

CEN TS 16702-1 - Elektronický výběr poplatků (EFC) – Zabezpečené monitorování pro autonomní systémy výběru mýtného – Zkoušení shody

Aplikační oblast: [Elektronický výběr poplatků \(EFC\)](#)

Počet stran: 101

Zavedení normy do ČSN: originálem

Rok zpracování extraktu: 2015

Skupina témat: Zabezpečení a kontrola

Téma normy: Kontrola důvěryhodnosti

Charakteristika tématu: Rozšířený kontrolní mechanismus pro zajištění důvěryhodnosti dat týkajících se využití silniční infrastruktury

Úvod, vysvětlení východisek
Popis architektury, hierarchie, rolí a vztahů objektů Popis vztahu a pozice procesu kontroly v rámci bezpečnostního rámce.
Popis procesu / funkce / způsobu použití Definice konceptu a procesů zahrnutých v kontrolním mechanismu. Definice procesů pro zpracování itineráře. Definice procesů pro kontrolu mýtných deklarací. Definice procesů pro správu bezpečnostních klíčů.
Popis rozhraní / API / struktury systému Využití transakčních primitiv z jiných norem (12813 a 12855). Požadavky na služby nižších vrstev. Jména API funkcí a parametry. Definice pravidel pro výměnu informací mezi poskytovatelem služby a výběřčím mýtného.
Definice protokolu / algoritmu / výpočtu Popis využití kryptografických nástrojů v rámci hashovacích funkcí, certifikátů a digitálních podpisů.
Definice reprezentace dat / fyzikálního významu Reprezentace datových struktur v ASN.1. Definice datových struktur pomocí UML diagramů.
Definice konstant / rozsahů / omezení

Úvod

Tato norma je součástí sady technických norem zabezpečeného monitorování pro autonomní [systémy](#). Umožňuje, v kombinaci s regulérní kontrolou dodržování pravidel podle [ISO/TS 12813](#), vybudovat důvěru mezi subjektem [výběru mýtného](#) a poskytovatelem [služby](#). Nástroje definované v [ISO/TS 12813](#) umožňují získat indikaci, zda je [OBE](#) plně [funkční](#), avšak tyto jsou definované na předpokladu, že [OBE](#) je zabezpečená a mezi subjektem pro [výběr mýtného](#) a poskytovatelem [služby](#) elektronického [mýtného](#) existuje důvěra. Na základě tohoto předpokladu zavádí popisovaný dokument nástroje, v kombinaci s již definovanými v [ISO/TS 12813](#), jež umožňují lepší kontrolu rizik, plynoucích z neexistence daného předpokladu, a sice existence důvěry k poskytovateli [služby](#) a jeho [OBE](#). Poskytuje subjektu pro [výběr mýtného](#) způsob, jakým ověřit důvěryhodnost [výkazů o mýtném](#) (jež jsou vytvořeny poskytovatelem [služby](#) a jeho [OBE](#)).

CEN/TS 16702 se skládá z následujících částí:

- Část 1: [Zkoušení shody](#)
- Část 2: Důvěryhodný záznamník

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

Užití

Cílem části 1 popisovaného dokumentu je definice [transakcí](#) mezi poskytovatelem [služby](#) ([centrální systém](#) a [OBE](#)) a subjektem pro [výběr mýtného](#), za účelem zabezpečeného monitorování a potažmo vybudování vzájemné důvěry. Metoda zabezpečeného monitorování – kontroly shody je vhodná pro obě výše zmiňované role, např. v rámci následujících procesů:

- Ustanovení důvěry mezi rolemi, bez ohledu na typ [mýtného](#) režimu
- Poskytování důkazů akceptovatelných soudem

Metoda je rovněž vhodná k použití jak pro lokální [mýtné schémata](#), tak pro interoperabilní [systémy](#), např. Evropská [služba](#) elektronického [mýtného](#) ([EETS](#)).

1. Předmět normy

Cílem popisovaného dokumentu je definice dat a [transakcí](#) v rámci kontroly shody a zabezpečeného monitorování. Toto zahrnuje následující aspekty:

- Koncept a procesy definované pro zabezpečené monitorování
- Definice [transakcí](#) za účelem kontroly (a zároveň využití již existující [transakce](#), resp. dat získaných z [transakcí](#), definovaných v [CEN ISO/TS 12813](#) a EN [ISO 12855](#))
- Popis technických a organizačních nástrojů zahrnutých v zabezpečeném monitorování
- Vzájemné vztahy mezi jednotlivými zúčastněnými entitami ([OBE](#), domény subjektu pro [výběr](#) elektronického [mýtného](#) a poskytovatele [služby](#) elektronického [mýtného](#)).

Popisovaný dokument se rovněž zabývá popisem vzájemných vztahů jednotlivých alternativ v rámci domén poskytovatele [služeb](#) a subjektu pro [výběr mýtného](#).

Popisovaný dokument rovněž úzce souvisí s normou [CEN/TS 16439](#), a sice jako množina konkrétních nástrojů definovaných pro použití při výskytu hrozeb, definovaných v této normě:

- Hrozby přiřazené uživateli
 - Manipulace vedoucí k neschopnosti registrace, nesprávná registrace užití silniční infrastruktury
 - Manipulace vedoucí ke ztrátě dat souvisejících s užitím silniční infrastruktury
- Hrozby přiřazené poskytovateli [služby](#) elektronického [mýtného](#)
 - Modifikace dat získaných z OBE
 - Chybná interpretace dat z OBE
 - Chybná konfigurace OBE

2. Související normy

ČSN ISO/IEC 29100 Informační technologie – Bezpečnostní techniky – Rámec soukromí

ČSN [ISO 17573:2012 Elektronický výběr poplatků](#) (EFC) – Architektura [systémů](#) zpoplatňujících vozidla

ČSN P [CEN ISO/TS 17444-1 EFC](#) – Metriky pro posouzení výkonnosti – Část 1: Metriky

ČSN P [CEN ISO/TS 12813 EFC](#) - Komunikace pro kontrolu shody autonomních [systémů](#)

ČSN EN [ISO 12855 EFC](#) - Výměna informací mezi poskytovateli a [výběřčími mýtného](#)

ČSN EN [ISO 14906 EFC](#) - Stanovení aplikačního [rozhraní](#) pro vyhrazené spojení krátkého dosahu

ČSN P [CEN/TS 16439 Elektronický výběr poplatků](#) - Bezpečnostní rámec

3. Termíny a definice

Kapitola obsahuje 24 termínů a definic souvisejících s touto technickou specifikací.

Klíčové termíny jsou následující:

- 3.2**
[autentikátor](#) (*Authenticator*)
data sloužící k autentizaci, která mohou být zašifrována
- 3.9**
[zmrazení itineráře](#) (*itinerary freezing*)
registrace itineráře a nesporné přihlášení se k němu
- 3.15**
[itinerářový záznam](#) (*itinerary record*)
atomický datový [prvek](#), který popisuje užití silniční sítě nebo vozidla
- 3.17**
[zmrazení v reálném čase](#) (*real-time freezing*)
zmrazení každého itinerářového záznamu, jakmile se jeho akvizicí ukončilo používání důvěryhodného záznamníku
- 3.18**
[zkoušení shody bezpečného monitorování](#) (*secure [monitoring](#) compliance checking*)
koncept, který [výběřčímu mýtného](#) umožňuje spoléhat na důvěryhodnost [výkazů o mýtném](#) vytvořených poskytovatelem [mýtné služby](#)
- 3.20**

výkaz o mýtném (*toll declaration*)

hlášení **výběřčímu mýtného**, které deklaruje použití dané **mýtné služby**

3.21

mýtná doména (*toll domain*)

oblast nebo část sítě pozemní komunikace, kde platí **režim mýtného**

3.22

důvěryhodný záznamník (*trusted recorder*)

logická entita schopná kryptografických funkcí, poskytující **OBE služby** zabezpečení zahrnující důvěrnost a **integritu dat**, autentizaci a **nepopíratelnost**

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

4. Symboly a zkratky

Tato kapitola obsahuje 30 zkratk (následující seznam uvádí pouze klíčové zkratky):

SM_CC- zkoušení shody bezpečného monitorování (*Secure Monitoring Compliance Checking*)

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

5 Procesy

Tato kapitola představuje konceptuální rámec požadavků na **systemy** a zařízení, jež zabezpečené monitorování – kontrolu shody implementují. Popisuje zúčastněné entity (poskytovatel **služby**, subjekt pro **výběř mýtného** a **uživatel služby**) a procesy a jejich vzájemné vazby v rámci procesu zpracování itineráře.

Reprezentace užití silniční infrastruktury je uložena v **OBE** ve formě tzv. Itineráře, jenž je zpracován (v reálném čase či s pevně stanoveným zpožděním) v rámci procesu nazvaném „zmrazení itineráře“. Tento proces zajišťuje **integritu** itineráře tím, že znemožňuje nedetekovatelnou pozdější manipulaci či výměnu dat itineráře. Proces zmrazení je definován v následujících variantách:

- zmrazení v reálném čase: Předpokládá se existence důvěryhodného zařízení (tzv. důvěryhodný záznamník) v **OBE**, jež je schopné provést operaci vytvoření digitálního **podpisu** pro itinerář v reálném čase;
- zmrazení po deklaracích: Itinerář je digitálně podepsán v **centrálním systému** poskytovatele **služby** elektronického **mýtného** a následně zaslán subjektu pro **výběř** elektronického **mýtného** skrze **rozhraní** definované v **ISO 12855** (zpráva Toll Declaration).

Mimi procesu zmrazení itineráře, poskytuje **zkoušení shody** poskytovateli **služby** nástroje pro kontrolu konzistence mezi reporty týkajícími se užití silniční infrastruktury a **mýtných** deklarací obsažených v itineráři:

- Kontrola zmrazení itineráře (Checking of Itinerary Freezing – CIF) – kontrola uložených itinerářů na základě pozorování užití silniční infrastruktury – tj. náhodných kontrol
- Kontrola **mýtných** deklarací (Checking of Toll Declaration – CTD) – kontrola správnosti **mýtných** deklarací na základě agregace dat z jednotlivých itinerářů
- Proces žádosti o zpětnou kontrolu při nálezů nekorektních údajů (v případě detekce problému s daty uloženými v itineráři)
- Přístup k datům **mýtného** kontextu (tyto data se týkají nastavení procesů tvorby itineráře)
- Správa zabezpečovacích klíčů

Kapitola popisuje výše zmíněné procesy a rovněž definuje požadavky na jejich **funkčnost** z hlediska požadovaných rysů a rolí v rámci **mýtného systému**, podmínek pro efektivní provedení kontroly shody a **dopadu** na soukromí uživatele.

6 Transakce

Tato kapitola popisuje sémantiku dat, jež jsou zpracovány procesy definovanými v předchozí kapitole (např. data itineráře, **transakce** kontroly shody mezi **OBU** a subjektem pro **výběř mýtného**, **transakce** kontroly shody mezi **centrálními systémy** poskytovatele **služeb** a subjektu pro **výběř mýtného** a **transakce** probíhající na straně silniční infrastruktury, províze **kontextových dat**). Rovněž popisuje **transakční modely** všech definovaných procesů. Pro **transakce** odehrávající se mezi poskytovatelem **služby** elektronického **mýtného** a subjektem pro **výběř** elektronického **mýtného** je využito specifikací protokolových datových jednotek definovaných v **ISO 12855**. Jedná se např. o:

- TollDeclarationADU – datová jednotka obsahující **mýtné** deklarace
- AckADU – datová jednotka obsahující potvrzující mechanismus

Popisovaný dokument rovněž definicí svých vlastních **transakcí** (a tudíž i protokolových jednotek) poskytuje rozšíření definice **rozhraní** mezi poskytovatelem **služby** a subjektem pro **výběř** specifikované v **ISO 12855**.

Pro každou [transakci](#) mezi subjektem pro [výběr](#) elektronického [mýtného](#) a poskytovatelem [služby](#) elektronického [mýtného](#) jsou definovány následující [atributy](#):

- typ zprávy (např. požadavek, potvrzení či jednotlivé protokolové datové jednotky s odpovídajícími [atributy](#), např. [mýtné](#) deklarace, kontrola itineráře)
- pravidlo pro poskytovatele [služby](#) specifikující podporu dané [transakce](#) (např. možnost iniciovat či odpovědět na [transakci](#))
- pravidlo pro subjekt pro [výběr mýtného](#) specifikující podporu dané [transakce](#) (např. možnost iniciovat či odpovědět na [transakci](#))

V rámci definic konkrétních [transakcí](#) je v této kapitole rovněž specifikována [transakce](#) pro informování poskytovatele [služby](#) elektronického [mýtného](#) subjektem pro [výběr](#) v případě detekce nesrovnalostí v rámci procesu kontroly shody.

7 Zabezpečení

Tato kapitola definuje zabezpečovací [prvky](#) implementované v zabezpečeném monitorování. Mezi tyto [prvky](#) patří následující:

- Bezpečnostní funkce a entity:
 - Hashovací funkce – použité jako hashovací algoritmus pro zmrazení itineráře
 - [MAC](#) – případ symetrické autentizace dat itineráře
 - Digitální [podpis](#) – případ asymetrické autentizace dat itineráře
 - Veřejné klíče, certifikáty a [CRL](#) – referenční datové [atributy](#) použité k identifikaci veřejných a soukromých klíčů použitých k výpočtu digitálního [podpisu](#) v rámci důvěryhodného záznamníku (certifikáty veřejných klíčů by měly obsahovat rozšíření specifikující např. základní omezující podmínky či předpokládané použití klíčů)
- Správa bezpečnostních klíčů:
 - Proces výměny klíčů mezi zúčastněnými stranami
 - Generování klíčů a certifikační proces
- Charakteristiky důvěryhodného záznamníku a modulu SAM v rámci verifikačního procesu (nikoliv požadavky na technickou funkcionalitu – ty jsou definovány v části 2 CEN/TS 16702).

Příloha A (informativní) – Specifikace datových typů

Příloha A obsahuje definici datových typů ve formátu [ASN.1](#). Definice pokrývají datové typy vztahující se k entitám a funkcím použitým v rámci zabezpečeného monitorování – kontroly shody.

Příloha B (normativní) – Formulář PICS

Příloha B obsahuje tabulky pro [dodatečné informace o zkoušení implementace](#) protokolu (např. podporované typy zabezpečeného monitorování, podporované procesy atd.).

Příloha C (informativní) – Příklady [transakcí](#)

Příloha C obsahuje příklady [transakcí](#), jež mohou být použity pro kontrolu procesu zmrazení itineráře v reálném čase. V této příloze jsou zahrnuty následující příklady [transakcí](#):

- [transakce](#) s daty itineráře nezávislými na kontextu
- kombinovaná [transakce](#) specifikovaná v [CEN ISO/TS 12813](#) a SM_CC [transakce](#)
- kombinovaná [transakce](#) specifikovaná v [CEN ISO/TS 12813](#) a SM_CC [transakce](#) s optimalizací na použití pouze 2 rámců

Příloha D (informativní) – Relevantní hrozby

Příloha D obsahuje souhrn relevantních možností [útoků](#) na provoz elektronického [mýtného systému](#). Rovněž prezentuje případy těchto [útoků](#), proti kterým může zabezpečené monitorování poskytnout účinný nástroj, např. zaslepení sensoru pro detekci míry užití silniční infrastruktury, odstranění či zničení [OBE](#), rušení sensoru používající technologii GNSS, manipulace s daty souvisejícími s užitím silniční infrastruktury, používání simulátoru OBE

Příloha E (informativní) – Základy konceptu SM_CC

Příloha E poskytuje detailnější náhled do motivace a filosofie konceptu zabezpečeného monitorování. Obsahuje [zdůvodnění](#) hlavních rozhodnutí a možné další alternativy, např.:

- Jaký je účel zabezpečeného monitorování a kontroly shody
- Jak [zkoušení shody](#) funguje
- Proč je nutná další norma vzhledem k existenci [ISO 12813](#)

Příloha F (normativní) – 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).

Související termíny

- [spojitý výkaz o mýtném](#)