné odvodit příslušná bezpečnostní opatření.

1. Scope

Popisovaný dokument popisuje:

- model důvěry mezi zúčastněnými stranami;
- bezpečnostní požadavky pro podporu implementací systému EFC;

- bezpečnostní opatření;
- bezpečnostní specifikace pro implementaci interoperabilního rozhraní;
- správu bezpečnostních klíčů;
- bezpečnostní profily;
- prohlášení o shodě implementace s popisovaným dokumentem;
- obecné cíle bezpečnosti informací zúčastněných stran;
- analýzu hrozeb na modelu systému EFC;
- příklady bezpečnostní politiky;
- doporučení pro implementace zaměřené na soukromí;

2. Associated Standards

Popisovaný dokument se odkazuje na 20 technických norem, jak z oblasti elektronického výběru poplatků, tak z oblasti informační technologie.

3. Terms and Definitions

Tato kapitola obsahuje 8 termínů a definic souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou:

certifikační autorita (certification authority) – subjekt důvěryhodný pro jeden nebo více subjektů za účelem přidělování a rušení certifikátů

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

4. Abbreviations

Tato kapitola obsahuje 39 zkratek souvisejících s popisovaným dokumentem, z nichž nejdůležitější jsou následující:

CA certifikační autorita (certification authority)

OBE palubní zařízení (on-board equipment)

RSE zařízení na infrastruktuře (roadside equipment)

TC výběrčí mýtného (toll charger)

TSP poskytovatel mýtných služeb (toll service provider)

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

5 Model důvěry

Tato kapitola v rozsahu 6 stránek definuje základní předpoklady a zásady pro nastolení důvěry mezi zúčastněnými stranami architektury EFC, tj. výběrčím mýtného, poskytovatelem mýtných služeb a managementem interoperability. Model důvěry je zde rozebrán na dvou úrovních, smluvní a technické.

6 Bezpečnostní požadavky

Tato kapitola v rozsahu 8 stránek uvádí funkční a nefunkční požadavky, které je nutné splnit pro eliminaci nebo zmírnění hrozeb na systém EFC. V tabulkové formě jsou zde uvedeny:

- požadavky na systém řízení bezpečnosti informací;
- požadavky na komunikační rozhraní;
- požadavky na uchovávání dat;

- požadavky pro ochranu prostředků výběrčího mýtného, poskytovatele mýtných služeb a managementu interoperability;

Pro ilustraci je níže uveden příklad požadavků na komunikační rozhraní.

No.	Requirement	DSRC	GNSS
RQ.IF.02	Data exchange shall be done using transmission channels with reliable availability.	X	X
RQ.IF.10	Data exchange shall guarantee data confidentiality.	X	X
RQ.IF.11	Data exchange shall guarantee data integrity.	X	X
RQ.IF.12	Data exchange shall guarantee the authenticity of the data originator.	X	X
RQ.IF.13	Data exchange shall guarantee non-repudiation with proof of origin.	X	X
RQ.IF.14	Data exchange shall guarantee non-repudiation with proof of delivery.	X	X
RQ.IF.20	Data exchange shall only be done between authenticated entities for the respective data exchange.	X	X
RQ.IF.30	Data exchange shall allow the detection of resent messages (protection against replay attacks).	X	X
RQ.IF.31	Data exchange shall allow the detection of mass rejection of toll declarations (protection against interface errors).	X	X
RQ.IF.32	Data exchange shall allow the detection of mass rejection of billing details (protection against interface errors).	X	X

Tabulka 1 – Požadavky na komunikační rozhraní (tab. 4 normy)

7 Bezpečnostní opatření

Tato kapitola v rozsahu 12 stránek uvádí soubor bezpečnostních opatření, které má adresovaný subjekt provést, aby splnil jeden nebo více požadavků definovaných v kapitole 6. V tabulkové formě jsou zde uvedena:

- obecná bezpečnostní opatření;
- bezpečnostní opatření pro komunikační rozhraní (konkrétně DSRC rozhraní, CCC rozhraní, LAC rozhraní, ICC rozhraní a rozhraní mezi back-office výběrčího mýtného a poskytovatele mýtných služeb);
- bezpečnostní opatření pro back-office výběrčího mýtného a poskytovatele mýtných služeb;

Pro ilustraci je níže uveden příklad opatření na DSRC rozhraní.

No.	Requirement	DSRC	GNSS
		Fulfilled RQ	
SM.210	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC message authentication code for TC (MAC_TC) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TC and the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TC.01 RQ.TSP.55 RQ.TSP.89	
SM.211	If toll declarations are acquired through the DSRC interface, the RSE shall request the OBE to calculate and provide a DSRC message authentication code for TSP (MAC_TSP) over at least the ISO 14906 attribute PaymentMeans using a key known only to the TSP during an EFC transaction. The OBE shall respond accordingly.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.04 RQ.TSP.89	
SM.212	The OBE shall implement an access control mechanism for an EFC command addressing its EFC data attributes. The RSE shall implement the calculation of the corresponding access codes.	X	n.a.
		RQ.IF.20 RQ.TC.22 RQ.TSP.05 RQ.TSP.07 RQ.TSP.40 RQ.TSP.41	
SM.213	The RSE shall read, increment and write a transaction counter to the OBE. The OBE shall support this.	X	n.a.
		RQ.TC.04 RQ.TC.05 RQ.TSP.21	
SM.214	The TSP shall implement a MAC_TSP authenticator in the OBE to prove its authenticity and integrity.	X	n.a.
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.03 RQ.TSP.04	
SM.215	The TSP shall implement a MAC_TC authenticator in the OBE to prove its authenticity and integrity.	X	X
		RQ.IF.11 RQ.IF.12 RQ.IF.13 RQ.TSP.62	

Tabulka 2 – Opatření pro DSRC rozhraní (tab. 13 normy)

8 Bezpečnostní specifikace pro implementaci rozhraní

Tato kapitola v rozsahu 1 stránky uvádí definice z dalších technických norem, které je nutné implementovat v rámci interoperabilního rozhraní, aby byly naplněny bezpečnostní opatření popisovaná v kapitole 8.

9 Správa klíčů

Tato kapitola v rozsahu 5 stránek rozebírá nastavení výměny klíčů mezi zúčastněnými stranami a několik provozních postupů, jako je vydání, uchovávání a zneplatnění klíče, a to pro symetrické a asymetrické klíče.

Příloha A (normativní) – Bezpečnostní profily

Příloha A v rozsahu 4 stránek definuje bezpečnostní profily pro komunikační rozhraní (DSRC rozhraní a rozhraní mezi back-office výběrčího mýtného a poskytovatele mýtných služeb) a bezpečnostní profily pro uchovávání dat (OBE, ICC, RSE).

Příloha B (normativní) – Prohlášení o shodě implementace

Příloha B v rozsahu 18 stránek obsahuje formulář pro prohlášení o shodě implementace (tzv. formulář ICS). Tento formulář vyplňuje dodavatel zařízení nebo implementátor systému, které je předmětem zkoušky, za účelem posouzení shody dané implementace s požadavky uvedenými v popisovaném dokumentu.

Formulář obsahuje:

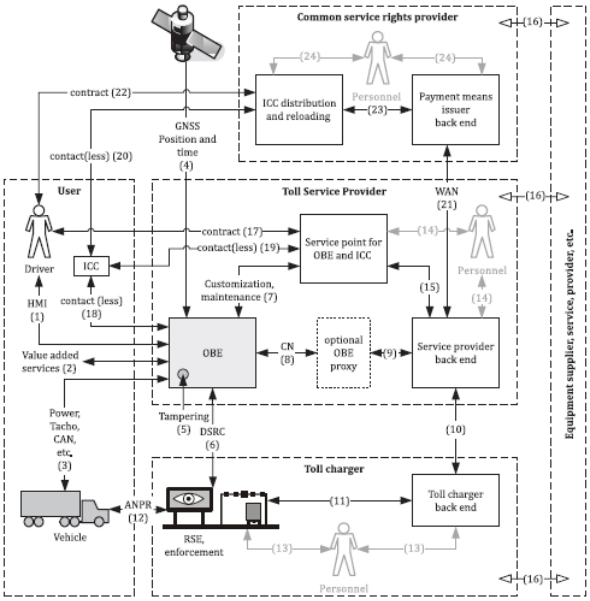
- 1 tabulku pro identifikace role v rámci architektury EFC;
- 6 tabulek pro zaznamenání souladu s modelem důvěry popsaným v kapitole 5;
- 1 tabulku pro zaznamenání souladu s bezpečnostním profilem popsaným v příloze A;
- 6 tabulek pro zaznamenání souladu s požadavky popsanými v kapitole 6;
- 14 tabulek pro zaznamenání shody s opatřeními popsanými v kapitole 7;
- 2 tabulky pro zaznamenání shody s DSRC rozhraním;

Příloha C (informativní) – Obecné požadavky na zúčastněné strany

Příloha C v rozsahu 4 stránek identifikuje obecné požadavky na zúčastněné strany, tj. výběrčího mýtného, poskytovatele mýtných služeb a management interoperability.

Příloha D (informativní) – Analýza hrozeb

Příloha D v rozsahu 57 stránek předkládá analýzu hrozeb provedenou pomocí dvou různých přístupů. První přístup vychází z analýzy na základě útoků, kde hnacím motorem útoku je záměr a výhoda útočníka. Tato analýza však nezahrnuje nezamýšlené hrozby ze strany uživatele a zařízení, které způsobily nehody nebo které měly přirozené příčiny (např. klimatické jevy). Tyto jsou doplněny v druhém přístupu, který vychází z analýzy na základě aktiv. Model, který je pro tuto analýzu uvažován, je ilustrován níže.



Obrázek 1 – Uvažovaný model pro analýzu hrozeb (obr. D.1 normy)

Příloha E (informativní) – Bezpečnostní politiky

Příloha E v rozsahu 6 stránek poskytuje příklad bezpečnostní politiky pro interoperabilitu systémů EFC. Tato příloha také vysvětluje hierarchickou strukturu založenou na této bezpečnostní politice nejvyšší úrovně doplněné bezpečnostními politikami druhé úrovně každého subjektu zapojeného do systému EFC.

Příloha F (informativní) – Příklad bezpečnostní politiky pro EETS

Příloha F v rozsahu 1 stránky uvádí příklad bezpečnostní politiky pro EETS, tj. rozšíření příkladu uvedeného v příloze E o ujednání z právních a regulativních aktů Evropské Komise.

Příloha G (informativní) – Doporučení pro implementace zaměřené na soukromí

Příloha G v rozsahu 2 stránek uvádí doporučení pro implementace zaměřené na soukromí.