FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Nástroj pro opatření certifikátů využívaných při V2X komunikaci
Student:	Adam Weisser
Vedoucí:	Ing. Jiří Dostál, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

Kooperativní inteligentní dopravní systémy (C-ITS) jsou jedním ze způsobů, jak zlepšit a zmodernizovat dopravu ve městech. Jedním z příkladů je přednostní signalizace pro vozidla městské hromadné dopravy na světelných křižovatkách. Pro výměnu informací mezi vozidly a dopravní infrastrukturou je využívána vehicle-to-everything (V2X) komunikace, která musí být bezpečná, důvěryhodná a pseudonymizovaná. Pro dodržení těchto požadavků využívají C-ITS stanice dvou certifikátů, Enrolment Credential a Authorization Ticket, vydávané příslušnou certifikační autoritou a seznamů důvěryhodných a zrušených certifikátů - Certificate trust list/ Certificate revocation list. Cílem práce je vytvořit nástroj, kterým bude možné si o potřebné certifikáty zažádat a zpracovat je.

1) Analyzujte bezpečnostní aspekty V2X komunikace, zaměřte se na práci s certifikáty a PKI.
2) Prozkoumejte funkcionalitu opensource V2X stacku Vanetza.
3) Vytvořte nástroj, který bude schopen pomocí komunikace s PKI získat certifikáty nutné pro podepisování a ověřování V2X zpráv.
4) Nástroj umožní získání: Enrolment credential, Authorization ticket, Certificate trust list, Certificate revocation list.
5) Komunikaci a práci s certifikáty vhodně zobrazte.
6) Výslednou aplikaci otestujte a zdokumentujte.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 3. ledna 2023 v Praze.

Bakalářská práce

NÁSTROJ PRO OPATŘENÍ CERTIFIKÁTŮ VYUŽÍVANÝCH PŘI V2X KOMUNIKACI

Adam Weisser

Fakulta informačních technologií
Katedra počítačových systémů
Vedoucí: Ing. Jiří Dostál, Ph.D.
11. května 2023

Obsah

Seznam obrázků

Chtěl bych poděkovat především vedoucímu práce Ing. Jiřímu Dostálovi, Ph.D. Dále bych rád poděkoval firmě TeskaLabs za poskytnutí testovacího prostředí.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 11. května 2023 .....

Abstrakt

Tato práce se zabývá komunikací vozidel s okolím, V2X, se zaměřením na její bezpečnostní aspekty. Popisuje funkci digitálních certifikátů, které jsou k zabezpečení komunikace použity, a metody, kterými jsou distribuovány. Dále zkoumá aktuální softwarová řešení a jejich bezpečnostní schopnosti. Výsledkem praktické části je aplikace, která si potřebné certifikáty dokáže zažádat od poskytovatele a pracovat s nimi. V rámci vývoje byla provedena implementace potřebných kryptografických algoritmů podle evropských standardů.

Klíčová slova V2X, C-ITS, digitální certifikáty, síťové zabezpečení, C++

Abstract

This thesis deals with vehicle-to-everything communication, V2X, focusing on its security aspects. It describes the function of digital certificates that are used to secure the communication and the methods by which they are distributed. It also examines current software solutions and their security capabilities. The result of the practical part is an application that can request the necessary certificates from the provider and work with them. As part of the development, the necessary cryptographic algorithms were implemented according to European standards.

Keywords V2X, C-ITS, digital certificates, network security, C++

Seznam zkratek

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
CAM	Cooperative Awareness Message
C-ITS	Cooperative ITS
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve DSA
ECIES	Elliptic Curve Integrated Encryption Scheme
ETSI	European Telecommunications Standards Institute
ITS	Intelligent Transport System
ITS-S	ITS Station
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OBU	On-board Unit
PKI	Public Key Infrastructure
RSU	Road-side Unit
V2X	Vehicle-to-everything

Úvod

Kooperativní inteligentní dopravní systémy (C-ITS) jsou jedním ze způsobů, jak zlepšit a zmodernizovat dopravu ve městech. Dovolují vozidlům sdílet informace nejen s dalšími vozidly, ale také s infrastrukturou či osobami, a umožňují tak například informovat o nečekaných událostech či dát přednost vozidlům IZS na světelném signalizačním zařízení. Pro posílání zpráv mezi C-ITS stanicemi se využívá V2X komunikace, která by měla zaručovat důvěryhodnost zpráv a anonymitu subjektů. Těchto vlastností se docílí vybudováním modelu důvěry a použitím několika typů certifikátů.

V současnosti existují nástroje na zajištění těchto certifikátů pouze jako součást komerčních řešení, proto je jedním z cílů práce zanalyzovat bezpečnostní aspekty V2X komunikace se zaměřením na práci s certifikáty a PKI a prozkoumat funkcionality open source knihovny Vanetza. Po této analýze následuje vytvoření nástroje, který bude schopný zajistit certifikáty potřebné pro podepisování a ověřování V2X zpráv, jeho otestování a zdokumentování.

První kapitola práce slouží jako úvod do V2X komunikace obecně, zatímco druhá kapitola je zaměřena na bezpečnostní model. Ve třetí kapitole se práce zabývá návrhem aplikace, jejíž implementace je popsána v kapitole čtvrté.

Kapitola 1

V2X komunikace

Tato kapitola slouží jako úvod do V2X komunikace, popisuje její fungování, standardizaci a současné řešení, nezabývá se však jejím bezpečnostním modelem.

1.1 C-ITS

Inteligentní dopravní systémy (ITS) jsou pokročilé aplikace, které mají za cíl poskytovat inovativní služby týkající se různých druhů dopravy a řízení provozu. Poskytují uživatelům lepší informovanost a umožňují bezpečnější, koordinovanější a „inteligentnější“ používání dopravních sítí [1].

Kooperativními inteligentními dopravními systémy se pak rozumí takové systémy, kde kooperace mezi dvěma a více ITS subsystémy vytváří ITS s vyšší kvalitou a úrovní služeb. Poskytují vozidlům možnost komunikovat s jinými vozidly (vehicle-to-vehicle, V2V), dopravní infrastrukturou (vehicle-to-infrastructure, V2I) či osobami (vehicle-to-person, V2P). Pro takový typ komunikace se využívá označení V2X (vehicle-to-everything) a účastníci této komunikace mezi sebou vytvářejí decentralizovanou síť nazývanou Vehicular Ad Hoc Network (VANET) [2].

Zařízení využívající V2X komunikaci lze rozdělit na on-board unit (OBU), jednotku, která je umístěná ve vozidle, a road side unit (RSU), která je součástí infrastruktury, např. světelné signalizační zařízení.

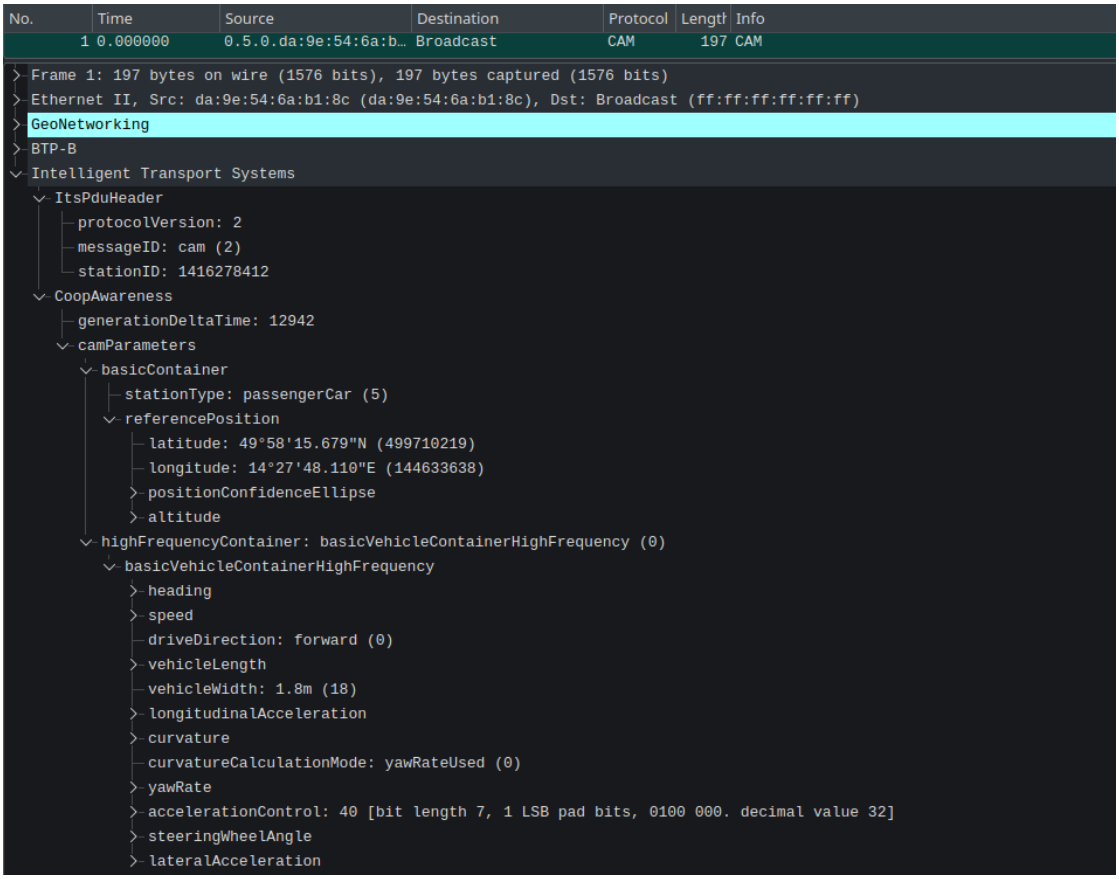
Z hlediska technologie pro přenos V2X zpráv existují dvě hlavní řešení. Prvním je DSRC (Direct Short Range Communication), v Evropě často označováno i jako ITS-G5, které je založeno na IEEE 802.11p WiFi standardu. Další možností je varianta C-V2X (cellular V2X), u které se využívá 4G LTE či 5G. Pro Evropský standard ITS-G5 jsou v tuto chvíli alokována tato frekvenční pásma: 5855-5875 MHz (ITS-G5B), 5875-5905 MHz (ITS-G5A) a 5905-5925 MHz (ITS-G5D). Pásmo ITS-G5A je používáno pro aplikace informující o bezpečnosti provozu, zatímco ITS-G5B pro aplikace, které s bezpečností provozu nesouvisí. Pásmo ITS-G5D je v tuto chvíli rezervováno pro budoucí použití. Každé pásmo je rozděleno na kanály po 10 MHz, které jsou vyhrazené pro různé účely.

1.2 V2X zprávy

Některými z využití V2X komunikace jsou například varování před kolizí, varování před prudkým brzděním, upozornění na blížící se vozidlo IZS nebo platooning – řízení vozidel blízko za sebou za účelem vyšší propustnosti pozemní komunikace a nižší spotřeby paliva. Pro zprostředkování těchto informací jednotky v rámci V2X komunikace posílají různé typy zpráv. Zprávy jsou zakódované podle ASN.1 struktur definovaných v IEEE 1609.2 [3].

1.2.1 CAM

Zprávy typu CAM (Cooperative Awareness Message) jsou periodicky vysílané za účelem vytváření a udržování přehledu o ITS stanicích mezi sebou. Mohou být také využity pro spolupráci vozidel. Obsahují informace o přítomnosti, pozici, pohybu a základních vlastnostech zdrojové ITS-S. Frekvence CAM zpráv vysílaných vozidlem se dynamicky mění podle zahlcení kanálu a rychlosti pohybu vozidla, pohybuje se však mezi 1-10 Hz.



Obrázek 1.1 Příklad zachycené CAM zprávy zobrazené v programu Wireshark

1.2.2 DENM

DENM (Decentralized Environmental Notification Message) zprávy mají za účel informovat ostatní účastníky provozu o nečekaných událostech, které by mohly ovlivnit bezpečnost či podmínky dopravního provozu. Zahrnují informace ohledně nebezpečí nebo neobvyklých podmínkách. DENM zprávy mohou být jednorázové, jako například v případě prudce brzdícího vozidla, nebo přetrvávající, pokud je nebezpečí dlouhodobé, například při namrznuté vozovce. V případě dlouhodobého nebezpečí si ITS stanice v místě nebezpečí zprávu předávají dokud některá ITS-S nedetekuje jeho zmizení.

1.2.3 MAPEM

MAPEM (Map Message) je typ zprávy vysílané RSU s informacemi o geografii silnice. Jednotky v infrastruktuře těmito zprávami mohou vozidlům poskytovat informace o křižovatkách,

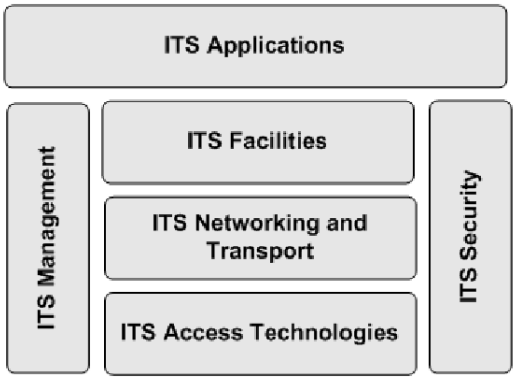
prudkých zatáčkách či jiných úsecích vozovky.

1.2.4 SPATEM

SPATEM (Signal Phase and Timing Message) je dalším typem zprávy, kterou vysílají RSU. Hlavní informací, kterou SPATEM zpráva obsahuje, je stav světelného signalizačního zařízení. Je tak možné optimalizovat rychlost vozidel za účelem zvýšení propustnosti křižovatky.

1.3 Vrstvová architektura ITS-G5

Vrstvová architektura evropského standardu ITS-G5 (na obrázku 1.2) se z velké části drží standardního ISO/OSI modelu, zahrnuje tři horizontální protokolové vrstvy, dvě vertikální protokolové vrstvy a ITS aplikace na vrcholu [4].



Obrázek 1.2 Vrstvová architektura ITS-G5 [4]

Přístupová (access) vrstva odpovídá fyzické a spojové vrstvě klasického modelu a definuje komunikační technologie pro ITS stanice. Na této vrstvě funguje také kontrola zahlcení (Decentralized Congestion Control, DCC), která se stará o ulehčení zahlcení v případech vysoké hustoty provozu.

Síťová a transportní vrstva zahrnuje protokoly pro doručování dat. Příklady takových protokolů jsou IPv6, GeoNetworking (kapitola 1.3.1) či Basic Transport Protocol (BTP, kapitola 1.3.2).

Facilities je vrstva, ve které jsou služby podporující ITS aplikace. Služby se starají o data různých typů a zdrojů a poskytují je aplikacím. Jedna z těchto služeb je například CA (Cooperative Awareness), která se stará o zasílání a přijímání CAM zpráv (viz 1.2.1).

1.3.1 GeoNetworking

GeoNetworking je protokol síťové vrstvy, který zajišťuje routování paketů v ad hoc síti. Dociluje toho pomocí geografických pozicí. Posílané zprávy obsahují geografickou pozici a rozsah, ve kterém jsou relevantní. Jednotky vozidel či infrastruktury v okolí zprávy zachytí a podle informací v nich se rozhodnou, co s nimi dále udělají. Při směrování si každý uzel zjistí svou pozici a cílovou pozici paketu a podle toho určí, kterému uzlu paket pošle dál. GeoNetworking podporuje několik typů komunikace: point-to-point (obdoba unicastu), point-to-multipoint (zpráva je poslána všem v okolí, ti ji opět přepošlou všem v okolí), GeoBroadcast (broadcast v určité geografické pozici) a GeoAnycast (anycast v určité geografické pozici). [4]

1.3.2 Basic Transport Protocol

Hlavním účelem Basic Transport protokolu (BTP) je multiplexování zpráv různých služeb z facilities vrstvy pro přenos pomocí GeoNetworking protokolu. BTP umožňuje protokolům facilities vrstvy přístup k GeoNetworking protokolu a k předávání protocol-control informací mezi facilities vrstvou a GeoNetworking protokolem. Mutliplexování či demultiplexování funguje pomocí portů ITS stanic. Každý port reprezentuje službu ITS ve zdroji či cíli. [5]

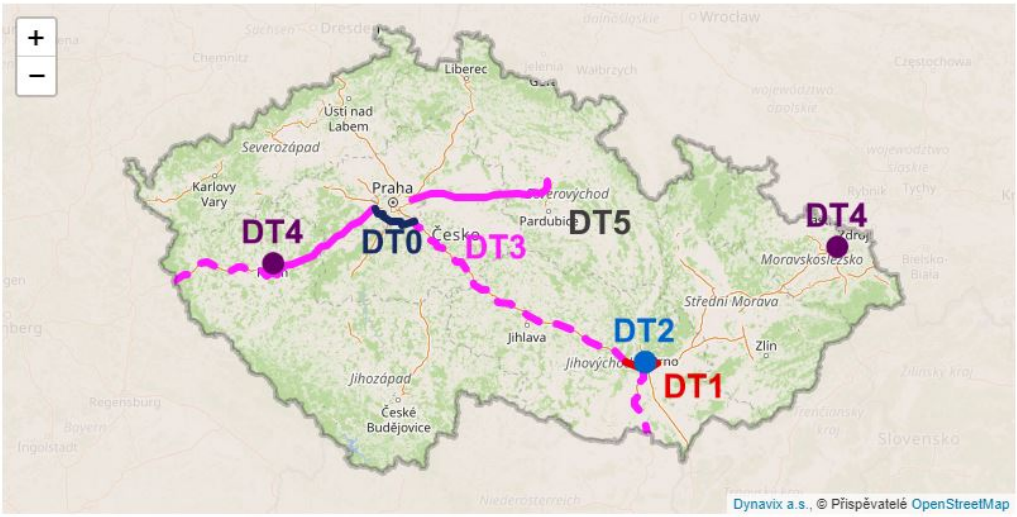
BTP je nenáročný protokol, obsahuje pouze 4 bajtovou hlavičku. Přenos paketů poskytovaný tímto protokolem je nespolehlivý, podobně jako u protokolu UDP. Entity používající protokol s tímto musí počítat.

1.4 Současné využití

V současnosti jsou C-ITS využívány hlavně v testovacích režimech. Ty probíhaly například v německém městě Hamburk (projek BiDiMoves), ve Francii (projekt SCOPP@F) či na cestě mezi Rotterdamem a Vídní (projekt C-ITS Corridor). Existují však i projekty, do kterých je zapojená také Česká republika, jedním z nich je evropský projekt C-Roads.

1.4.1 C-Roads

Platforma C-Roads [6] je společná iniciativa členských států EU a provozovatelů vozovek pro testování a implementaci C-ITS služeb, s ohledem na zajištění interoperability napříč různými zeměmi. Do projektu je zapojeno přes 15 zemí evropské unie, včetně České republiky. Smyslem projektu C-Roads Czech Republic je nasadit a ověřit v praxi na českých silnicích, ve městech, v prostředí městské hromadné dopravy a vybraných železničních přejezdech fungování kooperativních systémů ITS, aby bylo možné v případě potřeby systémy C-ITS doladit tak, aby navazující masové nasazení do ostrého provozu bylo bezproblémové [7].



Obrázek 1.3 Mapa rozmístění C-ITS v projektu C-Roads [7]

Na obrázku 1.3 je vidět pokrytí C-ITS projektu C-Roads v České republice. Jednotlivé úseky jsou:

DT0 Část pražského okruhu (D0) a malé úseky dálnic D1 a D5;

DT1 Okruh kolem Brna;

DT2 Město Brno;

DT3 Dálnice D1, D5, D11 a D52;

DT4 Města Ostrava a Plzeň, zde jde o implementaci C-ITS systémů v rámci veřejnéhromadné dopravy;

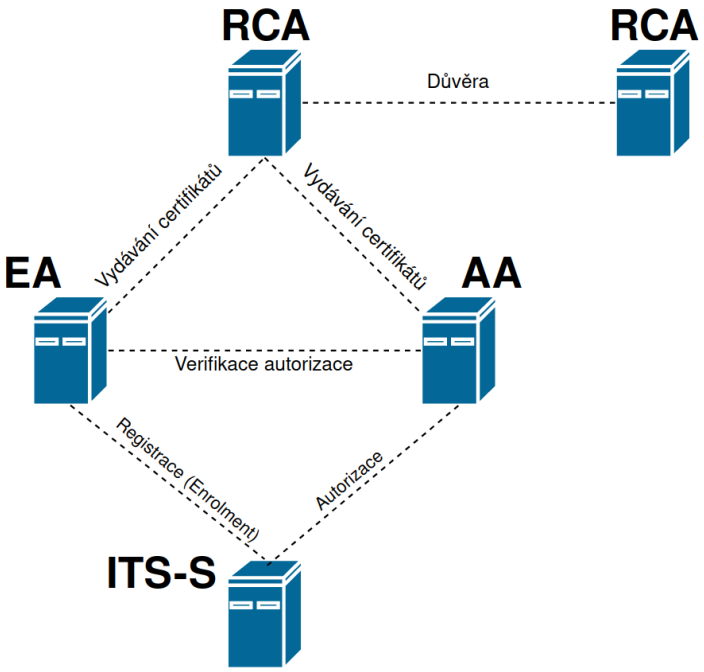
DT5 Železniční přejezdy;

V rámci projektu bylo v těchto lokalitách zabudováno celkem 115 RSU jednotek, jedná se tak o kvalitní základ pro vybudování C-ITS v České republice. Testovací projekt byl však ukončen v roce 2020 a není jisté, zda jsou RSU v tuto chvíli stále aktivní.

Kapitola 2
Bezpečnostní architektura

Tato kapitola se zabývá Public Key infrastrukturou standardizovanou pro V2X komunikaci. Popisuje strukturu PKI i vysokoúrovňové entity pro interoperabilitu více PKI.

Vzledem k tomu, že zprávy uvnitř VANET může posílat jakýkoliv subjekt, vznikají bezpečnostní rizika ve formě zasílání zpráv z falešnými informacemi, sledování uživatelů sítě či útoky typu denial of service. Tyto hrozby by mohly vézt k ohrožení bezpečí na silnicích. Standardy IEEE 1609.2 [3] a ETSI TS 103 097 [8] definují protokoly pro zabezpečení V2X komunikace pomocí asymetrické kryptografie veřejného klíče (PKI). Každá ITS-S, která se chce komunikace zúčastnit, musí být v PKI zaregistrována. Registrace probíhá u kořenové certifikační autority, která má většinou na starosti správu zařízení v určité oblasti. V České republice se o tuto část V2X ekosystému stará Ředitelství silnic a dálnic České republiky [9].



Obrázek 2.1 Schéma PKI

2.1 Struktura PKI

Na vrcholu hierarchie PKI pro V2X komunikaci je kořenová certifikační autorita. Důvěra v tuto autoritu by měla být zaručená a její certifikát je tedy podepsaný sám sebou. Pod kořenovou certifikační autoritou působí dva další typy autorit, registrační autorita (enrolment authority, EA), která ITS-S vydává dlouhodobé certifikáty, a autorizační autorita (authorization authority, AA), která vydává autorizační tikety používané pro podepisování zpráv vysílaných V2X jednotkou. Tyto dvě autority mají certifikát podepsaný kořenovou certifikační autoritou a certifikáty, které vydávají, podepisují svým certifikátem. Vzniká tedy certifikační strom, jehož schéma lze vidět na obrázku 2.1.

2.1.1 Kořenová certifikační autorita

Mezi kořenovou certifikační autoritou (RCA) a ITS-S přímo neprobíhá žádná komunikace, dokonce by ani neměla být připojená k žádné síti a provozována pouze offline. ITS-S by měla získat certifikát kořenové CA, u které je zaregistrovaná, přes zabezpečený komunikační kanál, například při výrobě zařízení. Hlavními úkoly kořenové certifikační autority je vydávat certifikáty pro EA a AA, revokovat tyto certifikáty v případě vypršení platnosti či odcizení soukromých klíčů, vytváření seznamu důvěryhodných a revokovaných certifikátů a další. [10]

Pokud ITS-S má k dispozici certifikát kořenové CA a adresu jejího distribučního centra, může si zažádat o CTL vydávaný touto CA. Tento seznam obsahuje všechny platné certifikáty EA a AA, které pod kořenovou certifikační autoritu patří, a adresu, na kterou se posílají žádosti o certifikáty, které tyto autority vydávají.

Pokud je součástí modelu důvěry více kořenových certifikačních autorit, má kořenová CA možnost distribuovat i seznam těchto autorit, podobně jako to dělá TLM (viz kapitola 2.2.2).

2.1.2 Registrační autorita

Registrační autorita (enrolment authority) ověřuje ITS-S jako celek – potvrzuje, že je ITS-S součástí systému a poskytuje jí registrační certifikát (enrolment credential, EC). Tento certifikát identifikuje autoritu, u které registrace proběhla, a obsahuje pseudonym pro ITS-S, pomocí kterého je možné ověřit identitu ITS-S bez toho, aby byla prozrazena citlivá data [11].

Enrolment credential je certifikát platný delší období, proto bývá často označován jako dlouhodobý certifikát. Po vypršení jeho platnosti je však nutné zažádat o nový, tomuto procesu se říká re-enrolment.

Kontrola, zda ITS-S od registrační autority certifikát získá, probíhá na principu asymetrické kryptografie. Žádost o dlouhodobý certifikát je ITS-S podepsán soukromým klíčem, jehož veřejný protějšek je EA předán při registraci jednotky. EA tak může pomocí veřejného klíče zkontrolovat podpis, a ujistit se, že je zpráva podepsána držitelem soukromého klíče.

Jednou ze součástí zprávy je také nově vygenerovaný verifikační klíč, respektive jeho veřejná část. Ten je autoritou uložen a ITS stanice ho využívá pro podepisování žádostí směrovaných k autorizační autoritě. Také se používá v případě, že jednotka žádá o re-enrolment, namísto kanonického klíče.

Mimo vydávání dlouhodobého certifikátu má registrační autorita na starost také ověření, zda ITS-S je registrována. O takové ověření si zažádá autorizační autorita ve chvíli, kdy si ITS-S zažádá o autorizační tiket pomocí žádosti podepsané dlouhodobým certifikátem vydaným registrační autoritou. Autorizační autorita se tak nedozví skutečnou identitu ITS-S, pouze jestli má jednotka dostatečná oprávnění pro zisk certifikátu, o který žádá.

2.1.3 Autorizační autorita

Jakmile má ITS-S dlouhodobý certifikát, může si zažádat u autorizační autority o autorizační tiket (authorization ticket, AT). Každý autorizační tiket definuje konkrétní povolení, která ITS-S může využít. Příkladem může být vysílání zpráv z určité skupiny, jako je CA (Cooperative Awareness).

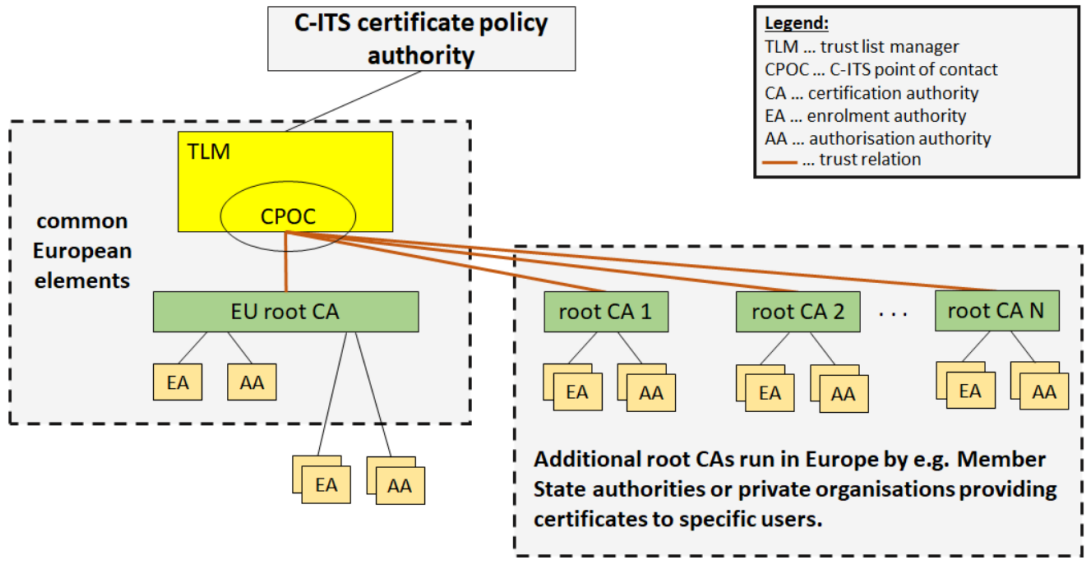
Na rozdíl od dlouhodobých certifikátů vydávaných registrační autoritou nenesou autorizační tikety žádnou informaci o jejím držiteli. Certifikáty tak ITS stanici poskytují soukromí.

Při žádosti o autorizační tiket ITS stanice generuje nový asymetrický klíč, jehož veřejnou část předává autorizační autoritě. Zprávy, které ITS-S chce vysílat jsou podepisovány právě tímto klíčem.

ITS stanice může vlastnit několik autorizačních tiketů zároveň. To je užitečné například v případě, že chce ITS-S vysílat zprávy z více skupin. Pokud tak chce třeba vozidlo integrovaného záchranného systému vysílat klasické zprávy o sdílení své polohy, ale i zprávy upozorňující na pohyb vozidla IZS, uplatní pro to dva rozdílné autorizační tikety.

2.2 Top level trust management

Pro zaručení důvěry mezi ITS-S, jejichž certifikáty jsou podepsány odlišnými kořenovými autoritami a jsou zaregistrovány do odlišných PKI, existují vysokoúrovňové entity, které jsou zodpovědné za zaručení důvěryhodnosti systému jako celku. V Evropě byl z tohoto důvodu Evropskou unií zřízen EU CCMS – European Union C-ITS Security Credential Management System [12]. Ústředními prvky tohoto systému jsou C-ITS Point of Contact (CPOC), Trust List Manager (TLM) a kořenová certifikační autorita evropské unie. Nejvyšší funkci C-ITS systému zastává Policy Authority. Pro schéma viz 2.2.



Obrázek 2.2 Schéma modelu důvěry EU CCMS [12]

V současnosti je v Evropě provozováno takzvané Level 0 prostředí, ve kterém zainteresované subjekty mohou testovat svá PKI řešení. Toto prostředí zahrnuje všechny prvky nutné k provozování CCMS, je však určeno pouze k testování. Datum přechodu na Level 1 prostředí, které by už mělo být v ostrém provozu, zatím není známo.

2.2.1 Policy autorita

Policy autoritou se rozumí složení zástupců veřejných a soukromých subjektů zainteresovaných v účasti na C-ITS modelu důvěry. Takovým subjektem mohou být správní orgány, provozovatelé pozemních komunikací, výrobci vozidel a další [10].

Hlavní zodpovědností Policy autority je jmenování TLM a CPOC provozovaných v C-ITS modelu důvěry. Dále rozhoduje, zda je kořenová certifikační autorita důvěryhodná, a přidává či odebírá kořenové autority z modelu tím, že informuje TLM o schválených a zrušených certifikátech kořenových certifikačních autorit [10].

2.2.2 Trust list manager

TLM vytváří seznam důvěryhodných kořenových certifikačních autorit a podepisuje ho. V Evropě se takto podepsaný seznam nazývá ECTL – European Certificate Trust List [10]. Certifikáty kořenových certifikačních autorit, které TLM získává z CPOC, jsou na základě instrukcí od Policy autority zahrnuty či vyloučeny z ECTL. Certifikáty, kterým vypršela platnost, TLM z ECTL odebírá, aby bylo možné přidat nový certifikát kořenové certifikační autority. Další zodpovědností TLM je podepisování ECTL a jeho distribuce na veřejných webových stránkách CPOC [12].

2.2.3 C-ITS point of contact

Role CPOC spočívá v shromažďování certifikátů kořenových certifikačních autorit v Evropě, distribuci těchto certifikátů Trust list manageru a publikaci European certificate trust listu [12].

CPOC je rozdělen na dvě části:

CPOC Entry funguje jako endpoint CPOC protokolu pro zisk certifikátů kořenových certifikačních autorit;

CPOC Web publikuje ECTL [13] a další související informace jako např. certifikát TLM [14] nebo seznam změn v ECTL;

2.3 ASN.1

Certifikáty a zprávy, které si mezi sebou ITS-S a certifikační autority vyměňují jsou definovány ve formě Abstract Syntax Notation One (ASN.1) struktur. ASN.1 je formát zápisu dat používaný v telekomunikacích, který je nezávislý na programovacím jazyku či platformě [15]. Struktury používané v bezpečnostní vrstvě jsou definovány ve standardech IEEE 1609.2 [3], ETSI TS 103 097 [8] a ETSI TS 102 941 [16]. Zároveň jsou tyto struktury také dostupné z oficiálního repozitáře ETSI [17]. Příklad ASN.1 struktury certifikátu je k vidění na obrázku 2.3. Pro ASN.1 struktury existuje několik formátů kódování, v případě certifikátů a zpráv souvisejících s PKI se využívá formát COER (Canonical Octet Encoding Rules).

```
EtsiTs103097Certificate::= Certificate (WITH COMPONENTS{...,
  toBeSigned (WITH COMPONENTS{...,
    id (WITH COMPONENTS{...,
      linkageData ABSENT,
      binaryId ABSENT
    }),
    certRequestPermissions ABSENT,
    canRequestRollover ABSENT
  })
})
```

Obrázek 2.3 ASN.1 definice certifikátu [17]

Kapitola 3

Návrh aplikace

Tato kapitola se zabývá návrhem aplikace. Popisuje předpoklady a procesy pro zisk certifikátů potřebných pro zabezpečení a anonymizaci V2X zpráv.

3.1 Vanetza

Vanetza [18] je open source knihovna napsaná v C++, která implementuje části ETSI C-ITS protokolů. Konkrétně se jedná například o GeoNetworking, Basic Transport Protocol či Decentralized Congestion Control. Jedná se o výzkumný projekt, který vznikl na Technische Hochschule Ingolstadt.

Knihovna obsahuje několik ukázkových programů, z hlediska bezpečnosti je zajímavý program `certify`, který umožňuje vytvořit vlastní certifikační autoritu a vydat si autorizační tiket. Program je však postavený na zastaralém standardu ETSI TS 103 097 v1.2.1, který se už nepoužívá. Implementace bezpečnostní vrstvy v knihovně dále obsahuje například funkce pro podepisování vysílaných zpráv autorizačním tiketem či ověření platnosti certifikátu, opět se ale jedná o implementace podle starého standardu. Knihovna však obsahuje ASN.1 definice bezpečnostních struktur podle nejnovějších standardů a má je zkompilované do jazyku C.

Celkově knihovna Vanetza implementuje velkou část V2X stacku a její vývoj stále pokračuje, což jí dělá ideálním pro vývoj aplikace.

3.2 Ostatní softwarové implementace

Firma Cohda Wireless [19] má vlastní V2X stack, který provozuje na svých zařízeních. Implementované jsou síťové, facilities a aplikační vrstvy. Podle informací o OBU jednotce [20] od této firmy to nevypadá, že by byla implementovaná část pro zisk certifikátů.

Další firmou nabízející komerční řešení je Commsignia [21]. Jedná se o řešení založené na Linux a operačních systémech reálného času. Podle dostupných informací je součástí řešení část pro práci s certifkáty a komunikaci s PKI.

Jedním z open source řešení je OpenC2X [22]. Jedná se o platformu pro experimentování a prototypování s dopravními síťemi (VANET). Projekt je však již několik let neaktivní a z hlediska bezpečnosti nepodporuje zisk certifikátů.

3.3 Postup získání certifikátů

Prvním krokem je registrace do PKI, pro kterou v tuto chvíli není popsán jednotný postup. V případě registrace do testovací PKI firmy TeskaLabs je přes e-mail zaslán kanonický identifikátor ITS-S, veřejný klíč a typ eliptické křivky, kterou byl klíč vygenerovaný. Následující podkapitoly popisují postup pro zisk dlouhodobého a krátkodobého certifikátu, který je už přesně definovaný v ETSI TS 102 941 [16].

3.3.1 Enrolment Request

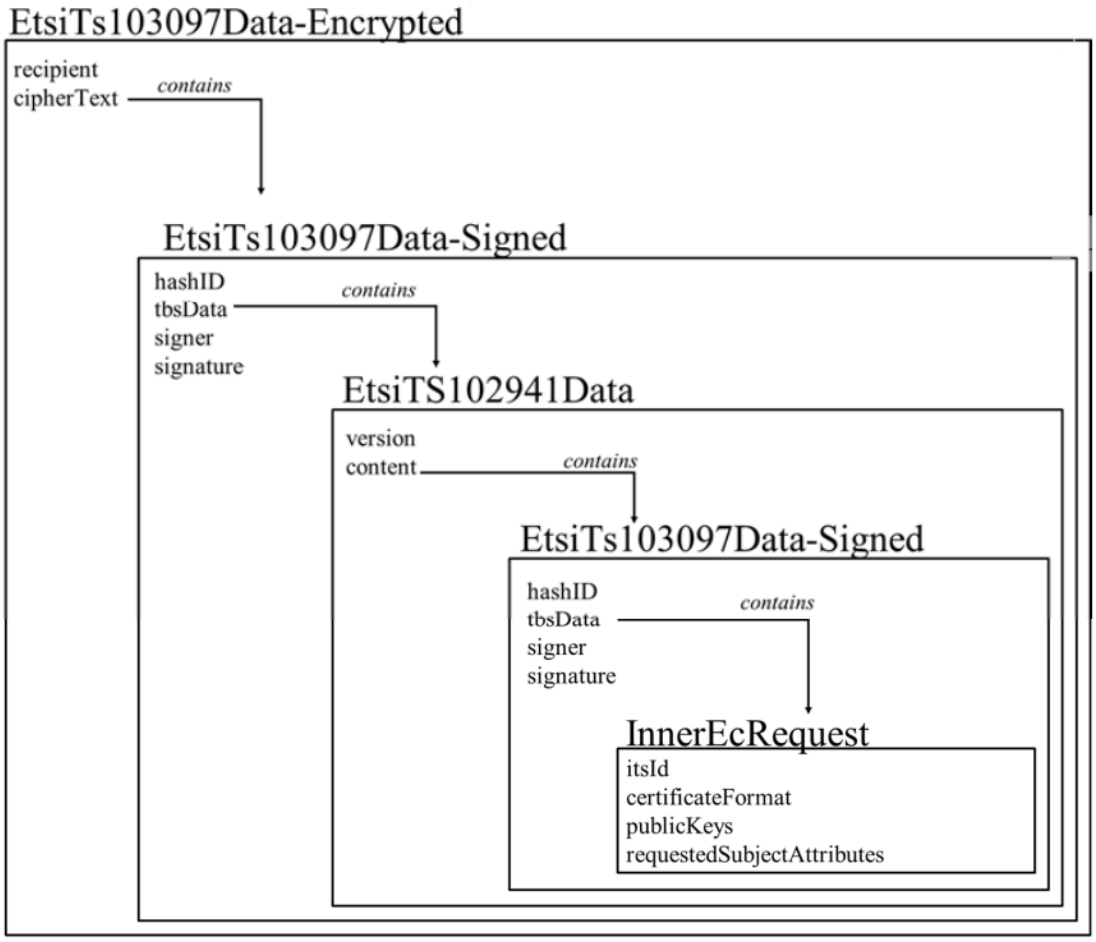
Při žádosti o dlouhodobý certifikát je žádající ITS stanicí vygenerovaný nový asymetrický klíč, takzvaný verifikační klíč. Tento klíč bude sloužit pro ověření totožnosti ITS-S při následných žádostech o autorizační tiket, případně pro re-enrolment.

Následuje vytvoření zprávy typu Enrolment Request, která se skládá ze struktury *InnerEcRequest*, která je dvakrát podepsaná a následně zašifrovaná. Struktura této zprávy je k vidění na obrázku 3.1. *InnerEcRequest* v sobě obsahuje kanonický identifikátor ITS-S stanice, veřejnou část nově vygenerovaného verifikačního klíč a oprávnění, které certifikát může využívat. Oprávnění jsou určena dvojicí PSID (Provider Serice Identifier) a SSP (Service Specific Permissions). V případě dlouhodobého certifikátu jsou oprávnění definována PSID *Secure Certificate Request* (SCR), kterému odpovídá hodnota 623, a SSP bitmapou s hexadecimální hodnotou 0x01C0, kde první bajt určuje verzi SSP, v tomto případě verze 1, a druhý bajt oprávnění, které v rámci SCR může certifikát využívat. Zde se jedná podle ETSI TS 102 941 [16] o bity na pozicích 0 a 1, které dávají certifikátu oprávnění podepisovat zprávy typu Enrolment Request (užitečné pro re-enrolment) a zprávy typu Authorization Request, tedy žádosti o autorizační tiket.

Struktura *InnerEcRequest* je následně podepsána verifikačním klíčem a zabalena do struktury *EtsiTs103097Data-Signed*. Tím si může registrační autorita ověřit, že podepisující opravdu disponuje soukromým verifikačním klíčem, jehož veřejný protějšek je zahrnutý ve zprávě.

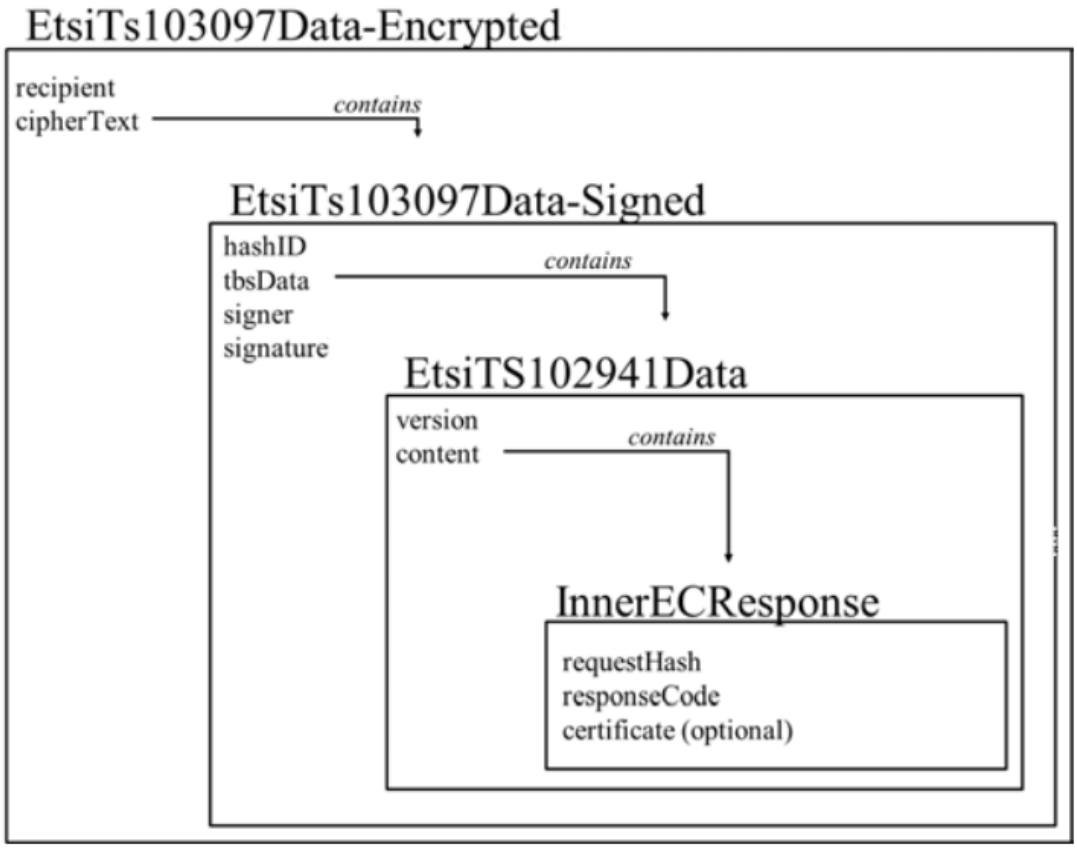
Podepsaná struktura je zabalena do struktury *EtsiTs102941Data*, která je opět podepsána, tentokrát kanonickým klíčem ITS-S a zabalena do struktury *EtsiTs103097Data-Signed*. Toto podepsání slouží registrační autoritě k verifikaci, že zpráva pochází od ITS stanice, za kterou se odesílatel vydává. Veřejný klíč pro ověření podpisu zná EA už od registrace stanice. V případě, že se jedná o občerstvení dlouhodobého certifikátu (re-enrolment), je tato struktura podepsána verifikačním klíčem posledního platného dlouhodobého certifikátu ITS-S.

Následně je zpráva zašifrována. Vnější podepsaná struktura *EtsiTs103097Data-Signed* je podle své ASN.1 definice (viz kapitola 2.3) zakódována do COER formátu. Tato binární reprezentace struktury slouží jako vstup do symetrické šifry AES-128-CCM. Klíč, který byl použitý pro AES, je zašifrovaný pomocí ECIES veřejným klíčem registrační autority. Pro detailnější popis šifrování viz kapitola 3.4.



Obrázek 3.1 Struktura Enrolment Request zprávy [16]

Odpovědí na žádost je zpráva Enrolment Response (obrázek 3.2), skládající se ze struktury *EtsiTs103097Data-Enrypted*, která obsahuje data zašifrované stejným AES klíčem, který byl použit na zašifrování žádosti. Dešifrováním se získá struktura *EtsiTs103097Data-Signed*, která je podepsaná soukromým klíčem registrační autority. ITS-S si tak může ověřit, že zpráva skutečně pochází od požadované EA. Vnitřní struktura *InnerEcResponse* pak zahrnuje prvních 16 bajtů SHA-256 hashe původní Enrolment Request zprávy, což umožňuje ověřit, že odpověď patří k původní žádosti. Dále je zde návratový kód, a pokud odpovídá hodnotě 0, obsahuje odpověď i dlouhodobý certifikát.



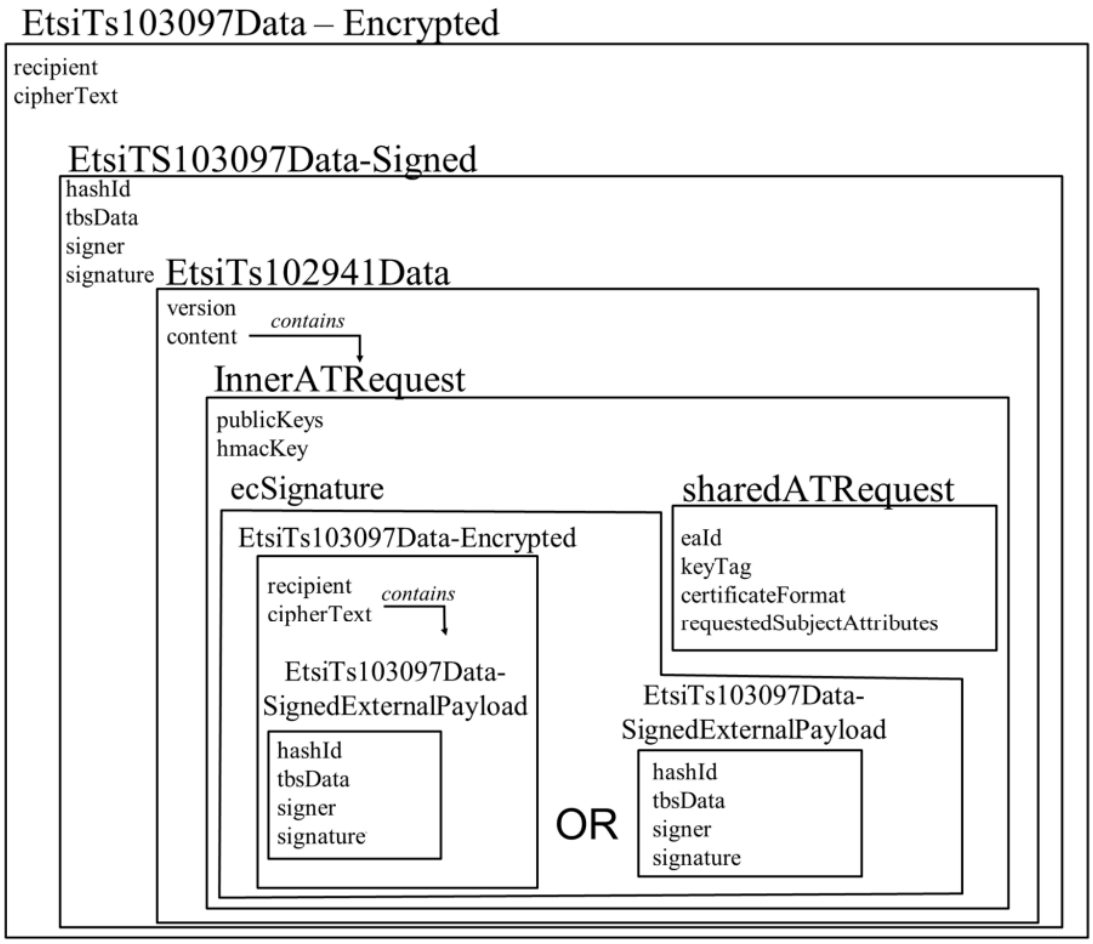
Obrázek 3.2 Struktura Enrolment Response zprávy [16]

3.3.2 Authorization Request

Při tvorbě zprávy Authorization Request (obrázek 3.3) je podobně jako u zprávy Enrolment Request vygenerovaný nový verifikační klíč. Tento klíč bude sloužit pro podepisování zpráv, které chce ITS-S vysílat. Zároveň je možné vygenerovat pro krátkodobý certifikát i tzv. šifrovací klíč. Jedná se o klíč, kterým se pomocí ECIES šifrují odpovědi ITS-S stanici. Použití tohoto klíče není nutné, jelikož je možné odpověď zašifrovat pomocí stejného AES klíče, který byl použitý pro šifrování žádosti, a není nutné tento AES klíč opět posílat ITS-S stanici.

Zároveň je náhodně vygenerován 32 bajtů dlouhý klíč pro HMAC-SHA256 funkci. Touto funkcí je vytvořen MAC zřetězení verifikačního a šifrovacího klíče, který je zkrácený na prvních 128 bitů zleva, tzv. *keyTag*. Tímto je autorizační autorita schopná ověřit ....

Hlavní informace zprávy nese struktura *SharedATRequest*, která obsahuje identifikátor registrační autority, kterou autorizační autorita může kontaktovat pro validaci registrace. Dále obsahuje dříve spočítaný *keyTag* a oprávnění, která ITS-S s autorizačním tiketem může využívat. Tato oprávnění jsou opět definována dvojicí PSID a SSP. Například pro oprávnění vysílat zprávy typu CA (Cooperative Awareness) je definováno PSID 36, jednotlivé bity SSP pak definují specifická oprávnění zasílaných CA zpráv, například jestli se jedná o vozidlo hromadné dopravy.

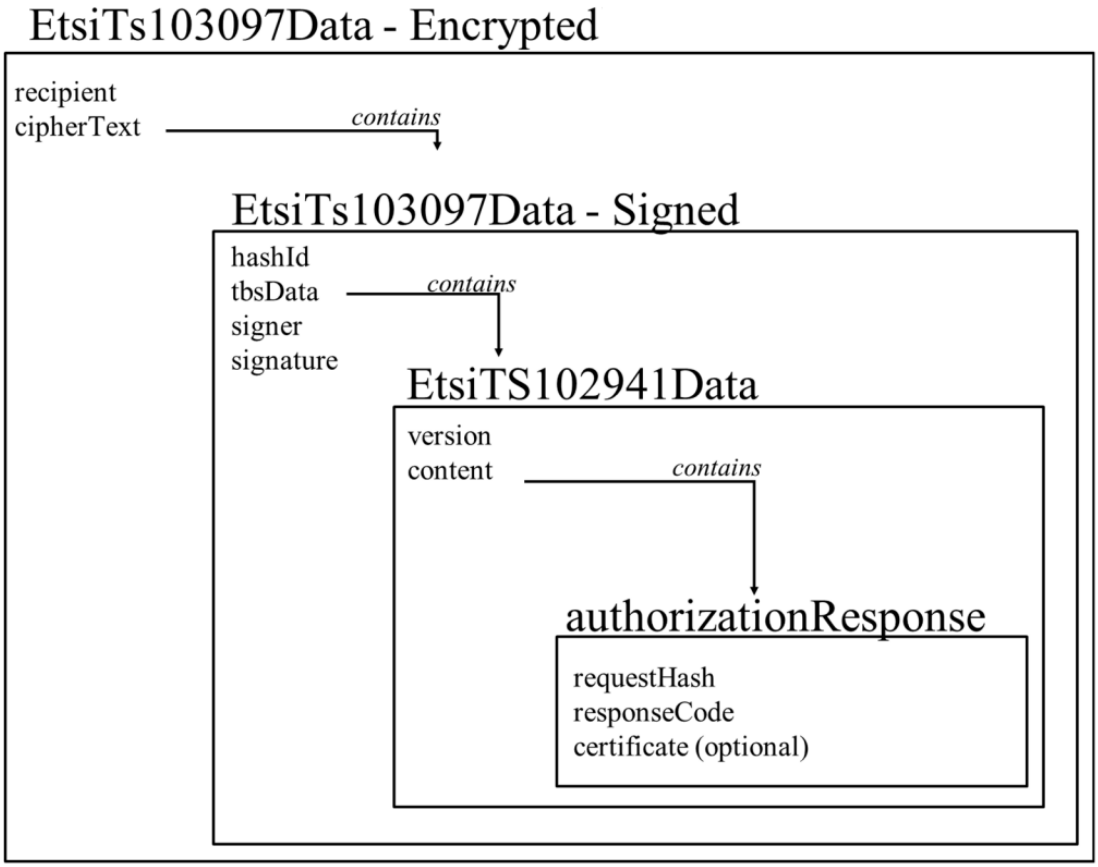


Obrázek 3.3 Struktura Authorization Request zprávy [16]

Hash struktury *SharedATRequest* je následně podepsán verifikačním klíčem dlouhodobého certifikátu a zabalena do struktury *EtsiTs103097Data-SignedExternalPayload*, která je zašifrována (viz kapitola 3.4). Tato struktura *ecSignature* je pomocí ECIES zašifrovaná veřejným klíčem registrační autority, autorizační autorita tedy zprávu rozšifrovat nedokáže a pro verifikaci tak zprávu musí poslat registrační autoritě. Pro jednotky, které nevyžadují soukromí, jako jsou například RSU, není tato část zprávy zašifrovaná.

Struktury *SharedATRequest* a *ecSignature* jsou obě součástí struktury *InnerATRequest*, společně s veřejnou částí nově vygenerovaného verifikačního klíče a klíče použitého k vypočtení HMAC. Tato struktura je zabalena do *EtsiTs103097Data-Signed* struktury a podepsána soukromou částí nově vygenerovaného verifikačního klíče, aby si AA mohla ověřit, že ITS-S soukromý klíč opravdu vlastní. Podepsání této struktury není striktně vyžadováno, ale doporučuje se, jelikož je důležitým bezpečnostním mechanismem pro zaručení důveryhodnosti ITS-S.

EtsiTs103097Data-Signed je následně zabalena do *EtsiTs102941Data* a zašifrována (viz kapitola 3.4). Tentokrát je pro ECIES použitý veřejný klíč autorizační autority.



Obrázek 3.4 Struktura Authorization Response zprávy [16]

Odpovědí na žádost o krátkodobý certifikát je zpráva Authorization Response (obrázek 3.4). Tato struktura je opět zašifrovaná stejným AES klíčem, který byl použit pro šifrování žádosti. Po dešifrování se získá struktura *EtsiTs103097Data-Signed*, která je podepsaná soukromým klíčem autorizační autority. ITS-S si může ověřit, že podpis opravdu pochází od požadované AA. Vnitřní struktura stejně jako u zprávy Enrolment Request obsahuje hash původní žádosti, návratový kód a v případě, že vše proběhlo v pořádku, autorizační tiket.

3.4 Šifrování

Aby se předešlo úniku informací při komunikaci mezi ITS-S a certifikačními autoritami jsou žádosti o dlouhodobé a krátkodobé certifikáty šifrovány. Data, která mají být zašifrována jsou serializována podle své ASN.1 definice do COER formátu. Následně jsou data zašifrována pomocí šifry AES v CCM módu s 128 bitovým klíčem. Postup pro šifrování dat je následující, podle ETSI TS 102 941 [16]:

1. ITS stanicí je náhodně vygenerován AES klíč o délce 16 bajtů;
2. ITS stanicí je náhodně vygenerován inicializační vektor o délce 12 bajtů;
3. Data jsou zašifrována AES-CCM za použití vygenerovaného klíče a inicializačního vektoru, vzniklá šifra je o 16 bajtů delší než nezašifrovaná data, posledních 16 bajtů je autentizační kód (MAC);

Pro dešifrování zprávy je nutné znát AES klíč, ten se tedy musí také zašifrovat a poslat společně se zprávou. Pro zašifrování klíče je použité hybridní šifrovací schéma postavené nad eliptickými křivkami jménem ECIES (Elliptic Curve Integrated Encryption Scheme). ECIES je postaveno na problému Diffie-Hellman a obsahuje následující kryptografická primitiva:

1. Funkce pro odvození klíče, zde Key Derivation Function 2 (KDF2);
2. Funkce pro výpočet MAC, zde HMAC-SHA256;
3. Protokol pro dohodu klíčů, zde Diffie-Hellman s použitím eliptických křivek (ECDH);
4. Symetrická šifra, zde XOR funkce;

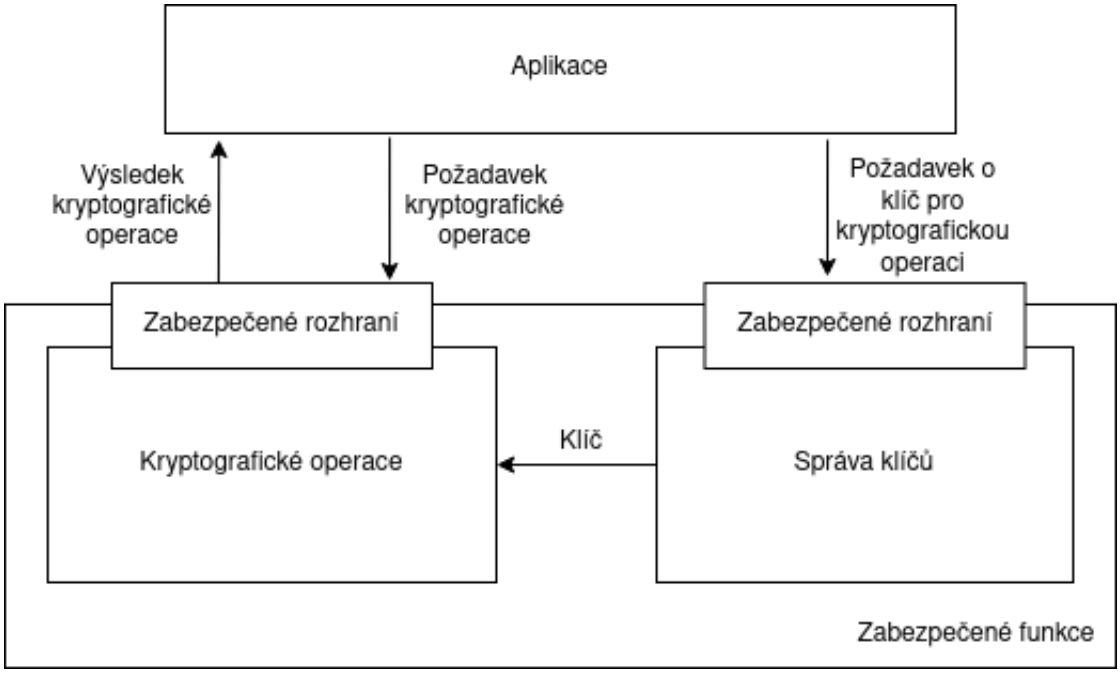
Postup pro zašifrování 16 bajtového AES klíče je následující, podle ETSI TS 102 941 [16] a IEEE 1609.2 [3]:

1. ITS stanicí je vygenerovaná dvojice soukromého a veřejného klíče;
2. Podle ECDH je vypočteno sdílené tajemství z soukromé části vygenerovaného klíče a veřejné části klíče příjemce;
3. Z hodnoty vypočítané v minulém kroku jsou pomocí KDF2 odvozeny dva klíče, první o délce 16 bajtů, druhý o délce 32 bajtů, jako vstupní parametr P1 funkce KDF2 je SHA-256 hash certifikátu, ze kterého ITS-S získala veřejný klíč příjemce;
4. Prvním 16 bajtovým klíčem je pomocí XOR funkce s AES klíčem vypočtena šifra;
5. Druhý klíč je použitý pro vygenerování MAC z šifry, tento MAC je zkrácený na prvních 128 bitů zleva;

Příjemci je ITS stanicí odeslán text zašifrovaný pomocí AES-128-CCM, inicializační vektor AES šifry, AES klíč zašifrovaný ECIES, veřejný klíč vygenerovaný pro ECIES a MAC ECIES šifry.

3.5 Hardware security modul

Pro zabezpečení aplikace se kryptografické operace a správa klíčů má odehrávat v hardware security modulu (HSM), pro schéma viz obrázek 3.5. Vzhledem k tomu, že je aplikace navržena nezávisle na použitém hardware, není možné tento požadavek splnit. Místo toho je pro kryptografické operace využita abstraktní třída `Backend` knihovny Vanetza, pro kterou existují implementace v kryptografických knihovnách Crypto++ a OpenSSL. V případě, že by byl zvolen konkrétní hardware, na kterém aplikace poběží, je možné vytvořit implementaci třídy `Backend`, která bude využívat funkcionality HSM. Aplikace tak v tuto chvíli slouží jako proof of concept využitých technologií.



Obrázek 3.5 Schéma HSM [10]

Kapitola 4
Implementace

V této kapitole je popsáno, jakým způsobem je aplikace implementována.

4.1 Vanetza

Aplikace byla implementována přímo do knihovny Vanetza, konkrétně do části `tools`, která obsahuje různé ukázkové aplikace. Důvodem pro výběr této knihovny je několik. Na rozdíl od většiny V2X stacků je Vanetza zdarma a plně open source. Cílem práce bylo vytvořit nástroj pro zisk certifikátů právě proto, že žádné jiné než komerční řešení v tuto chvíli neexistuje. Zároveň je Vanetza napsaná v jazyku C++, což je výhodné pro případný běh aplikace na embedded zařízení. V neposlední řadě je v knihovně již implementováno mnoho funkcionalit, které vývoj aplikace usnadňují.

4.2 Kryptografické operace

Zprávy posílané za účelem zisku registračních a autorizačních certifikátů využívají několika kryptografických principů k zaručení původu, integrity a zabezpečení dat. Aplikace pro kryptografické operace používá abstraktní třídu `Backend` z namespace `security` knihovny Vanetza, která je v tuto chvíli implementovaná dvěma způsoby, pomocí knihoven Crypto++ a OpenSSL. Díky tomu je možné jednoduše použít i jiné zdroje kryptografických operací, jako je například hardware security modul, vytvořením třídy, která dědí z `security::Backend` a implementuje její abstraktní metody.

4.2.1 Šifrování

Pro šifrování se využívá kombinace symetrické šifry v podobě AES v CCM módu se 128 bitovým klíčem a hybridní šifry ECIES. Odesílatel zprávy nejprve zašifruje zprávu pomocí AES-128-CCM a klíč, kterým tuto zprávu zašifroval, následně zašifruje veřejným klíčem příjemce pomocí ECIES. Knihovna Vanetza v současnosti takové šifrování neumožňuje, do knihovny tedy byla tato funkcionalita přidána.

Doplnění AES-128-CCM do knihovny je pomocí Crypto++ i OpenSSL poměrně přímočaré, obě tyto knihovny mají šifru implementovanou. Pomocí generátoru pseudonáhodných čísel se vygeneruje AES klíč o délce 16 bajtů a inicializační vektor o délce 12 bajtů. Těmito parametry se zinicializuje šifra, definuje se délka ověřovacího kódu a nešifrované zprávy a následně se data zašifrují. Tato šifra byla do knihovny Vanetza implementována v Crypto++ i OpenSSL, dá se

zavolat pomocí metody `encrypt_aes()` třídy `Backend`. Vstupem je struktura, kterou chceme zašifrovat, zakódovaná podle ASN.1 ve formátu COER, výstupem je vygenerovaný AES klíč, inicializační vektor a zašifrovaná data.

Pro ECIES neexistuje v OpenSSL přímo implementace, je tedy nutné spojit dohromady všechna kryptografická primitiva, která ECIES využívá. V Crypto++ je pro šifrování pomocí ECIES třída, ta však při derivaci klíče generuje pouze 32 bajtů dlouhou hodnotu. Podle ETSI TS 102 941 [16] je žádaný výstup funkce pro odvození klíče dlouhý 48 bajtů, kde prvních 16 bajtů je klíčem pro zašifrování AES klíče a následujících 32 bajtů klíčem pro vytvoření MAC zašifrované zprávy. Šifra byla přepsána tak, aby tyto požadavky reflektovala. Nejprve se vygeneruje soukromý klíč a k němu přidružený veřejný klíč. Z vygenerovaného soukromého klíče a veřejného klíče příjemce se odvodí společná hodnota pomocí ECDH. Přes funkci pro odvozování klíčů KDF2 se vypočtou symetrické klíče, které se následně použijí pro šifrování a výpočet MAC. Tato šifra byla do knihovny Vanetza implementována v Crypto++, dá se zavolat pomocí metody `encrypt_ecies()` třídy `BackendCryptoPP`. Vstupem je AES klíč využitý pro zašifrování dat, veřejný klíč příjemce a parametr P1, který je SHA-256 hash certifikátu, ze kterého veřejný klíč pochází, zakódovaný pomocí ASN.1 ve formátu COER. Výstupem je vygenerovaný veřejný klíč (ephemeral public key), zašifrovaný AES klíč a MAC zašifrované zprávy, zkrácený na prvních 128 bitů zleva.

4.2.2 Podepisování

Pro podepisování dat a ověřování podpisů obsahuje Vanetza implementaci ECDSA s hašováním pomocí SHA-256, kterou je možné vytvořit digitální podpis na 256 bitové eliptické křivce. Tento algoritmus je v knihovně Vanetza implementovaný jak v Crypto++, tak i v OpenSSL.

4.2.3 Hašování

Vzhledem k tomu, že některé certifikáty využívají 384-bitové eliptické křivky, je nutné k výpočtu jejich hashe použít funkci SHA-384 místo SHA-256. Vanetza podporuje výpočet hashe z dat pouze pomocí SHA-256, proto byla do knihovny přidána funkce `calculate_sha384_digest()`, která umožňuje výpočet jak pomocí Crypto++, tak i OpenSSL.

4.3 Komunikace s PKI

Žádosti jsou na server poskytovatele PKI odesílané pomocí protokolu HTTP1/1. Pro tento účel byla použita C++ knihovna cpr [23], která je wrapper pro C knihovnu curl [24].

Žádost o krátkodobý či dlouhodobý certifikát je posílána pomocí HTTP metody POST. V hlavičce metody má pole Content-Type hodnotu `application/x-its-request`. Posílaná data jsou zakódována v COER formátu podle ASN.1 definice zprávy. Adresa, na kterou je žádost posílaná, závisí na typu žádosti, pro registraci a autorizaci existují odlišné adresy.

Při žádosti o seznam důvěryhodných certifikátů od kořenové certifikační autority je posílaná HTTP GET metoda na adresu distribučního centra PKI. Adresa je doplněna o identifikátor kořenové certifikační autority. Volitelně lze k adrese připojit i sekvenční číslo, které indikuje poslední CTL, který má ITS-S k dispozici. V takovém případě je ITS-S poskytnutý takzvaný delta CTL obsahující informace o změnách, které v seznamu proběhly.

Seznam důvěryhodných certifikátů si ITS-S může zažádata i od evropského TLM. V takovém případě ITS-S posílá HTTP GET request na adresu definovanou v C-ITS Point of Contact protokolu [12]. I zde je možnost zažádat si pomocí sekvenčního čísla o delta ECTL.

4.4 Testování

Pro ověření funkčnosti aplikace bylo firmou TeskaLabs [25] poskytnuto testovací prostředí *Open C-ITS & C-V2X Test PKI*, které implementuje PKI podle standardů ETSI TS 103 097 v1.3.1 [8] a ETSI TS 102 941 [16]. Do PKI byla registrována dvě zařízení.

4.4.1 Šifrování

Zpráva typu Enrolment Request, která byla zašifrována ITS-S podle postupu v kapitole 3.4, byla odeslána na adresu registrační autority testovacího prostředí. Jako odpověď od registrační autority přišla zpráva obsahující SHA-256 hash AES klíče použitého k zašifrování zprávy pomocí AES-128-CCM. Hash se shodoval s hashem vypočítaným nad stejným AES klíčem lokálně. Zašifrovaná data, které zpráva obsahovala, byly následně úspěšně dešifrovány AES-128-CCM za pomocí stejného klíče, kterým byla šifrovaná žádost, a inicializačního vektoru, který byl také součástí zprávy. MAC na konci zašifrované zprávy byl také úspěšně ověřen. Příklad hexadecimální podoby takové zprávy je na obrázku 4.1.

```
03 82 01 01 82 9b 66 15 99 ad 60 e4 70 80 82 45 95 86 01 0c 08 d2 e4 a0 dc 67 19 b5 48 25 0c db 38 e7 39 8e 29 6d f3 54
77 11 03 56 f9 7b 11 6a 7a 87 cc 6d 61 dd 35 92 ba 2e 29 0e ec 90 86 7c 31 10 79 61 68 2e f0 04 fc 1d a5 48 ba 06 2f 80
ff 5d ca 4e eb a1 68 04 b8 76 b9 96 82 01 37 c0 b1 61 95 de 06 b3 ca cf b4 1b 86 2b 50 30 1f 31 91 61 c1 f6 8b b8 09 93
16 65 1a 61 8a 27 90 ca d9 4f 8b 74 77 0b 60 55 7e fe 36 8a 2d c8 14 1f 63 52 36 d6 f6 57 3e 71 8c cd aa bd 6b 1c 36 91
28 af 16 a3 ac a2 1d 21 a6 39 76 ba a4 4f 25 dd e0 bf b7 bd 10 26 d0 26 17 44 da f8 dd d0 80 a9 7b 49 00 1c d8 6a 2d ff
b4 82 95 9e 45 18 cf 23 76 f0 74 be 5b 61 23 f4 26 7e 44 22 f4 5d a4 6c 80 f6 54 31 82 4d cc 1b cf 84 8d 05 a7 56 f1 84
12 6d 2d 78 f7 e1 f0 69 16 0a ae c5 9e ba 3d 4a 69 47 64 39 98 9e 7d ce 73 b5 f6 d3 56 99 b0 e0 dc 94 ea 8d 0b 25 99 92
52 c7 dd 8f ac 83 8e ac 3c 7b a4 89 4a be 90 fc 7f 93 0a 84 30 88 4c 6c be 21 bb 61 59 fc b3 a9 77 a6 a4 f6 ab 0f 17 9e
81 3f 76 87 10 a7 d0 5f 54 e5 d1 df f5 a3 97 3d 72 29 28 aa a4 d3 7c b2 71 5e ef bd 17 f3 48 b6 40 f5 14 1a 90 8b b5 f2
96 b3 64 64 7c 1d 5b 03 8c 81 e6 bd d4 40 15 29 4c 22 fd b5 10 28 c0 ff 77 63 1b 52 1e a4 b7 2e 1c ce ec 74 b5 95 b5 08
43 f7 98 9c d3 42
```

Obrázek 4.1 Příklad zprávy typu Enrolment Request zakódované podle ASN.1 do formátu COER

Proběhl i test, ve kterém byl do žádosti umístěn jiný AES klíč, než kterým byla data zašifrována. V tomto případě byl součástí odpovědi od serveru hash odlišný od hashe AES klíče použitého k šifrování. K zašifrovaní dat odpovědi byl použit neznámý AES klíč a data nebylo možné dešifrovat. Návratový kód zprávy je *decryptionfailed*.

Podobného výsledku bylo dosaženo i v případě, kdy byl zašifrován správný AES klíč, ovšem pro ECIES byl použit odlišný klíč než veřejný klíč registrační autority. Opět bylo nemožné data dešifrovat, protože byl pro šifrování použit neznámý AES klíč, a návratový kód byl opět *decryptionfailed*.

Obě kryptografické operace používané pro šifrování byly také ověřeny pomocí testovacích vektorů definovaných ve standardu IEEE 1609.2 [3].

4.4.2 Podepisování

Pro testování podpisů byla opět na adresu registrační autority testovacího prostředí odeslána zpráva Enrolment Request. Po úspěšném dešifrování zprávy server také úspěšně ověřil oba podpisy, které zpráva obsahovala.

Byl proveden test, při kterém byla na server odeslaná žádost Enrolment Request, jejíž vnější *EtsiTs103097Data-Signed* struktura byla podepsaná jiným klíčem, než je veřejný klíč registrační autority. V takovém případě obsahovala odpověď od serveru návratový kód *invalidsignature*. Stejný výsledek získáme i v případě, že je vnitřní *EtsiTs103097Data-Signed* struktura podepsaná jiným klíčem, než který se v žádosti odesílá jako verifikační.

4.4.3 Zisk certifikátů

I přesto, že implementace proběhla podle standardů ETSI TS 102 941 [16], ETSI TS 103 097 [8] a IEEE 1609.2 [3], a že bylo úspěšně implementováno šifrování a podepisování dat, se nepovedlo od serveru získat dlouhodobý certifikát a v důsledku toho ani autorizační tiket. Návratový kód odpovědi na žádost o certifikát od serveru je *deniedrequest*. Pro tento návratový kód není blíže specifikováno, z jakého důvodu byla žádost zamítnuta.

Bez hlubšího porozumění vnitřní implementace PKI je odladění této chyby složité. Byly provedeny pokusy, při kterých byly části žádosti upraveny tak, aby vyvolaly určité chyby. Myšlenka za tímto pokusem byla identifikace části, ve které zpracování žádosti chybuje. Neexistuje však standard, který by určoval přesné pořadí, ve kterém se má žádost zpracovávat, proto i tento přístup nebyl úspěšný.

4.4.4 ECTL

Při žádosti o seznam platných certifikátů v evropském Level 0 prostředí bylo ověřeno, že certifikáty, které ITS-S získala, odpovídají certifikátům uvedeným v zápisu L0 CPOC-WEB Logbook [26].

4.5 Reálné využití

Aplikace v tuto chvíli není vhodná pro reálné nasazení do provozu. To vychází z faktu, že není uzpůsobená přímo na žádný hardware, přičemž generace klíčů musí probíhat v HSM. Aplikace je však navržena tak, aby implementace pro specifický hardware byla co nejjednodušší. Dalším nesplněným požadavkem pro nasazení je, že bezpečnostní stack pro C-ITS musí být v České republice ověřený na ETSI plugtestu.

Závěr

Cílem práce bylo zanalyzovat bezpečnostní aspekty V2X komunikace s důrazem na PKI a práci s certifikáty a vytvořit aplikaci, pomocí které se certifikáty pro V2X komunikaci dají získat.

Práce poskytuje úvod do technologie V2X komunikace a detailně popisuje architekturu PKI kooperativních inteligentních dopravních systémů, od nejvyšších řídících subjektů až po samostatná vozidla. Jsou uvedeny evropské standardy v oblasti. V práci je dále popsaná open-source knihovna pro V2X komunikaci Vanetza, její bezpečnostní schopnosti a její alternativy. Za pomocí této knihovny byla vytvořena aplikace *v2cat* (V2X Certificate Acquisition Tool).

Aplikace umožňuje vyžádat si seznam platných či anulovaných certifikátů od evropského TLM nebo distribučního centra kořenové certifikační autority. Naopak kvůli chybě, kterou se nepovedlo objasnit, neumožňuje zisk dlouhodobého a krátkodobého certifikátu. Pro kryptografické operace používané při vytváření žádostí o certifikáty a zpracovávání jejich odpovědí byly do knihovny přidány implementace v knihovnách Crypto++ a OpenSSL. Aplikace je zároveň navržena tak, aby umožňovala jednoduchou integraci dalších kryptografických nástrojů, kterým může být například hardware security modul. Získané certifikáty jsou rozčleněné do struktur podle ASN.1 definic, je tedy možné s nimi v knihovně Vanetza dále pracovat, případně je exportovat v COER formátu.

Zdrojový kód aplikace a změny v knihovně Vanetza jsou uloženy v online verzovacím systému Github jako fork knihovny Vanetza. V budoucnu je možné kontaktovat správce knihovny a domluvit se na začlenění kódu. Při úzké spolupráci s poskytovatelem PKI by bylo možné odladit chybu, která zabraňuje zisku certifikátů. Případně by bylo prospěšné pro tyto účely vytvořit otevřenou implementaci PKI. Aplikace v tuto chvíli nepodporuje podepisování zpráv pomocí HSM, existuje tedy možnost v budoucnu tuto podporu pro konkrétní hardware přidat.

Příloha A

Kompilace

Vanetza pro kompilaci využívá nástroj CMake, minimální požadovaná verze tohoto nástroje je 3.12. Knihovna má tři externí závislosti: Boost [27] (verze 3.12 a výše), GeographicLib [28] (verze 1.37 a výše) a Crypto++ [29] (verze 5.6.1 a výše).

Knihovny Vanetza společně s aplikací v2cat se zkompilují pomocí následujících příkazů. Předpokládá se, že se uživatel nachází ve složce knihovny Vanetza a že má k dispozici výše popsané knihovny, na kterých Vanetza závisí.

```
mkdir build && cd build
cmake -DBUILD_V2CAT=ON ..
make
```

Ve složce `build/bin` by se měla nacházet zkompilovaná aplikace v2cat.

Příloha B

Použití

Pro různé funkce aplikace lze využít několika přepínačů. Následuje jejich popis.

Vyžádání evropského seznamu důvěryhodných certifikátů (ECTL) od evropského TLM je možné příkazem:

```
./v2cat --ectl
```

Aplikace si zažádá o ECTL, a pokud se jí vrátí odpověď zpracuje jí. Při žádosti o CTL od TLM jsou v odpovědi zaslány kořenové certifikační autority a jejich distribuční centra. Do konzole je po provedení příkazu vypsán hash, jméno a URL distribučního centra každého certifikátu, který CTL obsahoval.

Pro vyžádání CTL od kořenové certifikační autority je nutné specifikovat cestu k certifikátu kořenové certifikační autority a URL jejího distribučního centra. V případě testovacího prostředí je certifikát kořenové certifikační autority uložen ve složce `certs`. URL distribučního centra je *https://via.teskalabs.com/cits-otenv/v1.3/dc/*. Příkaz pro zažádání CTL by tak mohl vypadat takto:

```
./v2cat --ctl --cert certs/RCA \
              --dc https://via.teskalabs.com/cits-otenv/v1.3/dc
```

Aplikace si zažádá o CTL od kořenové certifikační autority a zpracuje odpověď. Při žádosti o CTL od kořenové certifikační autority jsou v odpovědi zaslány certifikáty a URL všech registračních a autorizačních autorit, které jsou pod kořenovou certifikační autoritou aktivní. Výstupem příkazu je hash a URL distribučního centra kořenové certifikační autority, stejně tak jako URL všech registračních a autorizačních autorit.

V případě žádosti o dlouhodobý certifikát se dá použít přepínač `--enrol`. Zároveň je nutné specifikovat certifikát kořenové certifikační autority, pod kterou spadá registrační autorita, URL jejího distribučního centra, kanonický identifikátor ITS-S a kanonický soukromý klíč ITS-S. Soukromý klíč pro ITS-S, která je v testovacím prostředí zaregistrována pod ID *HYPEX-H1319A102-A0400157*, je zahrnuta ve složce `certs`. Příkaz pro žádost o enrolment credential od testovacího prostředí by tak vypadal takto:

```
./v2cat --enrol --cert certs/RCA \
                --dc https://via.teskalabs.com/cits-otenv/v1.3/dc \
                --canonkey certs/privkey \
                --id "HYPEX-H1319A102-A0400157"
```

Aplikace pošle zprávu Enrolment Request na server a zpracuje odpověď. Pro tento účel si nejdřív od distribučního centra kořenové certifikační autority zažádá o certifikát EA a URL pro enrolment. V případě, že je odpověď v pořádku, uloží aplikace dlouhodobý certifikát pod jménem

EnrolmentCredential. Zároveň je uložen i verifikační klíč, který byl pro certifikát vygenerován, pod jménem ECVerificationKey.

Pro žádost o krátkodobý certifikát existuje přepínač `--authorize`. Je nezbytné opět specifikovat certifikát kořenové certifikační autority, URL distribučního centra, dlouhodobý certifikát a verifikační klíč. Po úspěšném provedení minulého příkazu je tak možné zažádat o autorizační tiket takto:

```
./v2cat --authorize --cert certs/RCA \
                    --dc https://via.teskalabs.com/cits-otenv/v1.3/dc \
                    --verkey ECVerificationKey \
                    --ec EnrolmentCredential
```

Pokud je žádost úspěšná je autorizační tiket uložen pod jménem AuthorizationTicket a verifikační klíč, který byl pro certifikát vygenerován je uložen pod jménem ATVerificationKey.

Poslední tři kroky lze také skloubit do jednoho. Pomocí přepínače `--full` se provede popořadě žádost o CTL od kořenové certifikační autority, žádost o dlouhodobý certifikát a žádost o autorizační tiket. Opět jsou uloženy všechny vzniklé klíče a certifikáty.

```
./v2cat --full --cert certs/RCA \
               --dc https://via.teskalabs.com/cits-otenv/v1.3/dc \
               --canonkey certs/privkey \
               --id "HYPEX-H1319A102-A0400157"
```

Bibliografie

1. EUROPEAN PARLIAMENT. *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance.* 2010. Dostupné také z: https://eur-lex.europa.eu/eli/dir/2010/40/oj.
2. REHMAN, Sabih; KHAN, M. Arif; ZIA, Tanveer; ZHENG, Lihong. Vehicular ad-Hoc networks (VANETs)—An overview and challenges. *Journal of Wireless Networking and Communications*. 2013, roč. 3, s. 29–38. Dostupné z DOI: 10.5923/j.jwnc.20130303.02.
3. IEEE 1609.2-2022. *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Application and Management Messages* [online]. 2022. [cit. 2023-04-28]. Dostupné z: https://standards.ieee.org/ieee/1609.2/10258/.
4. ETSI EN 302 636-3 V1.2.1. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture* [online]. 2014. [cit. 2023-05-03]. Dostupné z: https://www.etsi.org/deliver/etsi_en/302600_302699/30263603/01.02.01_60/en_30263603v010201p.pdf.
5. ETSI EN 302 636-5-1 V2.1.0. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol* [online]. 2017. [cit. 2023-04-20]. Dostupné z: https://www.etsi.org/deliver/etsi_en/302600_302699/3026360501/02.01.00_20/en_3026360501v020100a.pdf.
6. C-ROADS. *C-Roads Czech Republic* [online]. [cit. 2023-04-29]. Dostupné z: https://www.c-roads.eu/pilots/core-members/czech-republic/Partner/project/show/c-roads-czech-republic.html.
7. MINISTERSTVO DOPRAVY ČESKÉ REPUBLIKY. *C-Roads* [online]. [cit. 2023-04-29]. Dostupné z: https://www.its-knihovna.cz/cz/knihovna/projekty/c-roads.
8. ETSI TS 103 097 V2.1.1. *Intelligent Transport Systems (ITS); Security; Security header and certificate formats* [online]. 2021. [cit. 2023-04-28]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/02.01.01_60/ts_103097v020101p.pdf.
9. ŘEDITELSTVÍ SILNIC A DÁLNIC ČESKÉ REPUBLIKY. *C-ITS* [online]. [cit. 2023-05-07]. Dostupné z: https://www.c-its.cz/uvod_.
10. ETSI TS 102 940 V2.1.1. *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management [online* [online]. 2021. [cit. 2023-04-24]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf.
11. ETSI TS 102 731 V1.1.1. *Intelligent Transport Systems (ITS); Security; Security Services and Architecture* [online]. 2010. [cit. 2023-04-30]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf.

12. JOINT RESEARCH CENTER. *C-ITS Point of Contact (CPOC) Protocol*. 2019. Dostupné z: https://cpoc.jrc.ec.europa.eu/.
13. EUROPEAN COMMISSION. *European Certificate Trust List (ECTL)* [online]. [cit. 2023-05-01]. Dostupné z: https://cpoc.jrc.ec.europa.eu/ECTL.html.
14. EUROPEAN COMMISSION. *Trust List Manager Certificate* [online]. [cit. 2023-05-01]. Dostupné z: https://cpoc.jrc.ec.europa.eu/TLMCertificates.html.
15. ITU-T. *The ASN.1 project* [online]. [cit. 2023-04-18]. Dostupné z: https://www.itu.int/en/ITU-T/asn1/Pages/introduction.aspx.
16. ETSI TS 102 941 V2.2.1. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management [online]* [online]. 2022. [cit. 2023-04-24]. Dostupné z: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/02.02.01_60/ts_102941v020201p.pdf.
17. EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. *Abstract Syntax Notation definitions for TC ITS* [online]. [cit. 2023-01-20]. Dostupné z: https://forge.etsi.org/rep/ITS/asn1.
18. RIEBL, Raphael. *Vanetza* [online]. [cit. 2022-11-30]. Dostupné z: https://github.com/riebl/vanetza.
19. COHDA WIRELESS. *V2X Stack* [online]. [cit. 2023-05-02]. Dostupné z: https://www.cohdawireless.com/solutions/v2x-stack/.
20. COHDA WIRELESS. *MK6 OBU* [online]. [cit. 2023-05-02]. Dostupné z: https://www.cohdawireless.com/wp-content/uploads/2023/04/CW_Product-Brief-sheet-MK6-OBU.pdf.
21. COMMSIGNIA. *V2X Software Stack* [online]. [cit. 2023-05-02]. Dostupné z: https://www.commsignia.com/products/v2x-software-stack/.
22. KLINGER, Florian. *OpenC2X* [online]. [cit. 2023-05-02]. Dostupné z: https://github.com/florianklingler/OpenC2X-standalone.
23. SAUTER, Fabian; TRAUB, Kilian. *C++ Requests: Curl for People* [online]. [cit. 2023-05-01]. Dostupné z: https://github.com/libcpr/cpr.
24. CURL. *Curl: command line tool and library for transferring data with URLs* [online]. [cit. 2023-05-01]. Dostupné z: https://curl.se/.
25. TESKALABS. *C-ITS Security / C-V2X Security* [online]. [cit. 2022-11-28]. Dostupné z: https://teskalabs.com/solutions/seacat-cits-security.
26. EUROPEAN COMMISSION. *C-ITS Point of Contact Documentation* [online]. [cit. 2023-05-01]. Dostupné z: https://cpoc.jrc.ec.europa.eu/Documentation.html.
27. BOOST ORGANIZATION. *Boost* [online]. [cit. 2023-05-08]. Dostupné z: https://boost.org.
28. KARNEY, Charles. *GeographicLib* [online]. [cit. 2023-05-08]. Dostupné z: https://geographiclib.sourceforge.io.
29. CRYPTO++. *Wei Dai* [online]. [cit. 2023-05-08]. Dostupné z: https://cryptopp.com.

Obsah přiloženého média

- `readme.txt` ..... stručný popis obsahu média
- `src`
  - `vanetza` ..... zdrojové kódy upravené knihovny Vanetza včetně vyvinuté aplikace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
- `certs`
  - `RCA` ..... certifikát kořenové certifikační autority
  - `canonicalKey` ..... kanonický klíč registrovaného zařízení