ISO/TS 21177 - **Inteligentní dopravní systémy – Služby zabezpečení stanice ITS pro zřízení bezpečného spojení a autentizaci mezi důvěryhodnými zařízeními**

Application Area: Cooperative systems

Publication Year, Number of Pages: Published 2019, 83 pages

Extract Creation Year: 2019

Standard Topic Group: Inteligentní dopravní systémy

Standard Topic: Zabezpečení ITS stanic

Topic Description: Popis služeb zabezpečení ITS stanic potřebných pro zajištění důvěryhodné komunikace

Introduction, Explanation of Starting Points

Specifikace služeb ITS stanice potřebných pro ověření autentičnosti zdorje a integrity informací vyměňovaných důvěryhodnými zařízeními

Description of Architecture, Hierarchies, Roles, and Object Relationships

Návrh logické a funkční architektury zabezpečení komunikace ITS stanic vycházející z ISO 21217

Description of Process / Function / Method of Use

Description of Interfaces / APIs / System Structure

Popis základních služeb (service primitives)

Protocol / Algorithm / Computation Definition

Definition of Data Representation / Physical Meaning

Reprezentace datových struktur v ASN.1.

Definition of Constants / Ranges / Restrictions

Introduction

V posledním desetiletí se objevily služby ITS, které vyžadují zabezpečený přístup k datům ze senzorických a řídicích sítí (SCN), např. ze sítí ve vozidle (IVN) nebo z infrastrukturní sítě (IRN), z nichž některé vyžadují bezpečný místní přístup k časově kritickým informacím.

Tato technická specifikace (dále jen popisovaný dokument) stanovuje množinu služeb zabezpečení ITS stanice potřebných pro zajištění autentičnosti zdroje a integrity informací vyměňovaných mezi důvěryhodnými prvky. Tyto služby zahrnují autentizaci a vytvoření zabezpečené relace, která je požadována pro výměnu informací důvěrným a bezpečným způsobem. Dokument je navržen jako standard pro zajištění zabezpečené komunikace a oboustranného ověření autentičnosti rovnocenných aplikačních procesů.

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

Application

Obsahem popisovaného dokumentu jsou požadavky na služby zabezpečení ITS stanic zajišťujících autentičnost zdroje, důvěryhodnost a integritu činnosti aplikací uskutečňující se mezi důvěryhodnými zařízeními. Tyto služby lze využít pro bezpečný přístup např. k datové síti vozidla nebo do jiné sítě ITS. Popisovaný dokument je tak určen především vývojářům ITS stanic a aplikací řešících zabezpečení datové komunikace mezi různými prvky konkrétního ITS. Dále

může být použita orgány státní správy nebo projektanty ITS systémů jako podklad pro návrh systému nebo specifikaci požadavků na navrhovaný systém.

Související případy užití tohoto dokumentu jsou odvozeny od požadavků a provozních potřeb ITS, kterými jsou:

- zabezpečení přístupu k časově kritickým vozidlovým datům v reálném čase za účelem zvýšení bezpečnosti provozu (např. vyhnutí kolizi, nouzová elektronická brzdová světla);
- zabezpečení lokálního přístupu k detailním datům aplikací pro zvýšení efektivity provozu v reálném čase (dynamické řízení dopravy, předcházení kolonám);
- ochrana osobních dat (např. v souladu s evropským nařízením GDPR)
- lokální přístup k ověřeným aktuálním datům pro využití aplikacemi udržitelného rozvoje (např. dynamické emisní zóny, prioritní průjezd křižovatkou pro minimalizaci emisí apod.)

Je popsána celá řada případů užití ITS služeb, pro které je výměna časově kritických informací v reálném čase zásadní a další případy užití budou přibývat. Mnoho z nich zahrnuje potřebu zajištění přístupu jednotek ITS stanic k datům z vozidel nebo infrastruktury, a to přístupu zabezpečeného. Nicméně dle ISO 21217, ITS-SCU obsažená v jednotce ITS stanice může komunikovat s externím zařízením, které není v souladu s architekturou dle ISO 21217. Příkladem takového zařízení může být přístupový uzel v internetu, senzoru, nebo řídicí síti. Úlohou tohoto dokumentu tak je zavést specifika zabezpečení ITS stanic pro tento typ komunikace, aby mohla být považována za důvěryhodnou.

1. Scope

Předmětem popisovaného dokumentu tak jsou následující tři úlohy:

1) Specifikovat služby zabezpečení ITS stanice pro zajištění důvěry mezi aplikačními procesy ITS-S běžícími na různých ITS-SCU stejných ITS-SU, tj. vytvoření důvěryhodné procesní platformy s ohledem na důvěryhodnost uvnitř ITS-SCU:

- ochranu aplikací před akcemi jiných aplikací;
- ochranu sdílených informací;
- ochranu sdílených zdrojů zpracování, jako je komunikační software a hardware, který zahrnuje metody stanovení priorit a omezený přístup.

2) Specifikovat služby zabezpečení ITS stanice pro zajištění důvěry mezi aplikačními procesy ITS-S běžícími na stejné jednotce ITS stanice.

3) Rozšíření těchto služeb zabezpečení ITS pro zajištění důvěry mezi ITS-SCU a zařízeními, která jsou součástí senzorické a řídicí sítě.

Tento dokument obsahuje specifikace pro množinu služeb zabezpečení ITS stanice, které jsou potřebné k zajištění pravosti zdroje a integrity informací vyměňovaných mezi důvěryhodnými entitami:

- zařízeními provozovanými jako zabezpečené spravované entity, tj. komunikační jednotky ITS stanice (ITS-SCU) a stanice ITS (ITS-SU) specifikované v ISO 21217 a
- jednotkami ITS stanice (ITSSU) složenými z jedné nebo několika ITS-SCU a externími důvěryhodnými entitami jako jsou senzorické a řídicí sítě.

Tyto služby zahrnují autentizaci a vytvoření zabezpečené relace, které jsou požadovány pro výměnu informací důvěryhodným a bezpečným způsobem a jsou nezbytné pro řadu aplikací a služeb ITS, včetně časově kritických bezpečnostních aplikací, automatického řízení vozidla, vzdálené obsluhy ITS stanic (dle ISO 24102-2) a služeb souvisejících se silniční infrastrukturou.

2. Associated Standards

ISO 21217 - Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture

ISO 24102 - Intelligent transport systems — Communications access for land mobiles (CALM) — Management

ISO 17419, Intelligent transport systems — Cooperative systems — Globally unique identification

IEEE Std 1609.2™, IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages

ISO 22418 - Intelligent transport systems — Fast service announcement protocol (FSAP)

3. Terms and Definitions

Dokument obsahuje celkem 10 termínů. Mezi nejdůležitější patří:
PDU pro řízení přístupu *(Access Control PDU)* – PDU vytvořená subsystémem zabezpečení za účelem vytvoření statusu autorizace komunikujícího aplikačního procesu jiné stanice ITS
zásady řízení přístupu *(Access Control Policy)* – zdroj dat určující jaký přístup ke zdrojům je povolen cizím aplikacím
subsystém zabezpečení *(security subsystem)* – funkční entita poskytující funkci zabezpečení pro aplikační proces stanice ITS
adaptér vrstvy zabezpečení *(Security Adaptor Layer)* – funkční entita poskytující funkci multiplexování a demultiplexování pro data a příkazy řízení relací
zabezpečená relace *(Secure Session)* – funkční entita zajišťující důvěrnost, integritu, autentizaci, zaručené zasílání ve správném sledu a ochranu proti přehrání datagramů, které jí procházejí
popisovač kryptografického materiálu *(Cryptomaterial Handle)* – odkaz na kryptografický materiál, který umožňuje jeho použití v kryptografických operacích, tzn. podpis, ověření, šifrování, dešifrování
služba zabezpečené relace *(Secure Session Service)* – funkční entita odpovědná za vytvoření relací se zabezpečenou komunikací s dalšími instancemi
Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS terminology.

4. Abbreviations

Kapitola obsahuje 24 zkratek souvisících s touto normou, z nichž nejdůležitější jsou následující:

ALPDU PDU vrstvy adaptéru *(adaptor layer PDU)*

APDU datová jednotka aplikačního protokolu *(application protocol data unit)*

ITS-S stanice ITS *(ITS station)*

ITS-SCU komunikační jednotka ITS stanice (*ITS station communication unit*)

ITS-SCP komunikační profil stanice ITS (Poznámka k heslu: Z ISO 21217) *(ITS station communication profile (Note to entry: From ISO 21217)*

ITS-SU jednotka stanice ITS [Zdroj: ISO 21217] *(ITS station unit [SOURCE: ISO 21217])*

PDU protokolová datová jednotka (*protokol data unit*)

SCN senzorová a řídící síť *(sensor and control network)*

SPAKE2 protokol pro vytvoření symetrického šifrovacího klíče *(secure password authenticated key Exchange 2)*

SSP oprávnění pro konkrétní službu *(service specific permission)*

SSTD zabezpečená relace mezi důvěryhodnými zařízeními *(secure session between trusted devices)*

TLS zabezpečení přenosové vrstvy; kryptografický protokol *(transport layer security)*

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

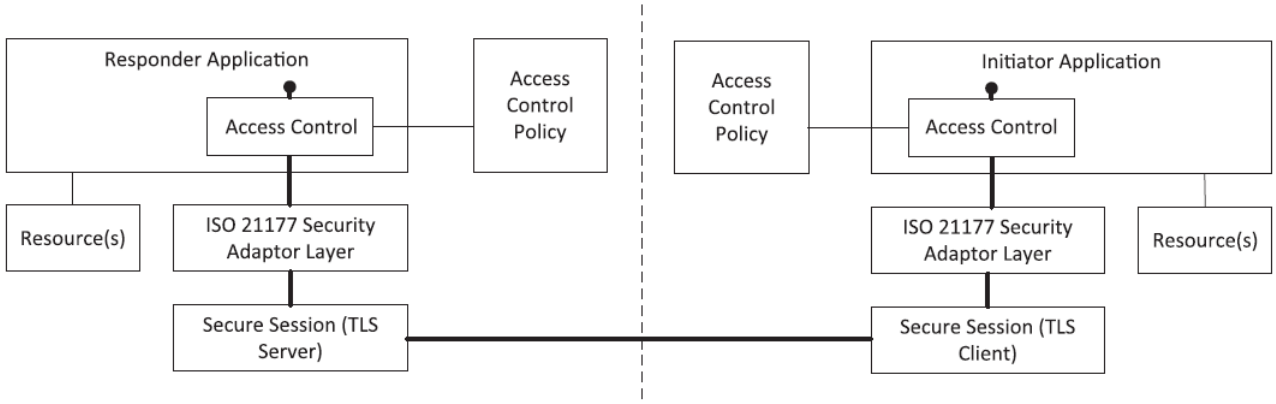
5 Přehled

Tato kapitola (rozsah 6 stran) představuje logickou architekturu, která je navržena k zajištění specifických cílů vyjmenovaných v článku 5.1. Příkladem těchto cílů jsou:

- Zajištění komunikace dvou různých aplikačních procesů ITS-S zabezpečeným způsobem.
- Umožnění vzájemné autentizace aplikačních procesů ITS-S na základě řízení přístupu založeného na rolích nebo atributech.

- Zajištění, aby každá příchozí APDU byla předmětem individuálního procesu řízení přístupu.

Tato architektura je zobrazena na obrázku 1 a dále popsána v článku 5.2 “Architektura a funkční entity” popisovaného dokumentu.

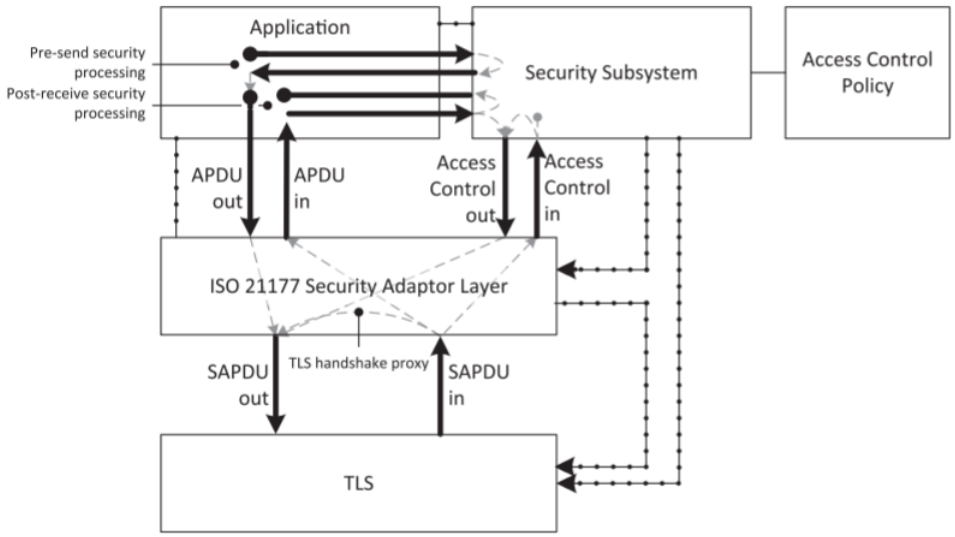


Obrázek 1 (obr. 7 normy): Logická architektura

Funkční entity, které jsou dále předmětem článku 5.2 jsou následující:

- Zdroje
- Aplikace
- Subsystém zabezpečení
- Adaptér vrstvy zabezpečení
- Zabezpečená relace
- Zásady řízení přístupu

Vztahy mezi těmito funkčními prvky v rámci jednoho zabezpečeného celku jsou pak znázorněny na obrázku 2



Obrázek 2 (obr. 8 normy): Vztahy mezi lokálními funkčními prvky

Další články kapitoly 5 popisují způsob logického přístupu k šifrovacím klíčům dle IEEE Std 1609.2, vytváření unikátních ID relací, dále obsahují popis základních příkazů řízení přístupu a stavů autorizace zabezpečení a v posledním článku kapitoly pak konvence základních příkazů služeb a další.

Architektura je dále rozdělena do tří funkčních celků, které jsou popsány v samostatných kapitolách 7, 8 a 9:

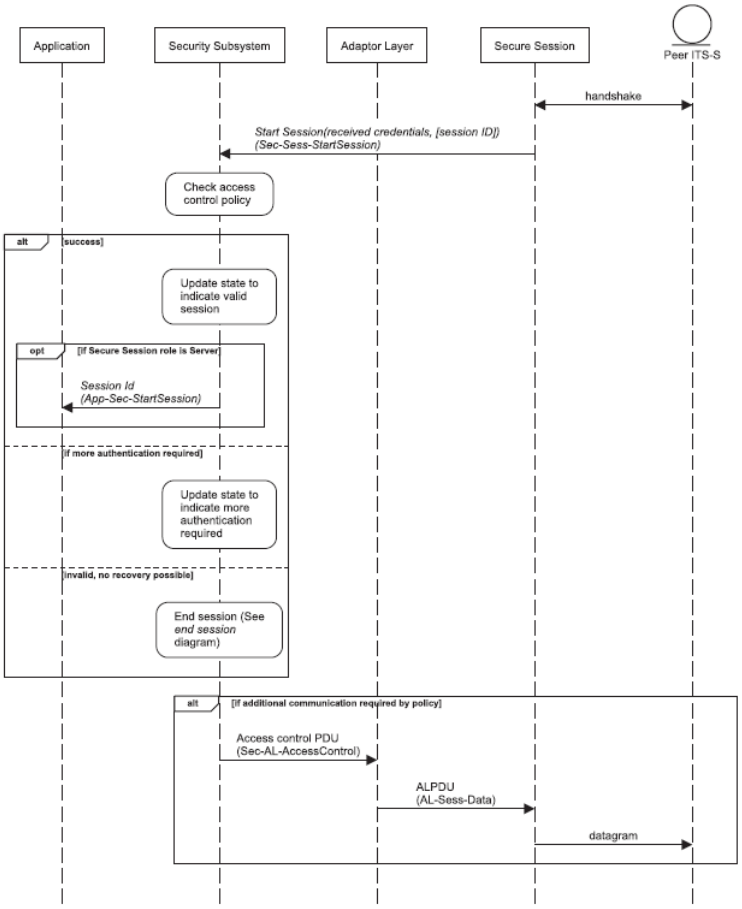
- Podsystém zabezpečení,

- Adaptační vrstva,
- Služby zabezpečení relace.

6 Průběh procesu a sekvenční diagramy

V této kapitole (rozsah 28 stran) je popsán průběh procesů (procesních toků) využívajících služby zabezpečení specifikované v tomto dokumentu a dále posloupnost datových toků spojených s každým z těchto procesních toků.

Článek 6.2 vyjmenovává přehled použitých procesních toků (např. konfigurace, zahájení relace, odeslání dat, odeslání PDU řízení přístupu atd.). Obsahem článku 6.3 jsou sekvenční diagramy jednotlivých toků a jejich popis (stavy, příkazy, odkazy na metody).



Obrázek 3 (obr. 12 normy): Sekvenční diagram zahájení relace

7 Bezpečnostní podsystém: rozhraní a datové typy

Tato kapitola (rozsah 18 stran) popisuje bezpečnostní podsystém (jako jednu z funkčních entit logické architektury) a jednotlivé funkce, které tento systém zajišťuje. Struktura popisu systému v jednotlivých článcích kapitoly je následující:

- Obecný popis funkcí,
- zásady a stavy kontroly přístupu,
- pokročilé ověřování
- rozšířené ověřování
- datové typy,
- rozhraní *Appsec*,
- vnitřní rozhraní podsystému zabezpečení.

V každém z článků je obsažen popis dané funkce, definice, stavy a stavové diagramy, metody, příkazy, použité datové typy, ASN.1 popis datových struktur, odkazy na externí mechanismy zabezpečení nebo šifrování atd.

8 Adaptační vrstva: Rozhraní a datové typy

Tato kapitola (rozsah 8 stran) obsahuje popis protokolu Adaptor Layer (vrstva adaptéru), který je modifikací protokolu *Record Protocol* TLS. Účelem tohoto protokolu je umožnit jednotlivým zabezpečeným relacím přenášet jak aplikační datagramy, tak kontrolní (bezpečnostní) datagramy, které ovlivňují konfiguraci relace. Struktura popisu systému v jednotlivých článcích kapitoly je následující:

- Obecný popis,
- datové typy,
- rozhraní *AppAL,*
- rozhraní *SecAL*

Kapitola obsahuje popis datových typů, základní příkazy služeb a jejich parametry a ASN.1 notaci.

9 Služby zabezpečené relace

Kapitola (rozsah 12 stran) obsahuje popis rozhraní služeb zabezpečení relace. Tyto služby udržují zabezpečený stav pro každou relaci. Struktura popisu systému v jednotlivých článcích kapitoly je následující:

- Obecný popis,
- rozhraní *AppSess*
- rozhraní *Secsess*
- rozhraní *ALSess*
- povolené mechanismy.

Kapitola obsahuje popis datových typů, základní příkazy služeb a jejich parametry a ASN.1 notaci.

Příloha A (informativní) Scénáře užití

Tato příloha popisuje scénáře užití mechanismů zabezpečených relací uvedených v popisovaném dokumentu a vysvětluje, jak lze mechanismy v popisovaném dokumentu použít ke splnění požadavků případů užití.

Příloha B (normativní) ASN.1 modul

Příloha obsahuje pouze odkaz na normu ISO/IEC 8824-1 a odkazy na ASN.1 dle ISO 21177. Modul ASN.1 je vložen formou elektronické přílohy.

© Silmos, s.r.o. 2018 - 2026. *We will help you navigate the field of Transport Telematics and find the right standard.*