EXTRAKT z technické specifikace

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

Elektronický výběr poplatků (EFC) – Zabezpečené monitorování pro autonomní systémy výběru mýtného – Důvěryhodný záznamník

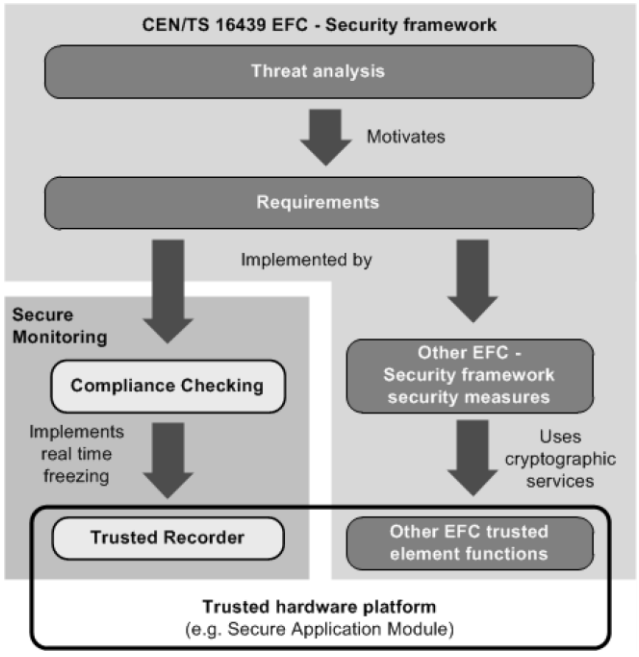
ČSN
CEN/TS 16702-2

01 8365

47 stran

Úvod

Tato norma je součástí sady technických norem zabezpečeného monitorování pro autonomní systémy, která se snaží o doplnění prostředků definovaných v technické specifikaci CEN/TS 16439 (znázorněno v diagramu níže - obsahuje analýzu rizik a definuje obecné požadavky na zabezpečení interoperabilních systémů EFC). Toto doplnění se týká zajištění důvěryhodnosti mýtných deklarací (tj. údajů týkajících se využití prostředků silniční infrastruktury).



Obrázek 1 – Doplnění normy 16439 pomocí důvěryhodného záznamníku (obr. 1 normy 16702-2)

CEN/TS 16702 se skládá z následujících částí:

Část 1: Zkoušení shody

Část 2: Důvěryhodný záznamník

Část 2 specifikuje kryptografické služby nutné k implementaci konceptu kontroly shody specifikované v části 1.

Užití

Cílem popisovaného dokumentu je definice mechanismu, včetně specifikace požadavků, pro ověření autentičnosti a důvěryhodnosti mýtných deklarací vytvořených na straně OBE (t.j. poskytovatele služby elektronického mýtného systému). Samotný proces ověřování probíhá na straně subjektu pro výběr elektronického mýtného.

2 Souvisící normy

ČSN P CEN/TS 16439 Elektronický výběr poplatků - Bezpečnostní rámec

ČSN P CEN/TS 16702-1 Elektronický výběr poplatků (EFC) - Bezpečné monitorování pro autonomní systémy výběru mýtného - Část 1: Zkoušení shody

ČSN EN ISO 14906 Elektronický výběr mýtného (EFC) - Stanovení aplikačního rozhraní pro vyhrazené spojení krátkého dosahu

ČSN ISO/IEC 10118-3 Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 9797-1 Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MACs) - Část 1: Mechanismy používající blokovou šifru

1 Předmět normy

Cílem popisovaného dokumentu je definice bezpečného aplikačního modulu (Secure Application Module), jenž je použit v konceptu procesu kontroly shody datových položek a je použit v následujících konfiguracích:

- Důvěryhodný záznamník (integrovaný v OBE a zodpovědný za zmrazení itineráře kalkulací autentikátoru pro jednotlivé itineráře)
- SAM (v ostatních entitách systému EFC a zodpovědný za kontrolu autentikátorů vypočtených pro itineráře pomocí důvěryhodného záznamníku)

Pro výše uvedené konfigurace uvádí popisovaný dokument některé z následujících aspektů:

- termíny a definice použité k popisu daných konfigurací
- požadavky na základní bezpečnostní funkce a procedury správy šifrovacích klíčů
- funkční požadavky pro obě SAM konfigurace společně s klasifikací různých úrovní zabezpečení

Obsah popisovaného dokumentu reflektuje architekturu systému EFC definovanou v normě ISO 17573 a dalších technických specifikacích od této normy odvozených (CEN/TS 16702-1 a 16439).

3 Termíny a definice

Kapitola obsahuje 31 termínů a definic souvisejících s touto technickou specifikací.

Klíčové termíny:

3.2
autentikátor *(Authenticator)*
data sloužící k autentizaci, která mohou být zašifrována

3.9
itinerář *(itinerary)*
cestovní záznamy organizované do jednoho nebo více itinerářových záznamů umožňující ohodnocení správnosti mýtných deklarací

3.15
zmrazení v reálném čase *(real-time freezing)*
zmrazení každého itinerářového záznamu, jakmile se jeho akvizicí ukončilo používání důvěryhodného záznamníku

3.20
zkoušení shody bezpečného monitorování *(secure monitoring compliance checking)*
koncept, který výběrčímu mýtného umožňuje spoléhat na důvěryhodnost výkazů o mýtném vytvořených poskytovatelem mýtné služby

3.22
výkaz o mýtném *(toll declaration)*
hlášení výběrčímu mýtného, které deklaruje použití dané mýtné služby

3.23
mýtná doména *(toll domain)*
oblast nebo část sítě pozemní komunikace, kde platí režim mýtného

3.28
důvěryhodný záznamník *(trusted recorder)*
logická entita schopná kryptografických funkcí, poskytující OBE služby zabezpečení zahrnující důvěrnost a integritu dat, autentizaci a nepopiratelnost

4 Značky a zkratky

Tato kapitola obsahuje 31 zkratek (následující seznam uvádí pouze klíčové zkratky):

RSA algoritmus pro šifrování veřejného klíče Rivest Shamir and Adleman *(Algorithm for public-key cryptography (Rivest, Shamir and Adleman)*

MAC autentizační kód zprávy *(Message Authentication Code)*

RTF zmrazení v reálném čase *(Real-Time Freezing)*

SAM bezpečný aplikační modul *(Secure Application Module)*

TR důvěryhodný záznamník *(Trusted Recorder)*

TDC čítač mýtných domén *(Toll Domain Counter)*

TTS důvěryhodný zdroj času *(Trusted Time Source)*

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

5 Koncepty a scénáře pro SAM

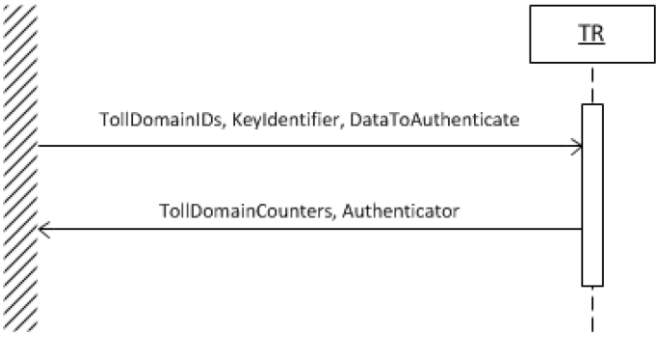
Tato kapitola popisuje koncept použití důvěryhodného záznamníku (pro použití na straně OBE) a bezpečného aplikačního modulu (pro použití na straně zařízení na pozemní komunikaci, poskytovatele služby elektronického mýtného a subjektu pro výběr elektronického mýta) a požadavky na podporu kryptografických služeb pro obě tyto entity (podpora symetrické a asymetrické kryptografie).

Na základě požadavků týkajících se podporovaných mýtných schémat, poskytuje důvěryhodný záznamník některé z následujících funkčních prvků:

- autentičnost a integrita datových prvků (na základě symetrických či nesymetrických kryptografických algoritmů)
- správa a archivace čítačů (pro zajištění správné sekvence itinerářů a případnou detekci chybějících položek)

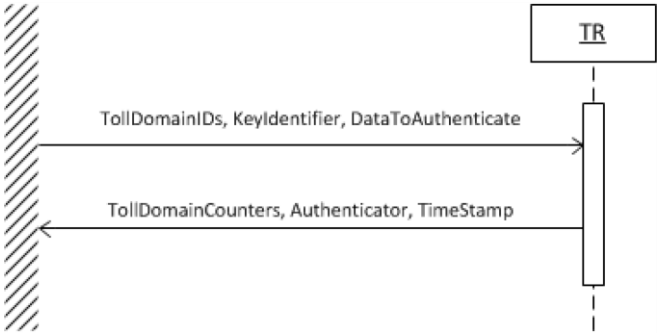
V jednotlivých podkapitolách jsou popsány základní principy fungování důvěryhodného záznamníku a bezpečného aplikačního modulu, společně s následujícími scénáři pro:

- důvěryhodný záznamník:
    - zmrazení itineráře v reálném čase bez použití důvěryhodného zdroje času (schéma komunikace viz níže)



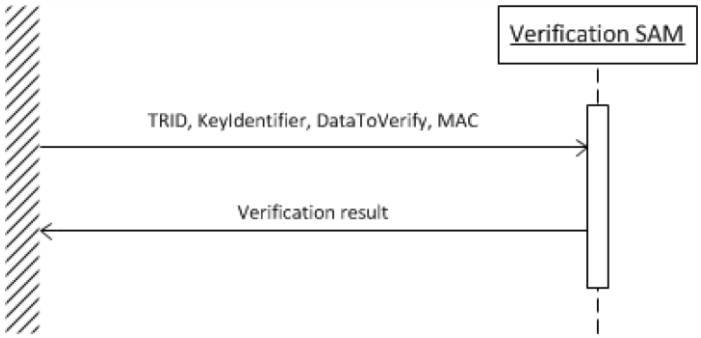
Obrázek 2 – Zmrazení bez použití důvěryhodného zdroje času (obr. 3 normy 16702-2)

- zmrazení itineráře v reálném čase s použitím důvěryhodného zdroje času (schéma komunikace viz níže)



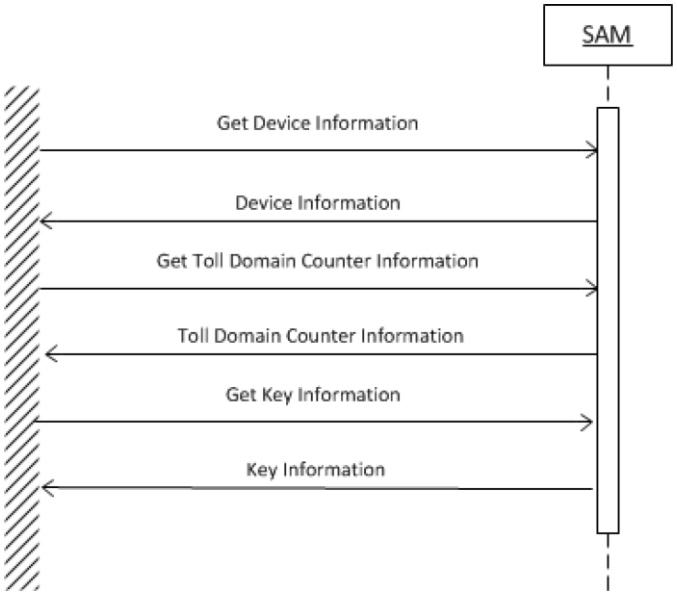
Obrázek 3 – Zmrazení s použitím důvěryhodného zdroje času (obr. 4 normy 16702-ě)

- bezpečný aplikační modul:
  - jednotný proces pro ověření MAC na straně poskytovatele služby elektronického mýtného, subjektu pro výběr elektronického mýtného a zařízení na pozemní komunikaci



Obrázek 4 – Ověření MAC (obr. 5 normy 16702-2)

- A popis obecných scénářů pro:
  - definici a správu čítačů pro jednotlivé mýtné domény v rámci důvěryhodného záznamníku (tyto čítače jsou použity při výpočtu autentizačního kódu pro data)
  - specifikace dat, která by měla být přítomna v bezpečném aplikačním modulu nebo v důvěryhodném záznamníku (např. identifikační kód zařízení, verze, čítač mýtných domén apod. – viz diagram níže)



Obrázek 6 – Identifikace SAM (obr. 6 normy 16702-2)

6 Funkční požadavky

Tato kapitola prezentuje možnosti a požadavky na funkčnost bezpečného aplikačního modulu (v závislosti na plánovaném využití). Tyto možnosti se týkají zejména procedur a funkcí pro symetrickou a asymetrickou kryptografii, import bezpečnostních klíčů, použití důvěryhodného zdroje času při autentizačním procesu apod. Jednotlivé funkční požadavky jsou rozděleny do následujících tříd:

- Základní požadavky (identifikace důvěryhodného záznamníku a ověření bezpečného aplikačního modulu a jeho klíčů)
- Správa bezpečnostních klíčů (import a generování bezpečnostních klíčů, jejich atributy a vlastnosti)
- Kryptografické funkce (funkce související s autentizací, integritou a důvěrností dat)
- Zmrazení v reálném čase
- Verifikace bezpečného aplikačního modulu (verifikační funkcionalita pro symetrickou kryptografii)
- Čítač mýtných domén (operace nad čítačem)
- Důvěryhodný zdroj času (funkcionalita důvěryhodného zdroje času)
- Úroveň zabezpečení (požadavky na zabezpečení pro důvěryhodný záznamník a bezpečný aplikační modul)

7 Požadavky pro rozhraní

Tato kapitola obsahuje definice aplikační protokolové datové jednotky (APDU) pro důvěryhodný záznamník (netýká se bezpečného aplikačního modulu) bez použití důvěryhodného zdroje času. Tyto definice obsahují zejména sémantické sekvence kroků a kódování dotazů a odpovědí. Kapitola rovněž poskytuje popis jednotlivých příkazů pro funkčnost důvěryhodného záznamníku (mimo příkazy pro uvedení do provozního stavu), jež zahrnuje následující procesy:

- Výpočet MAC pro zmrazení v reálném čase za použití symetrického bezpečnostního klíče
- Výpočet digitálního podpisu pro zmrazení v reálném čase za použití asymetrického bezpečnostního klíče
- Čtení specifických informací o zařízení
- Čtení hodnot jednotlivých čítačů mýtných domén
- Čtení informací ohledně bezpečnostních klíčů (symetrické i asymetrické)
- Správa chybových hlášení

Příloha A (normativní) – Specifikace datových typů

Příloha A obsahuje definici datových typů ve formátu ASN.1. Definice pokrývají datové typy vztahující se k entitám a funkcím definovaných v kapitolách 6 a 7.

Příloha B (normativní) – Formulář ICS

Příloha B obsahuje tabulky pro dodatečné informace o zkoušení implementace protokolu (např. implementované funkční požadavky a požadavky na rozhraní atd.).

Příloha C (informativní) – Problémy s implementací důvěryhodného zdroje času

Příloha C prezentuje vybrané aspekty (a případné problémy s potenciálním přístupem k řešení) týkající se implementace důvěryhodného zdroje času v rámci důvěryhodného záznamníku. Tyto aspekty se týkají zejména možných variant implementace důvěryhodného zdroje času (izolované hodiny, hodiny s nutnou externí kalibrací např. GNSS, důvěryhodná třetí strana či kalibrace používající protokol NTP) a jeho napájení.

Příloha D (informativní) – Použití této technické specifikace v rámci EETS

Příloha F vysvětluje pozici popisovaného dokumentu (resp. jeho obsahu) v rámci Evropské služby elektronického mýtného (nicméně popisovaný dokument nemá přímou souvislost s požadavky uvedenými v Rozhodnutí EC 2009/750/EC).