ISO/TR 21186-3 - **Kooperativní inteligentní dopravní systémy (C-ITS) – Návod pro používání norem – Část 3: Zabezpečení**

Application Area: Cooperative systems

Publication Year, Number of Pages: Published 2021, 125 pages

Extract Creation Year: 2021

Standard Topic Group: Kooperativní ITS

Standard Topic: Návod pro používání norem

Topic Description: Zabezpečení komunikace

Introduction, Explanation of Starting Points
Metodika návrhu zabezpečení komunikace ITS

Description of Architecture, Hierarchies, Roles, and Object Relationships
"Best practice" zabezpečení přístupu k datům ITS stanicí dle ISO 21177

Description of Process / Function / Method of Use
Uvedení příkladů z praxe (zabezpečení přístupu k datům vozidla při použití protokolu UGP dle ISO 21177)

Description of Interfaces / APIs / System Structure

Protocol / Algorithm / Computation Definition

Definition of Data Representation / Physical Meaning

Definition of Constants / Ranges / Restrictions

Introduction

Norma ISO/TR 21186 je vícedílný dokument, který si klade za cíl poskytnout směrnici pro standardizovaný rozvoj kooperativních systémů a vývoj C-ITS aplikací. První část normy popisuje standardizační aktivity spojené s C-ITS. Druhá část normy ISO/TR 21186 představuje hybridní komunikaci v rámci C-ITS, vysvětluje její koncept a funkce pro tento druh ITS systémů.

Třetí část normy ISO/TR 21186-3 je metodikou či nezávazným pokynem, jak přemýšlet o C-ITS z pohledu zabezpečení komunikace a přístupu k datům a informacím, jež tyto systémy využívají. Tato část dále obsahuje analýzy a doporučení pro zabezpečení aplikací, přístupu a zařízení za použití infrastruktury privátních a veřejných klíčů PKI, přičemž se často odkazuje na návrhy zabezpečení obsažené v ISO/TS 21177

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

Application

Norma obsahuje popis možností zabezpečení komunikace, přístupu k datům a zařízení, dále mechanismy zabezpečení pro různé možné scénáře využití C-ITS a seznamuje s konceptem PKI a procesem vydávání, správy a použití certifikátů pro zabezpečenou komunikaci. Norma může najít využití u odborné veřejnosti, která se seznamuje s kooperativními systémy, má za úkol jejich uvádění do praxe např. z pozice úřadu k tomu jmenovanému, nebo při návrhu konceptu C-ITS systému pro získání širšího pohledu na problematiku jeho implementace.

1. Scope

Tento dokument obsahuje návody pro zajištění zabezpečené komunikace a zabezpečeného přístupu k datům inteligentních dopravních systémů (ITS). Obsahuje také analýzy a osvědčené postupy pro zabezpečené připojení ITS s využitím normy ISO/TS 21177. Poskytuje doporučení pro zabezpečení aplikací, řízení přístupu, zabezpečení zařízení a požadavky na infrastrukturu veřejných klíčů (PKI) pro zajištění zabezpečeného ekosystému ITS.

2. Associated Standards

Originál dokumentu uvádí dvě souvisící normy:

ISO/IEC 27000, Information technology — Security techniques — Information security management — Overview and vocabulary

ISO/IEC 27032, Information technology — Security techniques — Guidelines for cybersecurity

Dále jsou v textu dokumentu zmíněny odkazy na další normy, z nich nejdůležitější týkající se zabezpečení C-ITS jsou:

ČSN ETSI EN 302 637-2 V1.4.1 (87 5173) Inteligentní dopravní systémy (ITS) – Vozidlové komunikace – Základní soubor aplikací – Část 2: Specifikace základní služby kooperativní připravenosti

ČSN ETSI EN 302 637-3 V1.3.1 (87 5173) Inteligentní dopravní systémy (ITS) – Vozidlové komunikace – Základní soubor aplikací – Část 3: Specifikace základní služby decentralizované environmentální notifikace

3. Terms and Definitions

Dokument obsahuje 1 termín či definici.

vektor útoku – *(attack vector)*
zneužití konkrétního známého slabého místo v kódu software pro kybernetický útok na cílový systém např. za účelem získání citlivých dat

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

4. Abbreviations

Kapitola obsahuje 58 zkratek, mezi nejdůležitější patří:

AA	schvalovací orgán *(authorization authority)*
ACL	seznam pro řízení přístupu *(access control list)*
CA	certifikační orgán *(certificate authority)*
CP	certifikační politika, zásady vydávání certifikátů *(certificate policy)*
CRL	seznam odvolaných certifikátů *(certificate revocation list)*
CTL	seznam důvěryhodných certifikátů *(certificate trust list)*
EA	registrační orgán *(enrolment authority)*
HSM	hardwarový bezpečnostní modul *(hardware security module)*
IDX	výměna dat ITS *(ITS data exchange)*
PKI	infrastruktura veřejných klíčů *(public key infrastructure)*
SSP	oprávnění pro konkrétní službu *(service specific permission)*
TLM	správce seznamu důvěryhodných subjektů *(trust list manager)*

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

Kapitola (rozsah 8 stran) poskytuje přehled zabezpečení v rámci C-ITS a zdůvodnění dalších kapitol obsažených v dokumentu. Následuje obecný popis zabezpečení systému ve smyslu ujištění zainteresovaných stran, že jim budou

poskytovány správné informace nezbytné pro dosažení jejich cílů v systému a ubezpečení, že strany, které nejsou autorizovány k obdržení těchto informací, k nim nebudou mít přístup. Norma nicméně nepředepisuje použití konkrétních mechanismů, jak zabezpečení zajistit.

V druhé části jsou stručně a velmi obecně uvedeny různé přístupy ke standardizaci zabezpečení ITS systémů různými standardizačními organizacemi a jimi vydanými normami či směrnicemi, závěr je opět takový, že všechny tyto přístupy konvergují ke stejnému cíli a struktuře.

Třetí část v obecné rovině popisuje mechanismus zabezpečení typů komunikace broadcast a uni/groupcast. Mechanismus je popsán pouze do úrovně, že je potřeba zajistit to, aby informace určená pro konkrétní cíle nebyla dostupná i cíli, pro který určena nebyla.

Čtvrtá část kapitoly se věnuje tématu ověřování zdroje informací využívaných C-ITS aplikacemi jako klíčového mechanismu pro řízení přístupu, tak aby byla poskytnuta jistota příjemci informace (např. příchozí zprávy) že její odesílatel měl specifická oprávnění k jejímu vytvoření. Dále jsou uvedeny dva typy autentizace (ověření): Ověření identity a ověření role v systému. Následuje znázornění různých scénářů komunikace a ověřování informací.

Pátá část popisuje certifikační autoritu a další orgány, které hrají roli v procesu vydávání certifikátů i proces samotný, nicméně opět na velmi obecné úrovni.

V poslední části je pojednáno o tom, co čtenáře čeká v dalších kapitolách.

6 Analýza zabezpečení a kontrola IDX zařízení

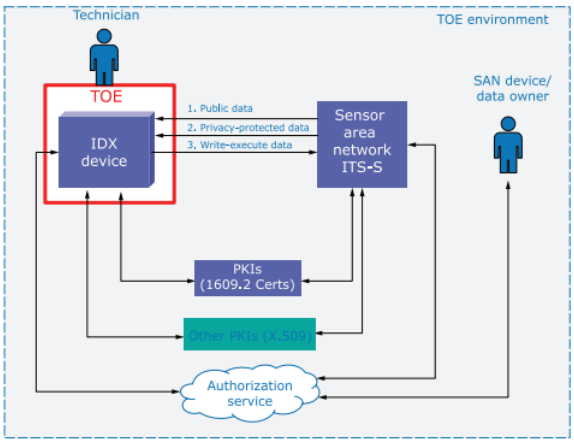
Kapitola o rozsahu 33 stran ve svém úvodu vysvětluje pozadí pro uvedení této kapitoly a to tak, že IDX aplikace je jakákoliv aplikace, která používá unicast komunikaci (spojení pouze s jediným cílem) pro výměnu dat přímo s právě jediným příjemcem. Jako příklady takové komunikace je spojení jednotky RSU s řadičem světelného signalizačního zařízení za účelem vygenerování SPaT zprávy, nebo komunikace vozidla s diagnostickou aplikací.

V další části je zaveden koncept funkce pro tři různé typy IDX zařízení:

- zařízení IDX, na kterých jsou spuštěny veřejné aplikace pracující s daty, kdy přistupující zařízení požaduje data, která následně nemají odkazovat na zařízení poskytující data (*pozn. aut.* složitě vysvětlena anonymizace dat)
- zařízení IDX provozující aplikace pro výměnu soukromých dat, kde přistupující zařízení žádá o data, která mohou následně odkazovat na zařízení, které data poskytnulo
- zařízení IDX s aktivními přístupovými aplikacemi, kdy přistupující zařízení žádá o zápis do hostitelského zařízení nebo o provedení operací na domovském zařízení.

Pro každý typ zařízení je v dokumentu uvedena bezpečnostní analýza v podobě a) hrozeb, b) cílů zabezpečení a za c) funkčních požadavků zabezpečení.

Navržená bezpečnostní analýza je založena na obecném konceptu TOE (cílů vyhodnocení) dle ISO 15408, který je zde blíže popsán, nicméně spíše na „manažerské úrovni“, než že by byl uveden konkrétní postup analýzy. Cílem vyhodnocení dle tohoto konceptu může být jakékoliv zařízení IDX (např. jednotka přistupující k diagnostickým datům vozidla). Prostředí analýzy zabezpečení je znázorněno na obrázku 8 normy.



Obrázek 1 (obrázek 8 normy): Systémový pohled na "cíl vyhodnocení"

Následuje obecný popis, že uživatel by měl k zařízení přistupovat zabezpečeným způsobem (např. TLS při vzdáleném připojení), zařízení by mělo k jinému systému přistupovat zabezpečeným způsobem na úrovni své protokolové sady a zabezpečení by mělo být řízeno infrastrukturou veřejným a privátních klíčů PKI.

Dále kapitola uvádí funkce a aktivity, u nichž se předpokládá, že budou zařízení z pohledu zabezpečení plnit. Tyto funkce jsou popsány formou tabulek, jejichž příklad je uveden na následujícím obrázku:

ID	Activity	Description
General activities (all Scenarios)		
G01	Bootstrap/enrol device into application PKI	The IDX device is bootstrapped and enroled into the PKI that generates such 1609.2 certificates. This activity includes type certification, provisioning with initial key material or random number generation seeds, and (if applicable) registration of the device platform with an appropriate registry.
G02	Download and install IDX device firmware	An IDX device manager downloads/retrieves and installs new IDX device platform firmware.
G03	Download and install IDX device applications	A device manager downloads/retrieves and installs new IDX device applications. These applications are installed on the IDX device for accessing SCN resources; they are not installed on the SCN.
G04	Obtain initial authorization certificates	The IDX device is provisioned with authorization certificate(s) in order to connect with SCN application(s). Scenario 1 authorization certificates do not require sensitive access. It is assumed that they only indicate that a valid IDX device is attached since they are only intended to read public data. Scenarios 2 and 3 authorization certificates are assumed to indicate authorized roles associated with special accesses.
G05	Refresh authorization certificates	The service updates its authorization certificate(s) in order to continue to be able to connect to peer ITS-SUs fronting an SCN.
G06	IDX device is configured with new user and mapped to role	The IDX device ITS-S should not allow all device functions to be available to all users. This can be restricted using roles mapped to permitted activities. Roles are indicated by certificate ITS-AIDs and SSPs associated with those ITS-AIDs. This activity results in an application access policy whereby some user identities are permitted to access certain applications and others are not.

Obrázek 2 (tabulka 1 normy): Příklad provozních funkcí zařízení

Obdobným způsobem jsou uvedeny vlastnosti zařízení z pohledu scénářů jejich použití (přístup k necitlivým datům, přístup k citlivým datům, přístup k funkcím sytému např. zápisu dat, spouštění příkazů), které by zařízení mělo mít, nebo které mají být analýzou zabezpečená vyhodnoceny.

Asset	Description	S1	S2	S3
SCN PII / tracking data / proprietary data	Data originating from the SCN that is privacy-sensitive or required to be privacy-protected. This can include metadata about the SCN owner, data that links the SCN to the owner, tracking-related data, PII/SPII or OEM/vendor-proprietary data. This information has an expectation of confidentiality and should require either a policy or technical control to restrict who has access to it. Regulatory test reports originating from the SCN can fall into this category if they contain data or metadata that is privacy-sensitive. Potentially sensitive to confidentiality, integrity and authenticity lapses.		x	
Writable or executable data	This data asset can include: — Commands or API calls from the IDX device to the SCN that enable writing of sensitive data. — SCN ECU firmware or applications. — Sensitive configuration files/data originating from the IDX device or vendor. This data can include confidentiality sensitivity if it contains vendor-proprietary information.			x
Cloud services trust anchors	Roots of trust for device, application or cloud service vendors that enable the IDX device to trust service endpoints.	x	x	x
Cloud services TLS public keys (incl. certificates)	These are public keys/certificates associated with the IDX device and also associated with the cloud service (e.g. third-party authorization service).	x	x	x
Cloud services TLS private keys	Private keys belonging to the IDX device that can be used to authenticate itself to cloud/vendor services.	x	x	x
IDX device application certificates	1609.2 certificates used by the IDX device to authenticate via ISO/TS 21177 TLS to the SCN ITS-SU.	x	x	x
IDX device application private keys	Private keys (pairwise to the IDX device application certificate public keys) belonging to the IDX device that can be used to authenticate itself to the SCN ITS-SU using ISO/TS 21177.	x	x	x
Application encryption public keys	An entity's application-specific 1609.2 encryption public key, typically embedded in a 1609.2 certificate.			x
Application encryption private keys	The pairwise private key for the encryption public key. This key is not shared/disclosed by the owner. It is used to perform an ECIES encryption over data.			x
SCN ITS-SU application certificates	Certificate(s) presented by the SCN ITS-SU when establishing secure TLS sessions with the IDX device. These certificates and the SCN ITS-SU's private keys can also be used for non-repudiation on transactions/data coming from the SCN ITS-SU.	x	x	x
Revocation information	Information sourced from applicable PKIs that indicates the revocation status of CA and end entity certificates. Can be in the form of CRLs or OCSP-type services/structures.	x	x	x

Obrázek 3 (v originálu nečíslovaná tabulka): Příklad vyhodnocovaných vlastností zařízení

Kapitola dále analogickým způsobem v tabulkách popisuje kategorie hrozeb a vektorů útoku, motivace útočníka, cíle zabezpečení organizační zásady, funkční požadavky zabezpečení, profily ochrany a „hluchá“ místa existujících profilů ochrany (*pozn. aut.:* ovšem bez vysvětlení, o jaké profily se jedná, jsou uvedeny C2CCC HSM PP, V-ITS-S Base a V-ITS-Comms PPs).

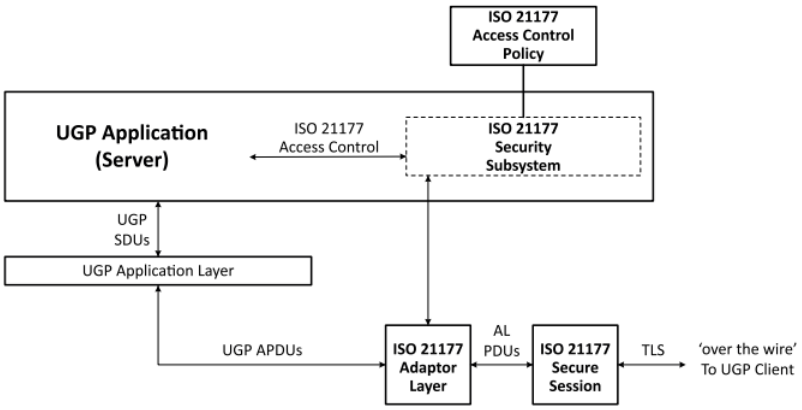
7 Pokyny k zavádění kontroly přístupu dle ISO/TS 21177

Kapitola (rozsah 32 stran) má být dle vlastních slov určena pro vývojáře zařízení a aplikací využívajících řízení přístupu založeného na standardu ISO/TS 21177. Toho má být dosaženo znázorněním případů užití řízení přístupu v automobilovém průmyslu a kroků, při kterých se zařízení pro údržbu a diagnostiku a vozidlo může zabezpečeně navázat komunikaci a zajistit tak řízený přístup dle ISO/TS 21177.

V této kapitole se norma přestává věnovat obecným mechanismům zabezpečení komunikace C-ITS jednotek, ale cílí pouze na zabezpečení přístupu C-ITS jednotky k senzorové a řídicí síti vozidla (SCN). Běžně jsou zde používány zkratky a termíny mimo oblast C-ITS (např. *Unified Gateway Protocol*), vycházející patrně ze souboru norem ISO 13185.

Kapitola obsahuje články o obecné architektuře (protokolu UGP), integraci UGP dle normy ISO 21177, příklad datových struktur zásad řízení přístupu v ASN.1 z normy ISO 21184, řízení přístupu k UGP dle ISO 21177 (formou části ASN.1 specifikace, pravděpodobně převzaté z jiné normy), případy užití řízení přístupu a sekvenční diagramy řízení přístupu (kde je popsán mechanismus TLS).

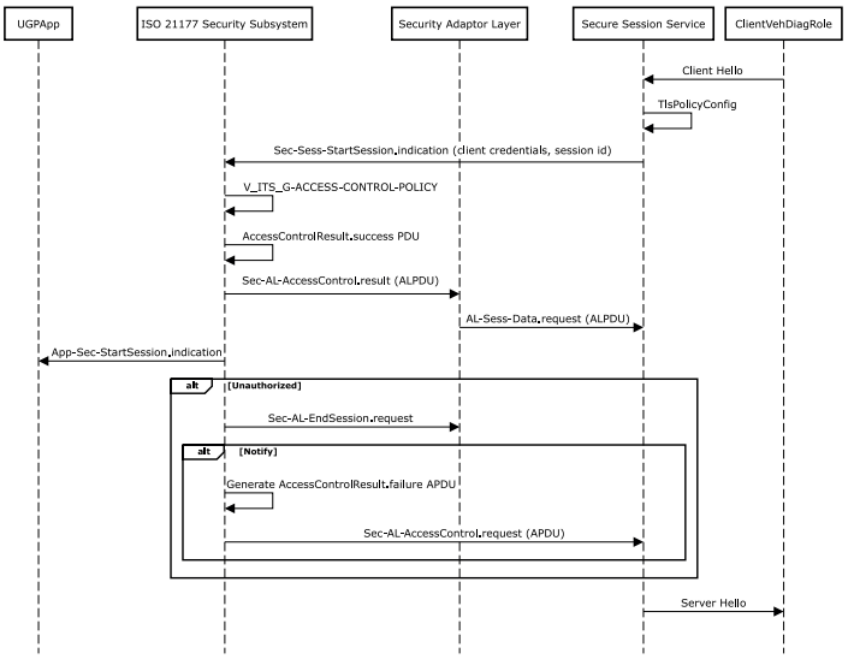
Příklady výstupů v této kapitole jsou znázorněny na následujících obrázcích:



Obrázek 4 (obrázek 15 normy): Integrovaná architektura mezi ISO/TS 21177 a UGP

```
Identifier ::= SNUM32 -- imported from ISO/TS 21184 Annex A.1
Version ::= INTEGER(0..255) -- imported from ISO/TS 21184 Annex A.1
AccessType::= BIT STRING {
    r   (0),
    w   (1),
    x   (2),
    i   (3),
    u   (4)
} (SIZE(5, ...)) -- imported from ISO/TS 21184 Annex A.1

acVersion Version ::= 1

AcConfig ::= SEQUENCE {
    configFile              VisibleString("V_ITS_G-ACCESS-CONTROL-POLICY"),
    configName              VisibleString,
    configVersion           VisibleString,
    role                    SEQUENCE OF ACRole, -- see ISO/TS 21184 Appendix A.3
    entrySet                SEQUENCE OF ACEntrySet,
    tlsPolicyConfig         TlsPolicyConfig, -- Extended from ISO/TS 21184
    ...
}

ACRole ::= SEQUENCE {
    id                      Identifier,
    name                    VisibleStrin,
    serviceMask             ACService,
    entrySetId              Identifier,
    ...
}

ACService ::=  BIT STRING {
    getsupported        (0),
    getvalue          (1),
    setvalue          (2),
    controlvalue        (3),
    getdtcinfo        (4),
    cleardtcinfo        (5),
    enablepassthrough   (6),
    listfile          (7),
    managefile-download (8),
    managefile-upload   (9),
    managefile-delete   (10),
    reset               (11),
    sendMsg             (12),
} (SIZE(14, ...))

ACEntrySet ::= SEQUENCE {
    id      Identifier,
    entry   SEQUENCE OF ACEntry,
```

Obrázek 5: Příklad ASN.1, jež je dle normy zamýšlen jako znázornění struktur k implementaci rámce řízení přístupu v ITS-SU



Obrázek 6 (obrázek 16 normy): Sekvenční diagram zahájení TLS session

Celkově je kapitola z pohledu autora extraktu nic nestandardizuje, pouze uvádí příklady převzaté z jiných norem (ISO 21177, ISO 13185 a ISO 21184).

8 Nedostatky a potřeby v oblasti bezpečnostních požadavků C-ITS CP

Kapitola v rozsahu 15 stran uvádí přehled evropské certifikační politiky v C-ITS, dále hrozby související s infrastrukturou veřejných a privátních klíčů PKI a metody k jejich zmírnění a na závěr analýzu nedostatků (mezer) ve schopnosti PKI podporovat či zabezpečit potřeby nových ITS aplikací a s nimi souvisejícími citlivými daty.

Přehled evropské C-ITS CP je uveden zhruba na jednu stranu a je velmi stručný. Následující analýzy hrozeb a nedostatků jsou uvedeny v tabulkách a vyplňují zbytek kapitoly.

Příloha A (informativní)

Příloha A obsahuje scénáře hrozeb (tabulky obdobné nebo shodné s tabulkami uvedenými v kapitole 6).

Příloha B (informativní)

Příloha B obsahuje tabulky scénářů mapování cílů zabezpečení na funkční požadavky zabezpečení.

Příloha C (informativní)

Příloha C obsahuje informativní návrh na vylepšení ISO/TS 21177:2019: CRL požadavku.

Příloha D (informativní)

Příloha D obsahuje informativní návrh na vylepšení ISO/TS 21177:2019: Vlastnictví a zásady přístupu

Příloha E (informativní)

Příloha E obsahuje informativní návrh na vylepšení ISO/TS 21177:2019: Errata,dodatečný zdůvodňovací materiál a zachování relace při vypršení platnosti certifikátu