TÉCNICO LISBOA



A secure data dissemination scheme for connected vehicle networks

Nuno Romeu Policarpo Lopes

Thesis to obtain the Master of Science Degree in

Electrical and Computer Engineering

Supervisors: Prof. Paulo Rogério Barreiros D'Almeida Pereira
Prof. Naercio David Pedro Magaia

Examination Committee

Chairperson: Prof. João Luís Costa Campos Gonçalves Sobrinho
Supervisor: Prof. Paulo Rogério Barreiros D'Almeida Pereira
Member of the Committee: Prof. António Manuel Raminhos Cordeiro Grilo

Jun 2024

I declare that this document is an original work of my own authorship and that it fulfills all the requirements of the Code of Conduct and Good Practices of the Universidade de Lisboa.

Acknowledgments

I thank my friends and family. I also give thanks to my Professors, Prof. Paulo Rogério Pereira and Prof. Naercio Magaia, who accompanied me and gave me advice throughout the process of doing my Master Thesis.

Abstract

Vehicular networks enable vehicles to communicate with each other and with the roadside infrastructure. They are part of the Intelligent Transport Systems (ITS) framework and provide safety, navigation, and other roadside services. To communicate with each other in the network, ITS stations (vehicles, roadside and portable units) use pseudonym certificates, called Authorization Tickets (ATs). These ATs are issued to certified ITS stations (ITS-Ss) and used by them to sign and encrypt messages in the network, building trust in ITS. ATs are of short validity, having to be renovated frequently due to privacy of ITS stations. Revocation of ATs is done in a passive way, not sending new ATs to compromised ITS-Ss, leaving a space between the moment an ITS-S is classified as compromised and the end of validity of its ATs, exposing the network to possible misleading messages. This work contains a study on ITS security management, resulting in a survey of the standards applicable on the topic, and proposes an active revocation algorithm, based on an Authorization Ticket Certificate Revocation List (ATCRL). This list is distributed in the ITS network and used by vehicles to discard messages associated with the compromised ATs. An analysis of the proposed algorithm was conducted, where several scenarios were built to compare and analyse different uses of the algorithm, including the two versions proposed, a decentralized and a centralized version. In the end, conclusions about the use of the active revocation algorithm were taken and possible optimizations and variants for future works are pointed.

Keywords

ITS; Security Management; Authorization Tickets; Active Revocation

Resumo

Redes veiculares possibilitam aos veículos comunicarem entre si e com a infraestrutura rodoviária. São parte do Sistema de Transporte Inteligente (ITS), e providenciam segurança, navegação e outros serviços rodoviários. Para comunicarem entre si na rede, estações ITS (ITS-Ss) (veículos, infraestrutura e unidades portáteis), usam certificados pseudónimos, denominados por Authorization Tickets (ATs). Estes ATs são enviados para as ITS-Ss certificadas e usados para assinar e cifrar mensagens na rede, construindo confiança na rede ITS. Os ATs são de validade curta, tendo que ser renovados frequentemente devido a razões de privacidade das ITS-Ss. A revogação dos ATs é feita de modo passivo, não reenviando novos ATs para a ITS-S comprometida, levando a um espaço entre o momento em que a ITS-S é dada como comprometida e o final de validade dos seus ATs, expondo a rede à possibilidade de mensagens maliciosas. Este trabalho apresenta um estudo da gestão de segurança em ITS, resultando numa análise dos standards aplicados, e propoẽ um algoritmo de revogação ativa baseado numa lista de certificados revogados, a Authorization Ticket Certificate Revocation List (ATCRL). A lista é distribuída na rede ITS e usada pelos veículos para descartar mensagens associadas aos ATs comprometidos. Uma análise do algoritmo proposto é efetuada, onde vários cenários são elaborados para comparar e analisar diferentes usos do algoritmo, incluindo as duas versões propostas, a versão descentralizada e a versão centralizada. No final, conclusões acerca do uso do algoritmo de revogação ativa são retiradas e possíveis estratégias de otimização e melhoramento são apontadas.

Palavras Chave

ITS; Gestão de Segurança; Authorization Tickets; Revogação Ativa

Contents

1 Introduction **1**

1.1 Motivation . . . 2

1.2 Problem . . . 2

1.3 Objectives . . . 3

1.4 Structure of the work . . . 3

2 State-of-the Art **4**

2.1 Communications architecture . . . 5

2.2 Security requirements of ITS applications . . . 9

2.2.1 Cooperative Awareness . . . 9

2.2.2 Decentralized Environment Notification . . . 10

2.2.2.A Authentication and Authorization . . . 11

2.2.2.B Confidentiality and Privacy . . . 11

2.2.3 Multiple Applications . . . 11

2.3 ITS security functional model . . . 11

2.3.1 Trust and privacy management . . . 13

2.3.2 Access control . . . 14

2.3.3 Identity Management . . . 15

2.3.4 Confidentiality . . . 15

2.3.5 Enrolment and Authorization assumption and requirements . . . 16

2.3.5.A Message Sequence . . . 16

2.4 ITS Security management system . . . 17

2.4.1 Root CA . . . 18

2.4.2 Distribution Center . . . 20

2.4.3 Trust List Manager . . . 20

2.4.4 Misbehaviour Authority . . . 21

2.4.5 ITS-S Security Lifecycle management . . . 22

2.4.5.A Manufacturer . . . 22

2.4.5.B Enrolment . . . 23
2.4.5.C Authorization . . . 23
2.4.5.D Maintenance . . . 24
2.4.5.E End of Life . . . 24
2.4.6 Usage of CTL and CRL by ITS-Ss . . . 24
2.4.7 Renewing CA certificates and updating the PKI . . . 25
3 Algorithms Proposal **26**
3.1 Traceability . . . 27
3.1.1 Algorithm . . . 27
3.1.1.A Algorithm Entities . . . 27
3.1.1.B Algorithm Steps . . . 27
3.1.1.C Requirements . . . 28
3.2 Active Revocation of ATs . . . 28
3.2.1 Algorithm . . . 29
3.2.1.A Requirements, Notes and Future Concerns . . . 30
3.2.2 Decentralized Approach . . . 31
3.2.2.A Algorithm . . . 32
3.2.2.B Notes . . . 33
3.3 Security and Communications Requirements . . . 33
3.3.1 Communication Paths . . . 33
3.3.2 Communication Profiles and Protocols . . . 34
3.3.2.A Communication Profiles . . . 34
3.3.3 Security in Communications . . . 36
3.3.3.A Confidentiality . . . 36
3.3.3.B Authentication and Integrity . . . 38
3.3.4 Secure Message Data Structures . . . 38
4 Performance Evaluation **39**
4.1 Overview . . . 40
4.2 Data Dimensions, Cryptographic Operations and Access Rates . . . 40
4.2.1 ATCRL . . . 40
4.2.2 Messages Content dimensions . . . 40
4.2.3 Cryptographic Operations . . . 41
4.2.4 Access Technologies . . . 42
4.3 Formulas . . . 43
4.4 Configuration scenarios . . . 46

4.4.1 Scenario 1 - Base Scenario 46
4.4.2 Scenario 2 - Increase in RSUs 47
4.4.3 Scenario 3 - Use of delta ATCRLs 48
4.4.4 Scenario 4 - Addition of cryptographic operations 49
4.4.5 Scenario 5 - Alternative paths 50

5 Conclusion **52**

5.1 Synthesis of the work 53
5.2 Results and Conclusions 54
5.3 Future work 54

Bibliography **55**

A Standard Data Structures and Authorization Request Message **59**

A.1 Signed and Encrypted Data Structures 59
A.2 Authorization Request Message 60

List of Figures

2.1 Scenario Illustration 5
2.2 ITS station reference architecture 7
2.3 Examples of possible elements in the ITS station reference architecture 8
2.4 A vehicular network architecture 9
2.5 ITS communications reference scenario 12
2.6 Sequence to achieve signed message transfer between ITS-Ss 17
2.7 PKI architecture 18
2.8 ITS Station Security Life Cycle 22

3.1 Traceability Algorithm in a compromised situation 28
3.2 Active Revocation algorithm 29
3.3 Active Revocation algorithm - decentralized approach 32
3.4 Communication paths for ITS-S communication with the PKI 33
3.5 Communication protocols between the ITS-S and PKI authorities 35
3.6 Communication protocols between an ITS-S and an ITS-S Roadside Gateway using Ipv6 over GeoNetworking 36
3.7 Communication protocols between an ITS-S Vehicle and an ITS-S Roadside Gateway using GN/BTP protocol 37
3.8 Communication protocols between an ITS-S Vehicle and an ITS Roadside Gateway using Ipv6 over G5 37

4.1 ATCRL components illustration 40

A.1 AuthorizationRequest message 63
A.2 AuthorizationRequestMessageWithPop 64

List of Tables

2.1 Functional element roles of the PKI 19
2.2 Functional element roles of the top-level trust management 19

3.1 ITS-G5 frequency bands and intended usage 34

4.1 Messages contents and respective dimensions 41
4.2 ATCRL components dimension 41
4.3 Cryptographic Operations data and dimensions 41
4.4 Cryptogram lengths and ratio for different plaintext sizes with an ECIES 512 bits key . . . 42
4.5 SHA-256 execution times 42
4.6 Encryption and Decryption rates for ITS entities public and private key sizes with ECIES . 42
4.7 Signatures operations time over the SHA-256 hash of a message 43
4.8 Active Revocation algorithm Access Technologies data rate 43
4.9 Protocols headers sizes 46
4.10 Variables configuration for scenario 1 46
4.11 Active Revocation algorithms transmission times 47
4.12 Variables configuration for scenario 2 47
4.13 Decentralized AR algorithm time increase with RSUs 47
4.14 Values of variables for scenario 3 48
4.15 Decentralized AR algorithm times with the use of a delta ATCRL and the full ATCRL . . . 48
4.16 AR algorithms times with security operations 50
4.17 Communication time over the various communication paths for sending the MR 51

Acronyms

AA	Authorization Authority
AT	Authorization Ticket
BTP	Basic Transport Protocol
C-ITS	Cooperative Intelligent Transport System
CA	Certificate Authority
CARA	Centralized Active Revocation Algorithm
CAM	Cooperative Awareness Message
CCMS	Cooperative-ITS Certificate Management System
CRL	Certificate Revocation List
CTL	Certificate Trust List
CPM	Collective Perception Message
CPOC	C-ITS Point of Contact
DARA	Decentralized Active Revocation Algorithm
DC	Distribution Center
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communications
EA	Enrolment Authority
EC	Enrolment Certificate
ECDSA	Elliptic Curve Digital Signature Algorithm

ECIES Elliptic Curve Integrated Encryption Scheme

ECTL European Certificate Trust List

ETSI European Telecommunications Standards Institute

EV Electric Vehicle

GN GeoNetworking

HTTP Hypertext Transfer Protocol

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IVIM Infrastructure to Vehicle Information Message

IP Internet Protocol

IPv6 Internet Protocol version 6

ISO International Organization for Standardization

ITS Intelligent Transportation Systems

ITS-AID ITS Application ID

ITSC ITS Communications

IoV Internet of Vehicles

ITS-S ITS Station

LKL Last Known Location

LTE Long Term Evolution

MA Misbehaviour Authority

MAC Media Access Control

MQTT Message Queueing Telemetry Transport

NAP National Access Point

OBD On-Board Diagnostic

OBU On-Board Unit

OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
POP	Prove of Possession
PSID	Provider Service Identifier
RCA	Root CA
RSU	Roadside Unit
RTT	Round Trip Time
SOC	Security Operational Center
SAEM	Services Information Announcement Essential Message
SDO	Standard Development Organisation
SSP	Service Specific Permissions
TCP	Trasmission Control Protocol
TLM	Trust List Manager
TLS	Transport Layer Security
TS	Technical Specification
TTP	Trusted Third Party
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VRU	Vulnerable Road User
WLAN	Wireless Local Area Network

1

Introduction

Contents

1.1 Motivation 2
1.2 Problem 2
1.3 Objectives 3
1.4 Structure of the work 3

1.1 Motivation

Vehicular networks are a particularly challenging class of mobile networks that enable vehicles to communicate with each other and with the roadside infrastructure. They are part of the Intelligent Transportation Systems (ITS) framework, providing safety, navigation, and other roadside services. As of today, they are understood as having evolved into a broader Internet of Vehicles (IoV) and are expected to evolve into an Internet of autonomous Vehicles.

ITS message applications, such as Cooperative Awareness Messages (CAMs), the beacon-like messages of ITS, used to generate traffic in the setup, and event-focused Decentralized Environmental Notification Messages (DENMs), have security requirements as authentication, authorization, confidentiality and privacy. In order to protect users privacy, ITS messages should not be linked to users or vehicles identity and messages coming from the same ITS station (vehicles, roadside or portable units) should not be linked together. To achieve the desired security requirements, ITS stations (ITS-Ss) have to be enrolled and authorized to communicate in the ITS network, following an enrolment process.

In the enrolment process, an ITS station communicates with the Enrolment Authority (EA) using its canonical (unique and immutable) identity to obtain an Enrolment credential (EC), giving the ITS-S access to communicate in the ITS network. The ITS-S then uses the obtained EC to acquire Authorization Tickets (ATs), in the form of pseudonym certificates, from the Authorization Authority (AA), providing the ITS-S with authoritative proof that may use specific ITS applications.

1.2 Problem

With the use of ATs, an ITS-S can send misbehaviour messages in the ITS network, endangering the safety of other users. To detect compromised messages, a misbehaviour detection system embedded in ITS-Ss sends a Misbehaviour Report (MR) to the Misbehaviour Authority (MR), who classifies it and takes the appropriate response. The response can be of different levels: no action, sending an alert to the user or to the ITS station's manufacturer, or initiate the revocation process (e.g. blocking the ITS-S Enrolment Credential).

Revocation of ATs is conducted in a passive way, by blocking the ITS-S EC, and thus not issuing more ATs to the compromised ITS-S. The problem is that even though ATs are of a short validity period, having to be renovated frequently, the time between the ITS-S is classified as compromised by the MA and the end validity of its ATs remains open to communication from the compromised ITS-S to the ITS network. To tackle this issue, an active revocation algorithm is developed based on a Authorization Ticket Certificate Revocation List (ATCRL), to be distributed in the network.

1.3 Objectives

The first goal of this work is the development of an active revocation algorithm. The second goal, is the optimization of the developed algorithm. In this work, two algorithm versions are developed. A decentralized version and a centralized version, with the first having less messages exchanged in the algorithm and theoretically being faster. Other optimization strategies are applied, such as the use of a delta version of the ATCRL, containing only the updated entries regarding the full ATCRL.

The third and final goal of the work is to evaluate the proposed algorithms. For that, several scenarios are conceived, assigning different values for the following variables: the number of ATs adding to the ATCRL, the number of ATs present in the ATCRL, and the number of Road Side Units (RSUs) used to disseminate the list in the network. We aim to evaluate different aspects of the algorithm, namely the difference between the two algorithm versions, the increase in the number of RSUs distributing the list, the use of a delta ATCRL, the impact of cryptographic measures and the use of alternative paths for sending the MR. In the end, conclusions for each scenario are drawn.

1.4 Structure of the work

This work has the following structure:

- In chapter 1, an introduction to the work is given;
- In chapter 2, the state-of-the art of ITS security management is presented;
- In chapter 3, the active revocation algorithm versions and a traceability algorithm used in the active revocation algorithm are detailed;
- In chapter 4, the performance evaluation results of the use of the active revocation algorithm developed in the different scenarios conceived are presented and conclusions in each scenario are taken;
- In chapter 5, a summary of the work developed, conclusions and future works are addressed.

In Annex A, standard secure message data structures are introduced and the relation between the ITS-S obtaining ATs, the EA and the AA is demonstrated with the Authorization Request Message.

2

State-of-the Art

Contents

2.1 Communications architecture 5
2.2 Security requirements of ITS applications 9
2.3 ITS security functional model 11
2.4 ITS Security management system 17

2.1 Communications architecture

Intelligent Transport Systems (ITS) are systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (cars, trains, planes, ships). Elements of ITS are standardized in various standardisation organisations, called Standards Development Organizations (SDOs), such as ETSI TC ITS [1].

ITS Communications (ITSC) is to a large extent independent from specific communication technologies and specific ITS applications. The ITSC architecture is intended to be an open systems architecture, i.e. an architecture that is open and not proprietary.

ITS applications make use of wireless communications:

- Communications between mobile ITS stations (vehicles), and between mobile ITS stations and fixed ITS stations (roadside installations), with single-hops or multiple hops between the source and destination ITS stations.
- Access to public and private (local) networks including the global Internet.
- Infrastructure and satellite broadcast.

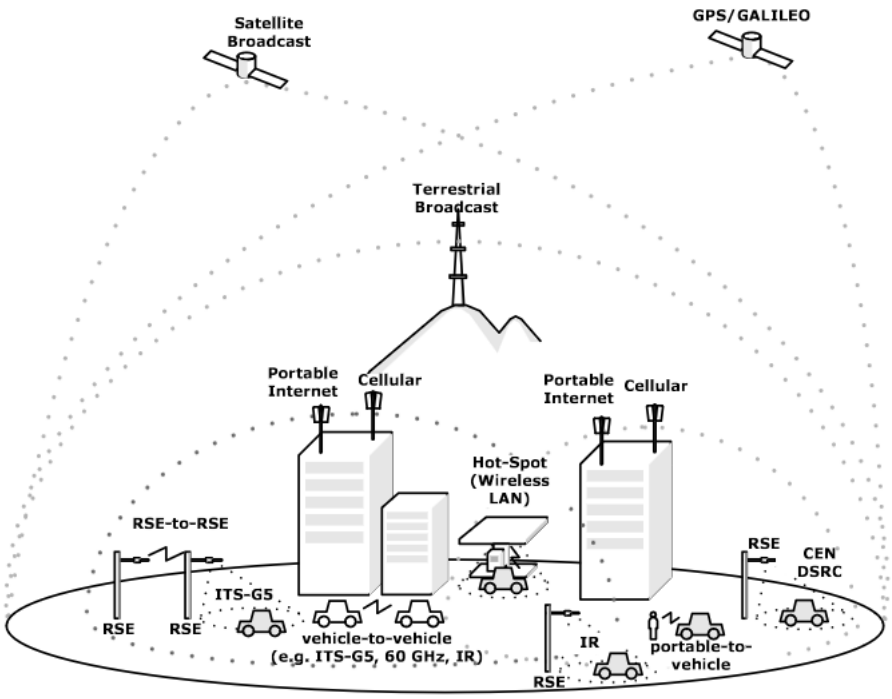


Figure 2.1: Scenario Illustration [1]

ITSC is a new type of communication system dedicated to transportation scenarios, e.g. as illustrated in Figure 2.1. It is based on two domains:

- ITS domain; and
- Generic domain

ITS domain refers to all elements of ITSC which are specified in ITS/ITSC standards. Generic domain refers to other elements used for ITS/ITSC. The following list presents the aspects considered for the development of ITSC standards [1]:

- mobility of ITS stations causing high dynamics of their topology;
- potential support of any kind of communication technology, including Internet, public networks and legacy systems such as Bluetooth TM , technologies for road tolling (DSRC), . . . , i.e. abstraction from implementation details;
- potential support of any kind of application including those:
  - designed for ITSC;
  - using the ITS station as a transparent communication means;
  - using station-internal communications only.
- dynamic and flexible consideration of user needs, e.g. with respect to communications capacity (data rate), communications cost (in terms of money), communications reliability, communications availability and communications privacy;
- potential of efficient prioritization of application classes;
- potential of dedicated relations between applications and communication technologies dependent on regional requirements, e.g. for road safety and traffic efficiency applications, for road tolling, etc.;
- support of modular implementations with multiple physical units networked in a single ITS station;
- support of profiling;
- global applicability.

ITS stations reference architecture follows the principles of the Open Systems Interconnection (OSI) model for layered communication protocols. This architecture is illustrated in Figure 2.2.

The Networking service mainly implements the GeoNetworking (GN) protocol [2]. It is a geographical addressing and packet forwarding system for point-to-point and point-to-multipoint communications. This

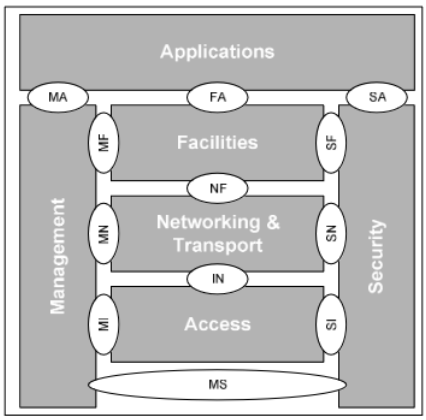


Figure 2.2: ITS station reference architecture [1]

service also implements the IPv6 protocol [3], and the GN/IPv6 adaptation sublayer (GN6ASL) [4] to combine IPv6 and GN routing features.

The Transport service implements the Basic Transport Protocol (BTP) [5], a transport layer protocol used for ITS communications similar to User Datagram Protocol (UDP) [6], the Transmission Control Protocol (TCP) protocol [7] and others. BTP provides port numbers to address upper-layer sub-services and is similar to UDP in that it does not provide a reliable connection between devices like TCP.

The Facilities layer supports various ETSI ITS defined sub-services. It provides support for the processing of Cooperative Awareness Messages (CAMs) [8], the beacon-like messages of the ETSI ITS vehicular systems and used to generate traffic in the setup, event-focused Decentralized Environmental Notification Messages (DENMs) [9], Infrastructure to Vehicle Information Messages (IVIMs) [10], radar-based Collective Perception Messages (CPMs) [11] and Services Information Announcement Essential Messages (SAEMs) [12].

A more detailed picture of the ITS station reference architecture is depicted in Figure 2.3.

The following ITS sub-systems are identified in ITSC:

- personal ITS sub-system or Vulnerable Road User (VRU); in hand-held devices,
- central ITS sub-system; part of an ITS central system, enables the continuous monitoring of road activity,
- vehicle ITS sub-system or On-Board Unit (OBU); in cars, trucks, etc., in motion or parked,
- roadside ITS sub-system or Roadside Unit (RSU); on gantries, poles, etc.

Each of these ITS sub-systems contains the functionality described by the ITS station reference architecture.

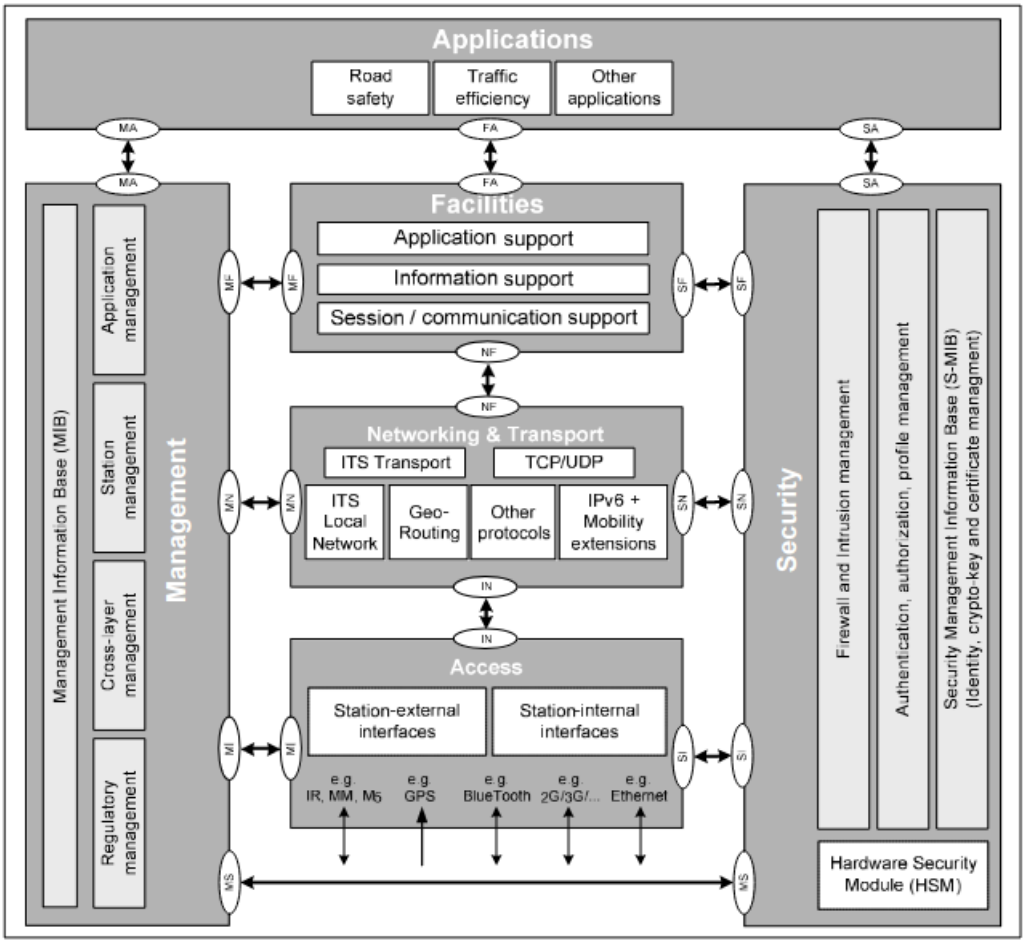


Figure 2.3: Examples of possible elements in the ITS station reference architecture [1]

Vieira et al. develop a vehicular communications framework, as part of the design and implementation of mobility testbeds in Portugal [13] and developed under the pan-European C-Roads initiative [14], where the roadside scope consists of RSUs equipped with ETSI ITS G5 communications technology connected to the backhauling network by either fiber optics or cellular networks. The cloud scope consists of a cloud-based Message Queueing Telemetry Transport (MQTT) Broker, which makes use of the publish-subscribe messaging protocol MQTT. The MQTT Broker is used by all RSUs, facilitating information exchange and connecting them to the central ITS Platform. Additionally, the Cooperative Intelligent Transport System (C-ITS) Platform is continually connected to the National Access Point (NAP) for the exchange of high-level transport-related data and to the Portuguese Public Key Infrastructure (PKI) for the implementation of the security measures outlined in ETSI standards. This scenario is illustrated in Figure 2.4.

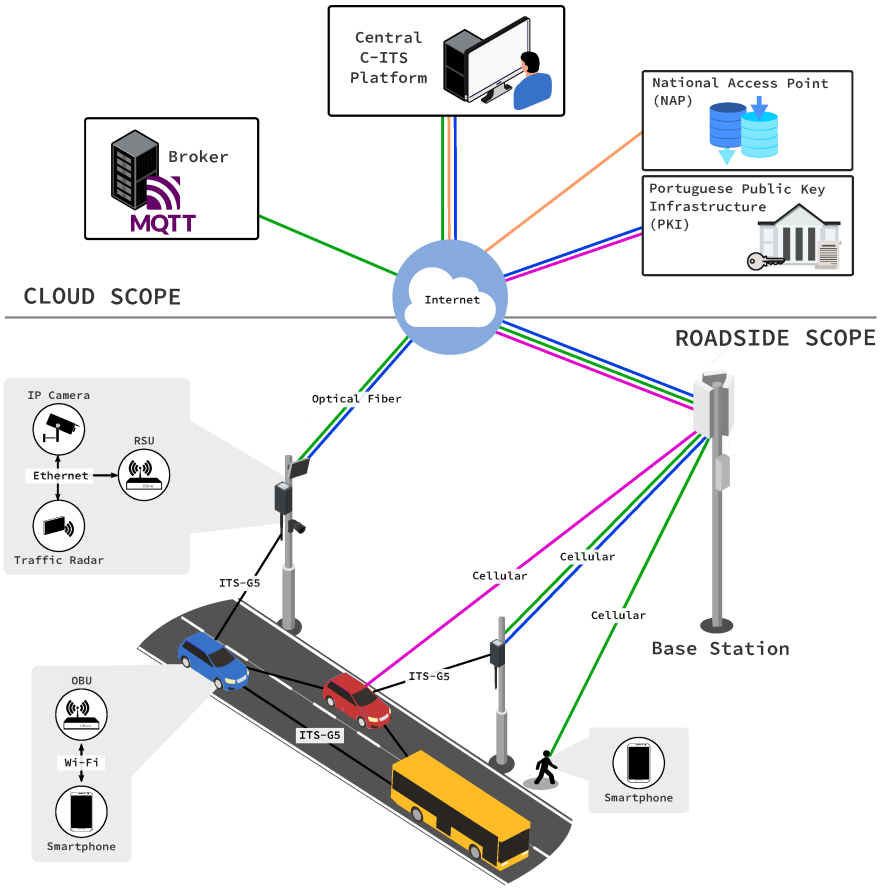


Figure 2.4: A vehicular network architecture [13]

2.2 Security requirements of ITS applications

2.2.1 Cooperative Awareness

Cooperative Awareness Messages (CAMs) allow ITS users to provide other users with information regarding their status and environment in order to improve road safety. CAMs are broadcast, single-hop, time-critical, with low data content, transmitted frequently, vehicle-to-vehicle and require no established communication session (single message with no explicit coordination). Some examples of CAMs are emergency vehicle warning, slow vehicle indication, across traffic turn collision risk warning and cooperative merging assistance.

In general, authentication is required for applications that intend to send messages over the network, such as the Cooperative Awareness application. In addition to authenticity and integrity, authorization is required in order to restrict access to legitimate users.

There are several classes of CAM authorization:

- Basic CAM authorization
  - linked to basic data such as length, speed, heading, acceleration and brake status;
  - granted to all enrolled ITS stations to enable participation in the basic ITS.
- Advanced CAM authorization:
  - contains additional information such as that required for across traffic turning, merging assistance and collision warning;
  - depends on the abilities of the sending station such as cryptographic algorithms implemented, its sensors and its perceived trustworthiness.
- Authorization to claim priority rights for emergency vehicles:
  - granted only to specially authorized emergency vehicles or public transport vehicles according to national legislation. Multiple layers of priority may be defined, for example priority for emergency vehicles and on a lower level authorization to use a special lane reserved for public transportation;
  - granted by a governmental organization or its authorized proxy agency;
  - priority rights asserted by the user during operation, not during authorization.
- Authorization to state regulatory orders such as speed limit and road closures:
  - granted only to specially authorized ITS stations such as RSUs and police vehicles;
  - granted by a governmental organization or its proxy agency.

CAMs are sent periodically up to several times a second by every ITS Station (ITS-S), containing substantial status information (e.g. location) relating to the sending ITS-S. Consequently, it is necessary to ensure that the data cannot be linked to any vehicle or individual so that no personally identifying information is leaked by the CAM service. As CAMs are broadcasts to any possible receiver there are no confidentiality requirements.

2.2.2 Decentralized Environment Notification

Decentralized Environment Notification Messages (DENMs) are broadcast and then forwarded by the receiving stations to form a geocast. They are sent event-driven to inform about a specific event or a specific condition to improve road safety. They can be categorized as follows:

- broadcast;
- multi-hop with geocasting;

- time-critical;
- low data content;
- transmitted frequently, but only when hazard exists;
- require no established communication session.

Some examples of DENMs are emergency electronic brake lights, stationary vehicle - accident, stationary vehicle - vehicle problem, traffic condition warning, roadwork warning and decentralized floating car data, such as hazardous location, precipitation, road adhesion, visibility and wind.

Area hazard warnings (DENMs) are not always linked to a specific ITS-S as a point of origin, consequently they cannot be usually used for tracking. Security mechanisms need to take into account the forwarding of the messages.

2.2.2.A Authentication and Authorization

Authorization for DENMs could be granted on several levels depending on sensor equipment, sensor quality and algorithmic and processing capabilities of the ITS-S. Apart from that, requirements apply as for CAM.

2.2.2.B Confidentiality and Privacy

As the service is event-driven and, therefore, sporadic and as neither the properties of the sender nor its identity are important for the reported area warning, the privacy issues are reduced compared with the CAM service. Confidentiality is not required.

2.2.3 Multiple Applications

In general, Authentication and Authorization are handled separately for each individual application. As for confidentiality and privacy, it is assumed that each ITS application uses its own identifiers that cannot be linked to each other.

In particular, DENM and CAM originating from the same vehicle should not be linkable.

2.3 ITS security functional model

The main functional elements of the ITS security functional model can be determined by considering a simple ITS communications scenario such as that shown in Figure 2.5. In this scenario, an ITS-enabled vehicle needs to communicate with the following entities:

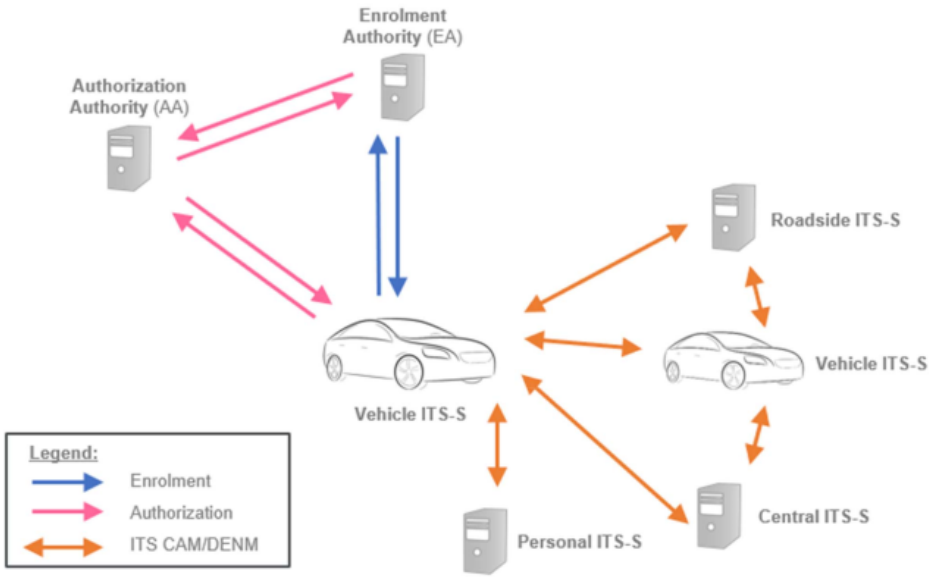


Figure 2.5: ITS communications reference scenario [15]

- Enrolment Authority (EA): authenticates an ITS-S and grants it access to ITS communications.
- Authorization Authority (AA): provides an ITS-S with authoritative proof that it may use specific ITS services.
- other ITS-equipped vehicles; and
- other ITS-equipped devices:
  - roadside units or central units; and
  - personal units such as portable devices.

The ITS security reference model (Figure 2.5) can be used as the basis for specifying all ITS security services related to single-hop broadcast services such as CAM. However, a different model involving a third ITS-S for relaying messages needs to be considered for all ITS security services associated with forwarding, broadcast services such as DENM.

In the security reference model, the vehicle (sending ITS-S) communicates with the Enrolment Authority (EA) to acquire rights for access ITS communications and then uses those rights to negotiate authoritative proof to invoke ITS services from the Authorization Authority (AA).

The ITS communication system relies on indirect trust relationships built statically using certification by Trusted Third Parties (TTPs). Enrolment is the main access control to the ITS and the possession of a valid enrolment certificate grants permission to the station to be part of the ITS and, subsequently, to gain authorization for the use of further services.

2.3.1 Trust and privacy management

ISO/IEC identify the following four key attributes relating to privacy:

- anonymity;
- pseudonymity;
- unlinkability; and
- unobservability.

Anonymity alone is insufficient for protection of an ITS user's privacy and unsuitable as a solution for ITS, as one of the main requirements of ITS is that the ITS-S should be observable in order to provide improved safety. Consequently, pseudonymity and unlinkability offer the appropriate protection of the privacy of a sender of basic ITS safety messages (CAM and DENM). Pseudonymity ensures that an ITS-S may use a resource or service without disclosing its identity but can still be accountable for that use. Unlinkability ensures that an ITS-S may make multiple uses of resources or services without others being able to link them together.

Pseudonymity shall be provided by using temporary identifiers in ITS safety messages, and never transmitting the station's canonical identifier in communications between ITS stations. Unlinkability can be achieved by limiting the amount of detailed immutable (or slowly changing) information carried in the ITS safety message, thus preventing the possible association of transmissions from the same vehicle over a long time period (such as two similar transmissions broadcast on different days) [16].

ITS Privacy is provided in two dimensions:

i) privacy of ITS registration and authorization tickets provisioning:
   - ensured by permitting knowledge of the canonical identifier of an ITS-S to only a limited number of authorities (EAs);
   - provided by the separation of the duties and roles of PKI authorities into an entity verifying the canonical identifier known as the Enrolment Authority (EA) and an entity responsible for authorizing and managing services known as the Authorization Authority (AA);

ii) privacy of communications between ITS-Ss:
   - ITS-Ss should protect integrity and authenticity of packets by using digital signatures, computed with the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in IEEE Std 1609.

2.3.2 Access control

Before an ITS station can make full use of the ITS applications, services and capabilities that are available to it, it is required to obtain specific credentials from the Authorization Authority. These credentials, in the form of cryptographically signed certificates, are used to assure any receiving ITS-S that the station has the necessary permission to send the particular service-specific information and that it can be trusted.

Authorization tickets are only issued to an ITS-S after a comprehensive procedure has been followed in order to protect its identity and avoid misuse of ITS services and capabilities. This procedure involves:

- Initialization:
  - performed in conjunction with the manufacturer of the vehicle or ITS device;
  - establishes a set of initialization credentials:
    - a canonical (unique and immutable) identity for the ITS-S;
    - a canonical public and private cryptographic key pair for the ITS-S;
    - a generic profile of the properties of the ITS-S (for example, the proven stability of its software and hardware, its resistance to attack and the ITS facilities that it is able to support);
    - optionally, a cryptographic certificate (self-signed bootstrap certificate) linking the canonical identity with the public key of the ITS-S and its generic profile.
- Enrolment:
  - performed as a dialogue between the ITS-S and the Enrolment Authority;
  - uses the canonical credentials to establish a set of enrolment credentials at initialization and then the previously issued enrolment credentials to renew the enrolment credentials:
    - one or more cryptographic certificates indicating the applications, services and capabilities that the ITS-S is permitted to use and which enable the ITS-S to pseudonymously request authorization from the Authorization Authority to invoke those services.
- Authorization:
  - performed as a dialogue between the ITS-S and the Authorization Authority;
  - uses the enrolment credentials to establish a set of authorization credentials:
    - one or more cryptographically signed authorization ticket which, when combined with a transmitted ITS message, enables the ITS-S to assert pseudonymously to other ITS stations its right to send that particular message or information.

2.3.3 Identity Management

The Authorization Authority provides an ITS station with multiple authorization tickets (or pseudonym certificates) to be used in the ITS communication over its life time. The authorization ticket pseudonymises the ITS-S identity whilst in the same time proving it is authenticated and authorized to access communication resources and services. The ITS-S shall provide a mechanism for changing frequently the ITS-S pseudonym certificate. Changing authorization tickets in the communication stack may only provide unlinkable pseudonymity, if all identifiers are changed at the same time.

All the IDs associated with the ITS-S across different layers of the communication stack shall be changed synchronously with the Authorization Ticket (AT): this requires that the Security Entity communicates the certificate identifier (ITS-S) each time it is changing of authorization ticket. The information used to identify an ITS-S certificate shall be the hash of the certificate [16].

The ITS station shall apply the following requirements when changing of pseudonym certificate (AT) [16]:

- All the IDs associated with a node across different layers of the ITS stack shall be changed synchronously using the ID Change Notification service;
- All communication layers and components which use an identification information shall register for the ID Change Notifications using the Subscribe ID change Notification service. When the Security Entity indicates an identifier change event, all registered layers shall invoke a two-phase commit process. When the commit is successful, the communication layer shall change their identification.
- In the communication profile for CAM and DENM, all the layers' identifiers (MAC address, GN Source address, IPv6 address, and stationID) shall be derived from the identifier provided by the Security Entity in the ID Change Notification, the hash of the AT.

To this end, it is not mandatory to change the AT prior to use the ID Change service. When no AT change occurs, the hash passed with the ID Change service should contain a random value [16].

2.3.4 Confidentiality

Many of the applications and services used in the ITS environment are based on the transmission of broadcast messages which are intended to be viewed and processed by all recipients. Consequently, there are no confidentiality requirements associated with these messages other than the protection of the sender's identity. However, there are some applications and services which will use point-to-point unicast communications containing sensitive information of a personal or commercial nature. These services will require access to security services that can ensure that this information can only be viewed by the intended recipient(s). [15]

The confidentiality of transmitted information is protected primarily by the encryption of messages within an established security association such that it can only be decrypted by the recipient to whom it is addressed. Messages are encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES) as defined in IEEE Std 1609.2.

2.3.5 Enrolment and Authorization assumption and requirements

For obtaining security credentials from the PKI, the ITS station has to set up a communication with the Certificate Authority (EA or AA). The ITS station may use different communication types for the provisioning of certificates, for instance:

- An ITS G5 communication via a roadside station.
- A Wireless Local Area Network (WLAN) consumer network using IEEE Std 802.11 protocol (via a public or private hotspot or a home network).
- A Cellular network link (3G, 4G or LTE).
- A wired or wireless connection at Electric Vehicle (EV) Charging station.
- Using the Vehicle On-Board Diagnostic (OBD) port and a diagnostic system at the Service Garage or inspection workshop.

An ITS-S can use different communication paths to communicate with a Certificate Authority (EA or AA). The ITS-S can contact the CA directly via a cellular network or indirectly by sending the certificate request message to a roadside ITS-S, which relays it via the infrastructure network to the recipient Certificate Authority. The certificate request message shall be sent in one-hop or multi-hops using the ITS network protocol GeoNetworking and relaying ITS stations.

For all the communication profiles which are using IP protocol, HTTP/1.1 over TCP/IP shall be used in end-to-end communication paths. No supplementary cryptographic layer such as TLS is required [16].

2.3.5.A Message Sequence

The overall ITS-S initialization sequence to achieve ITS secured message transfer on ITS communications is given in Figure 2.6.

Note that the AA has to contact the EA for validation of the enrolment credential, which is sent encrypted along with the authorization request. The AA has no way to disclose the canonical identity of the sending ITS-S, being the EA the only CA who can decrypt and validate the enrolment credential, associated with the canonical identity of the sending ITS-S.

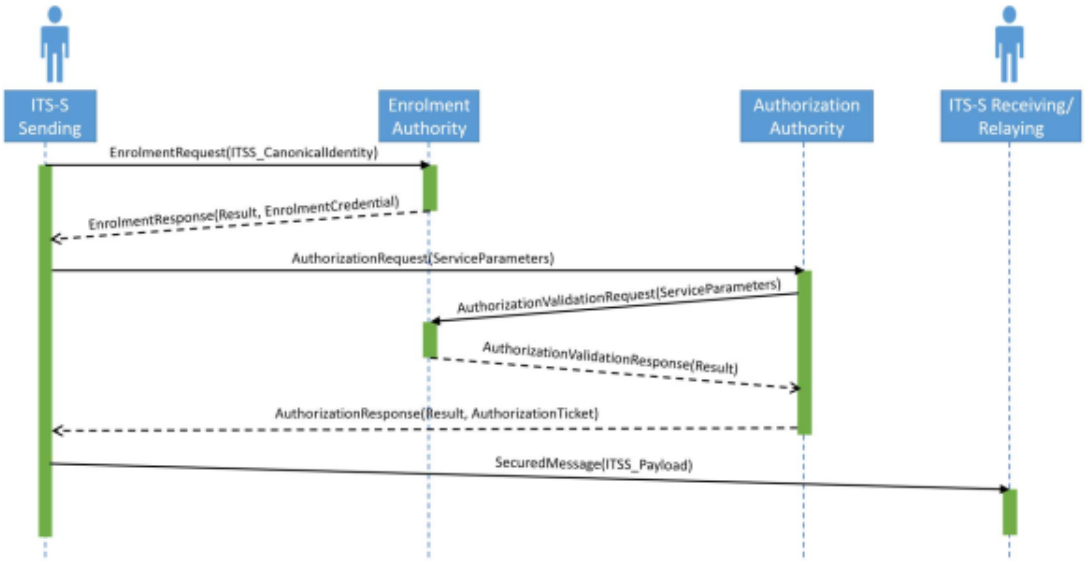


Figure 2.6: Sequence to achieve signed message transfer between ITS-Ss [16]

The AA only sends the encrypted hash of the Enrolment Certificate (EC) to the EA for validation, and does not disclose any identity information of the sending ITS-S, thus assuring pseudonymity and unlinkability. For ITS-Ss which do not require privacy and are allowed to be re-identified by the AA, e.g. RSUs, the encryption of the EC is skipped as it is not necessary.

For more details related to secure management messages for PKI implementation and messages and certificates data structures refer to ETSI Technical Specifications (TS) ETSI TS 103 097 and ETSI TS 102 941 [16, 17].

2.4 ITS Security management system

This section presents the global architecture of the Cooperative-ITS Security Certificate Management System (also named C-ITS Trust Model), its functional entities and the list of services that are provided by the C-ITS Trust Model to support the life-cycle management of Trusted C-ITS Stations.

The Cooperative-ITS Security Certificate Management System architecture is demonstrated in Figure 2.7.

Each of the functional elements in the PKI 'single root CA' trust model has a specific role to play, summarized in Table 2.1.

The Root CA stores its security certificates information and the trusts list information, the Certificate Trust List (CTL) and the Certificate Revocation List (CRL), in a local repository. It may also store the Distribution Center (DC) access information (URL) in its local repository, if DC is present. Optionally the Distribution Center may be used to distribute this information to all the PKI participants.

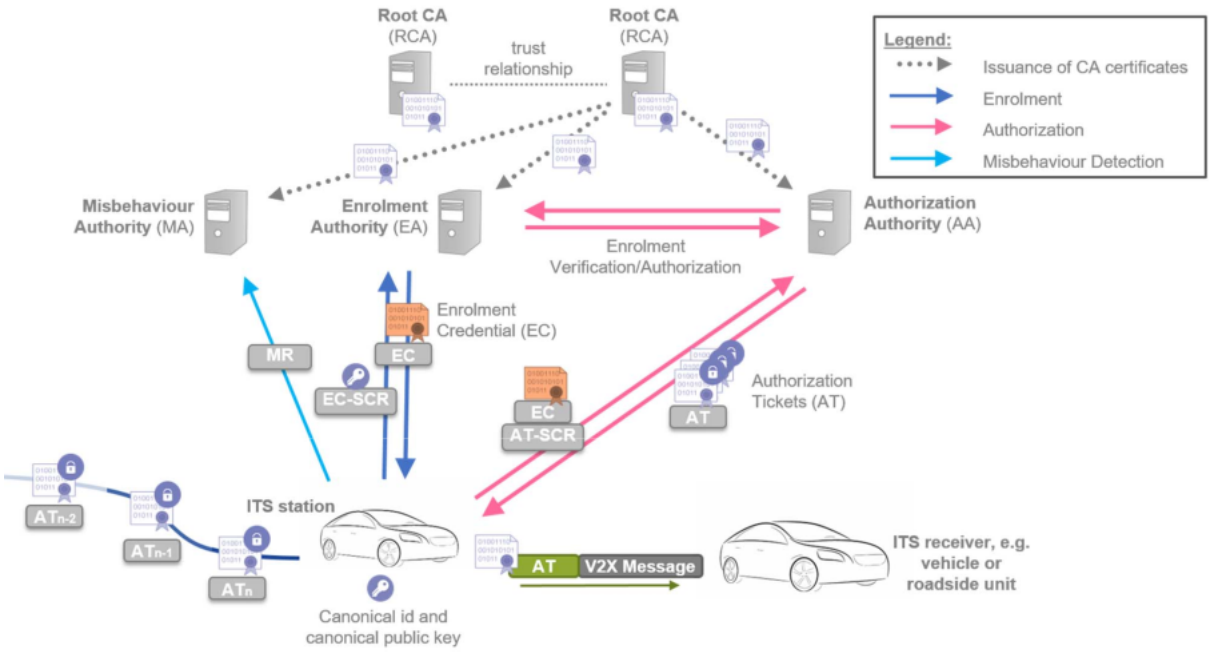


Figure 2.7: PKI architecture [15]

When multiple Root CAs exist and cooperate within the C-ITS Trust Domain, the C-ITS Security Management System follows the Certificate Trust List approach. Described in Table 2.2, the entities responsible for the trust management of the C-ITS system (i.e. governing all aspects related to the operational PKI) are the following:

- Policy Authority;
- Trust List Manager (TLM);
- C-ITS Point of Contact (CPOC).

The Policy Authority is the top level role of the C-ITS Trust system. It is responsible for certificate policy management and for the management of the C-ITS Trust system operational entities such as the TLM, the CPOC and the Root CAs. The TLM stores its security certificates information and the trusts list information (ECTL) in a local repository. The CPOC is used to distribute these information to all PKI participants.

2.4.1 Root CA

Each CA hierarchy (for EA or AA) has at its summit a Root CA, which is the ultimate root of trust for all certificates within that hierarchy.

Functional element	Description
Root Certification Authority	The Root CA is the highest level CA in the certification hierarchy. It provides EA and AA with proof that it may issue enrolment credentials and authorization tickets, respectively.
Enrolment Authority	Security management entity responsible for the life cycle management of enrolment credentials. Authenticates an ITS-S and grants it access to ITS communications.
Authorization Authority	Security management entity responsible for issuing the use of authorization tickets. Provides an ITS-S with authoritative proof that it may use specific ITS services.
Distribution Center (optional)	Provides to ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorized ITS-S or a PKI certification authority by publishing the Certificate Trust List (CTL) and the Certificate Revocation List (CRL).
Misbehaviour Authority	Responsible for processing misbehaviour reports, investigating on potentially misbehaving ITS-S and taking a reaction accordingly in relation with the ITS-S device operator or manufacturer. It has the capability to detect misbehaviour types and to revoke misbehaving ITS stations to exclude them from the C-ITS trust domain in order to no longer consider their messages when received by other entities.
Sending ITS-S	Acquires rights to access ITS communications from Enrolment Authority Negotiates rights to invoke ITS services from Authorization Authority Sends single-hop and forwarded broadcast messages Sends messages to local or back-end services
Forwarding ITS-S	Receives transmitted message from the sending ITS-S and forwards them to the receiving ITS-S if required.
Receiving ITS-S	Receives transmitted messages from the sending or forwarding ITS-S
Manufacturer	Installs necessary information for security management in ITS-S at production
Operator	Installs and updates necessary information for security management in ITS-S during operation

Table 2.1: Functional element roles of the PKI [15]

Functional element	Description
Policy Authority	Policy authority is a role composed by the representatives of public and private stakeholders (e.g. Authorities, Road Operators, Vehicle Manufacturers, etc.) participating to the C-ITS trust model. It designates and authorizes the TLM and the CPOC to operate in the C-ITS Trust system. It decides if root CAs are trustable and approves/removes the Root CAs operation in C-ITS trust domain by notifying the TLM about approved/revoked Root CAs certificates.
C-ITS Point Of Contact (optional)	The CPOC is a unique entity appointed by the Policy Authority. It has responsibility to establish and contribute to ensure communication exchange between the Root CAs, to collect the Root CA certificates and provide them to the Trust List Manager (TLM). The CPOC is also responsible for distributing the CTL issued by the TLM to any interested entities in the trust model.
Trust List Manager	The Trust List Manager is responsible for creating the list of root CA certificates and TLM certificates and signing it. In Europe, the signed list issued by the TLM is called ECTL (European Certificate Trust List).

Table 2.2: Functional element roles of the top-level trust management [15]

The Root CA (RCA) shall be able to update the list of trusted sub CA certificates and to revoke a sub CA certificate within its hierarchy.

The functions provided by the Root CA are the following:

- issuing CAs certificates for EA or AA;
- creation, renewal and distribution of the Root CA certificates;
- revocation of CA certificates (EA or AA) at the end of life or in case of an exception (e.g. compromising of the CA private keys);
- generation and issuance of the signed lists (CRL and CTL) corresponding to the sub CAs, EA and AA, with the CTL containing the associated DC URL and optionally the URLs of the sub CAs;
- generation of log files of the RCA operational activities for auditing purpose.

When a RCA is used as a Trust anchor for the ITS-S, the RCA certificate shall be transmitted to the ITS-S for initialization using a secure communication channel, e.g. during the manufacturing process.

In order to trust an incoming message, an ITS-S shall have secure access at least to the root certificate at the summit of the hierarchy for the authorization ticket attached to the message. The ITS-S may obtain root certificates during the manufacture or maintenance lifecycle stages (Figure 2.8).

2.4.2 Distribution Center

The Distribution Center (DC) may optionally be provided. If present, the following requirements apply:

- The DC shall ensure the access to trust list information (CTLs, CRLs) to all entities of the PKI hierarchy managed by the Root CA.
- The DC shall provide an unrestricted read access to the trust lists.
- The DC shall provide a write access to the lists only for authorized, authenticated users.
- If multiple Root CAs are operating within the C-ITS Trust model, the DC may give access to ECTL.
- If multiple Root CAs are operating within the C-ITS Trust model, the DC may give access to CRLs of other Root CAs.

NOTE: In the EU Certificate Policy, the RCA shall publish and distribute the updated CTL and CRL via a Distribution Centre (DC). [18]

2.4.3 Trust List Manager

The functions provided by the TLM shall be as follows:

- Creation and renewal of the TLM certificates and their associated link certificates;

- Distribution of TLM certificates and their associated link certificates via a local repository or via the CPOC;
- Insertion or removal of Root CA certificates in the ECTL (after approval by the Policy Authority, e.g. when a RCA certificate is created, renewed or revoked);
- Insertion of CPOC distribution centre URL and optionally the URLs of the RCA distribution centers;
- Creation of the signed list of root CA certificates and TLM certificates (ECTL)
- Distribution of ECTL to all participants of the C-ITS trust domain via a local repository or via the CPOC;
- Generation of log files of the TLM operational activities for auditing purpose

NOTE: The CPOC is mandatory in the EU Certificate Policy [18].

2.4.4 Misbehaviour Authority

Within the C-ITS Trust Domain, the misbehaviour detection management is the set of processes for detecting, reporting, assessing, responding to, and understanding the suspicious, abnormal or malicious events in order to provide status information to the systems operator e.g. about the misuse or compromission of credentials or the identification and investigation of misbehaving ITS-Ss [15].

The Misbehaviour Authority (MA) shall provide the following functions [15]:

- Collection of the misbehaviour reports generated by a misbehaviour detection system (or probe) embedded in the ITS-Ss. This activity consists of validating the structure of misbehaviour reports, filtering the received reports (e.g. depending on time period, geographic areas, ...), correlating the received reports and storing them in a local database.
- Investigation on the detected misbehaviours. This activity consists of assessing the accuracy and reliability of detected misbehaviour events, to analyze them to identify different misbehaviour patterns and then to decide whether a reported ITS-S is misbehaving, faulty or genuine. Machine Learning algorithms can be used for an efficient analyses of the expected large quantity of data in the received reports and the misbehaviour event types classification.
- Following the qualification of the investigated misbehaviour events, the MA shall take the appropriate response. The response to misbehaving ITS-S may be of different levels: no action, sending an alert to the user or to the ITS station's manufacturer or device operator, initiate the revocation process (e.g. blocking the ITS-S Enrolment Credential), etc.

The Misbehaviour Authority is part of the PKI as show in Figure 2.7. It requires its own certificate signed by the RCA and shall be able to communicate securely with other entities of the system [15]:

- using an off-line communication with the RCA to request a MA certificate;
- with ITS-S to receive reports and analyze them;
- with the EA and AA to get information about an ITS-S and trigger a reaction.

2.4.5 ITS-S Security Lifecycle management

The ITS-S Security Lifecycle includes the following stages (see Figure 2.8):

- initial ITS-S configuration during manufacture;
- enrolment;
- authorization;
- operation and maintenance;
- end of life.

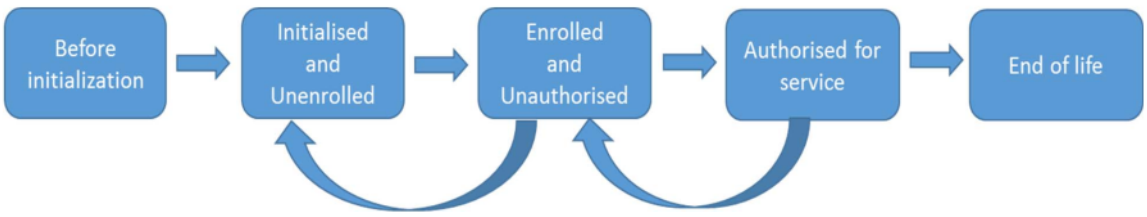


Figure 2.8: ITS Station Security Life Cycle [16]

2.4.5.A Manufacturer

As part of the ITS-S manufacturing process, the following information elements associated with the identity of the station shall be established within the ITS-S itself and within the Enrolment Authority (EA):

- In the ITS-S, the following information elements shall be established using a physically secure process:
  - a canonical identifier which is globally unique;
  - contact information for the EA and AA which will issue certificates for the ITS-S:
    - network address;

    - public key certificate.
  - the set of current known trusted AA certificates which the ITS-S may use to trust communications from other ITS-S;
  - a public/private key pair for cryptographic purposes (canonical key pair);
  - the trust anchor (Root CA) public key certificate and the DC network address;
  - in case of a multiple root CAs architecture, the TLM public key certificate and the CPOC network address.

- In the EA, the following three items of information shall be established, all associated with each other:
  - the permanent canonical identifier of the ITS-S;
  - the profile information for the ITS-S that may contain an initial list of maximum appPermissions (ITS applications IDs (ITS-AIDs) with Service Specific Permissions (SSPs), region restrictions and assurance level which may be modified over time;
  - the public key from the key pair belonging to the ITS-S (canonical public key).

2.4.5.B Enrolment

The ITS-S requests its enrolment certificate from the EA. After a successful enrolment process, the ITS-S shall possess an enrolment credential that shall be used in subsequent authorization requests.

For renewing the Enrolment Certificate at the EA, the ITS-S shall send an enrolment request message signed by the previous valid enrolment credential issued by this EA.

2.4.5.C Authorization

Having received the enrolment credentials, the ITS-S is able to request its authorization ticket(s) from the AA.

When in the state “Authorized for service”, the ITS-S has a set of authorization tickets to allow signed transmission of messages to any other ITS-S that do not reveal the canonical identity nor the enrolment credential of the transmitting ITS-S. When the complete set of authorization tickets is exhausted, the ITS-S cannot sign transmission of messages to others ITS-S and is back to the state Enrolled. Authorization Tickets are of limited validity and geographical region.

NOTE: Revocation of authorization tickets is not possible as passive revocation is preferred (the ITS-S receives ATs of limited validity period and of limited allowed preloading period i.e. issued before validity starts, renewing them frequently so that compromised ITS-S can be evicted from the ITS network by not

reissuing them new ATs). According to the European Certificate Policy, the validity period for ATs should not exceed one week and the preloading period three months [16, 18].

2.4.5.D Maintenance

If an EA or AA is added to or removed from the system, the Root CA shall inform enrolled ITS-Ss of this change.

When multiple Root CAs are used in the same Trust Domain, the trust relationship between the different PKIs is managed by a Trusted Third Party (Trust List Manager). If a Root CA is added or removed from the system, the TLM should inform enrolled ITS-Ss of this change.

The process for updating the trust information lists, such as the CTL and the CRL, and for publishing these lists by the associated trust authority, include different possible methods for updating the enrolled ITS-Ss:

- requesting ECTL, TLM certificates and their linkage information (TLM link certificate messages) to the distribution centre of the CPOC;
- requesting CRL and CTL from the distribution centre associated to the root CA;
- sending a trust information list (CRL or CTL) across a wireless interface e.g. using a RSU able to transmit the CRL/CTL on ITS G5; or
- providing information to a trusted maintenance entity to enable it to update an individual ITS-S in a controlled environment. This entity can be the Manufacture in the Initialization stage and an Operator during Maintenance.

2.4.5.E End of Life

In case of the device's end of life or following a compromise (revocation decided by its issuing EA), the ITS Station should be revoked and removed from operation in the ITS G5 communication network by means of a passive revocation mechanism, i.e. the EA shall reject the authorization of all the next Authorization Ticket requests for this specific ITS-S.

2.4.6 Usage of CTL and CRL by ITS-Ss

ITS stations use the CTL to update its trust information list in terms of trust anchors. This information allows to build a candidate certificate chain based only on the declared issuer component of ITS messages.

ITS stations extract the list of revoked CA certificates from the CRL and use this information while performing the validation of the certification path.

2.4.7 Renewing CA certificates and updating the PKI

For renewal of RCA and TLM certificates, link certificates messages should be used, signing the messages containing the new certificates (with a new pair of keys) with the previous but still valid certificate. These messages have an expire validity equal to the validity of the “old” certificate. Valid RCA certificates appear in the CTL and are removed when their validity expires. It is possible to see the linkage of certificates in the ECTL. The CRL contains the certificates revoked by active revocation (other than validity expiring, revoked by an authorized entity). For new TLM certificates, ITS entities can ask the CPOC about TLM link certificate messages, since the TLM does not provid any link information associated to a TLM certificate in the ECTL.

For renewal of EA and AA certificates, the CAs should send the new certificate request signed by the previous but still valid certificate. As for RCAs, valid certificates appear in the CTL and revoked certificates in the CRL.

A validity window should be considered when renewing certificates, assuring the time for ITS entities to update their PKI.

When broadcast over ITS G5, the CTL should be transmitted as delta CTL with the different entries (added or deleted in case of revocation) always generated with respect to the last issued CTL. Both the delta version and the full list version are identified by a Sequence Number, increased by one unit in each update. The delta and the full list version have the same sequence number, with the delta list sequence number being one unit more relatively to the full list it is generated from. For example, the delta CTL sequence number 5 exists in parallel with the CTL sequence number 5 and is generated with respect to the CTL 4 [16].

3

Algorithms Proposal

Contents

3.1 Traceability 27

3.2 Active Revocation of ATs 28

3.3 Security and Communications Requirements 33

3.1 Traceability

Traceability is required in ITS in order to make the behaviour of an ITS-S observable. Observability and other privacy requirements are described in Section 2.3.1 of Chapter 2. Based on the standard Authorization Request Message detailed in Appendix A, specifically the connection between the new created public key for the AT and the `keyTag` and its sharing in the `SharedATRequest` between the AA and the EA, a Traceability algorithm is proposed. The Algorithm was developed with the goal to link an Authorization Ticket (AT) to an Enrolment Credential (EC), which is linked to the canonical ID of the ITS Station (ITS-S), thus making the behaviour of an ITS-S observable.

An example situation of a compromised ITS-S is used, in which a neighbour ITS-S receives a message coming from a compromised ITS-S, classifies it as possibly compromised and sends the corresponding Misbehaviour Report (MR) to the MA, containing the AT associated with the possibly compromised message. From this moment on, the Misbehaviour Authority starts the Traceability process by communicating with the AA and the EA.

This algorithm is suitable for passive revocation of ITS-Ss, in which the EA revokes an ITS-S by revoking its EC, thus stopping the authorization of new ATs to the compromised ITS-S. The Algorithm is illustrated in Figure 3.1 and the detailed steps are presented in the section below.

3.1.1 Algorithm

3.1.1.A Algorithm Entities

The Algorithm includes the following entities:

- Misbehaviour Authority (MA);
- Enrolment Authority (EA);
- Authorization Authority (AA);
- ITS Station (ITS-S).

3.1.1.B Algorithm Steps

The Algorithm has the following steps:

1. An ITS-S reports another ITS-S by sending a Misbehaviour Report (MR) to the MA, containing the AT associated with the misbehaviour situation.
2. The MA analyses the MR and decides that the ITS-S is compromised.

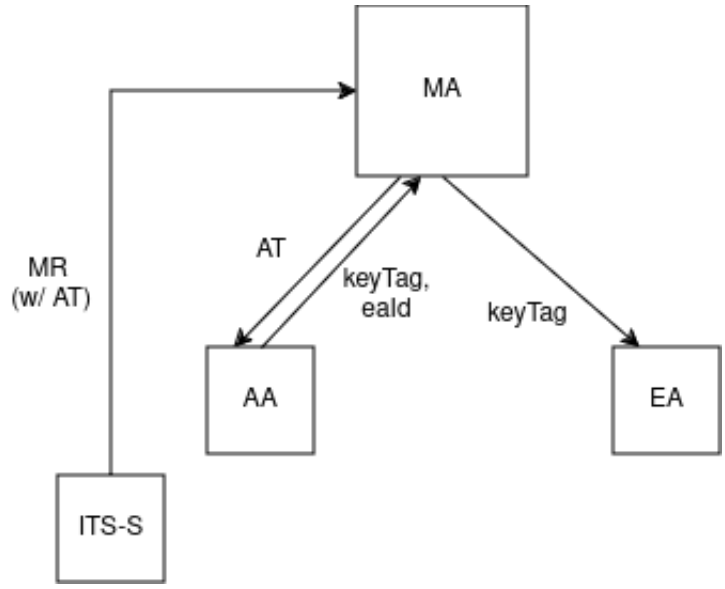


Figure 3.1: Traceability Algorithm in a compromised situation

3. The MA initiates the revocation process:

   (a) Contacts the AA asking for the keytag associated with the AT and the identifier of the EA associated with the ITS-S that issued the EC associated with the AT.

   (b) The AA sends back the associated keytag and the EA identifier (ID).

   (c) Contacts the EA sending the keytag associated with the AT.

   (d) The EA links the keytag with the EC of the compromised ITS-S, which is linked to the ITS-S canonical identity.

3.1.1.C Requirements

For linking the AT with its respective keytag, the AA has to store all active ATs and the associated keytags and EA IDs in a database. The EA shall group all the keytags of active ATs by the associated EC.

NOTE: Not only ATs within the validity period should be considered, but also the preloaded (issued before validity starts) ATs.

3.2 Active Revocation of ATs

Active Revocation is a problem not considered by ITS security standards. In this work, we developed an Algorithm, based on the Traceability algorithm presented above, for active revocation of ATs. This algorithm consists of the Traceability algorithm further developed to create an Authorization Tickets CRL

(ATCRL) to be disseminated in the ITS network by the used of location-based RSUs. The Algorithm steps are described in the section below and its illustration represented in Figure 3.2.

3.2.1 Algorithm

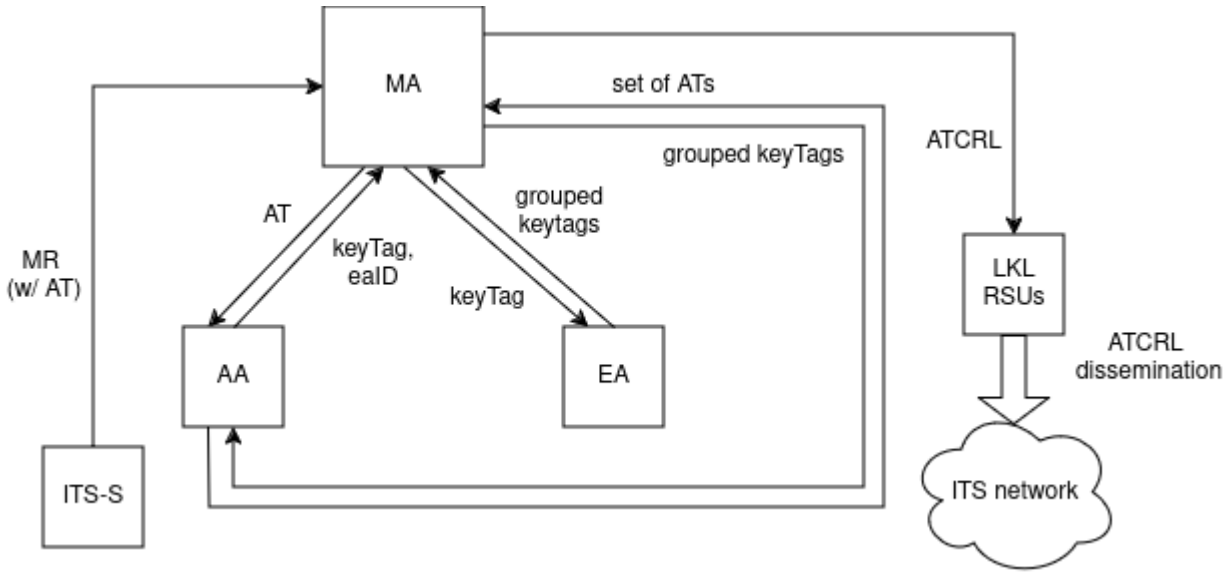


Figure 3.2: Active Revocation algorithm

The steps for the creation of the Active Revocation algorithm are the following:

1. An ITS-S reports another ITS-S by sending a Misbehaviour Report (MR) to the MA, containing the AT associated with the misbehaviour situation.
2. The MA analyses the MR and decides that the ITS-S is compromised.
3. The MA initiates the revocation process:
   (a) Contacts the AA asking for the keytag associated with the AT and the EA identifier.
   (b) The AA sends back the associated keytag and the EA ID.
   (c) Contacts the EA sending the keytag associated with the AT.
   (d) The EA links the keytag with the EC of the compromised ITS-S.
4. The EA sends back to the MA all the grouped keytags associated with the compromised ITS-S EC.
5. The MA sends the keytags to the AA, asking for all the ATs associated with the keytags.
6. The AA answers the MA by sending a list with the requested ATs.

7. The MA checks the Last Known Location (LKL) of the compromised ITS-S, adds the ATs identifiers (SHA-256 hashes) to the ATCRL containing the identifiers of the previous revoked and active (or in a preloading state) ATs, the respective validity period and, a nextUpdate field and a sequence number. It then sends the ATCRL to an RSU close to the LKL (denominated central LKL RSU or LKL RSU) who then sends it to its neighbours RSUs in a pre-defined distance radius for further dissemination in the network. The list sequence number is increased by one unit.

8. RSUs broadcast the ATCRL through ITS G5 access technology to the ITS network.

ITS-Ss receiving the ATCRL will then compare ATs of new incoming messages against the ATCRL, discarding messages whose ATs are present in the Authorization Tickets revocation list (ATCRL). Before comparing against the ATCRL, ITS-S will first verify the trust chain of the AT (with the CTL and CRL) and its validity period, discarding messages associated with expired ATs.

The ATCRL should be updated in the ITS network every time new entries are added to the list and have a nextUpdate field indicating the time when a next update is expected and consequently the time after which the CRL is to be expired, the sequence number should be increased of one unit and the ATCRL disseminated in the network. As with the CTL of Root CAs, the sequence number is a monotonically increasing counter, with increased value of 1 and a maximum value of 255.

3.2.1.A Requirements, Notes and Future Concerns

ITS-Ss should store the list of revoked ATs. The list is updated by RSUs dissemination or with the use of the Internet, by requesting the list to the MA, with possible RSUs and ITS-Ss relaying, as it happens with the CRLs issued by Root CAs. Since the validity period plus the preloading period of ATs are limited and there should not be a high number of revoked active ATs within that period, the ATCRL should have an appropriate size, even thought the number of active ATs in the network is very high.

If possible scalability or distribution problems arise, several strategies can be adopted for the dissemination of the ATCRL. The division of the ATCRL into multiple ATCRLs and distribution based on the compromised ITS-S last location, calculating a possible distance range considering the remaining of the validity of the ITS-S ATs and distributing the ATCRL within that range. Another option is using an extensible perimeter approach, where the list is first distributed within a specified perimeter around the LKL, to RSUs in the border and in a small distance outside of the specified perimeter, if the RSUs detect the use of any of the revoked ATs the perimeter is enlarged and the is list distributed in the additional area, and to new border and external RSUs, repeating the process. These strategies can be adopted besides the main geographical factor of division of the ATCRL, the ATs use range. For dissemination of the revoked ATs belonging to a compromised ITS-S in a broader distance range, the list can be send directly from the MA to other RSUs, than the central LKL RSU, and the same strategy of dissemination

adopted or a broader distance radius can be specified, where RSUs transmit the list in a sequential manner within that radius.

Another option for solving eventual ATCRL list scalability (size) problems that may arise is the distribution of delta ATCRLs by RSUs instead of the distribution of the full ATCRL. A delta ATCRL contains the added entries in relation to the last issued ATCRL, with a sequence number and a next update field, usually being of a smaller size than the full ATCRL. The sequence number is one unit more regarding the full ATCRL it is generated from, and equal to the new and updated ATCRL sequence number. For the use of delta ATCRLs an extra field should be added to lists, a `isFullList` flag indicating if the list is a full list (true) or delta list (false).

The addition of the validity period of ATs in each entry of the ATCRL is for ITS-Ss to know when to discard expired ATs from the list and to possibly reduce the ATCRL to the currently active ATs, excluding the ones in a preloading state (yet to become valid) by running an algorithm to build a smaller internal ATCRL containing only the revoked and active ATs. The option to add the starting date of ATs to the ATCRL adds a bit more memory to the list (equivalent to the size of the date), since it does not only includes the necessary expiration date but also the ATs starting date. This addition was considered not having a significant impact on the ATCRL list size, while reducing the number of comparisons against the ATCRL per each message received by an ITS-S. In this way, given the compromise between memory and performance, the little extra addition of memory to store the starting date would be compensated in terms of performance in the ITS-S message trust verification time complexity.

3.2.2 Decentralized Approach

The Active Revocation Algorithm presented above uses the Misbehaviour Authority (MA) as a centralized Authority, controlling all the Algorithm and by consequence, the revocation process. In this section, an alternative algorithm is proposed, where the role of the MA as a centralized authority in the algorithm is downsized by using direct communication between the AA and the EA, making use of the already established connection for the Authorization Validation protocol. In this way, the MA no longer serves as intermediary in the communication between the EA and the AA, rather has its role reduced to classifying the MR, assembling the ATCRL and sending it, either to the RSUs or as a response to an ATCRL request.

The Decentralized approach has the advantage to be faster in relation to the previous active revocation Algorithm, since it has fewer communications. In scenarios where the MA does not need the full control over the Active Revocation process, for keyTag data information retrieving and processing, the current Algorithm should be selected over the previous one.

The Decentralized Active Revocation Algorithm is illustrated in Figure 3.3 and the Algorithm steps are detailed below.

3.2.2.A Algorithm

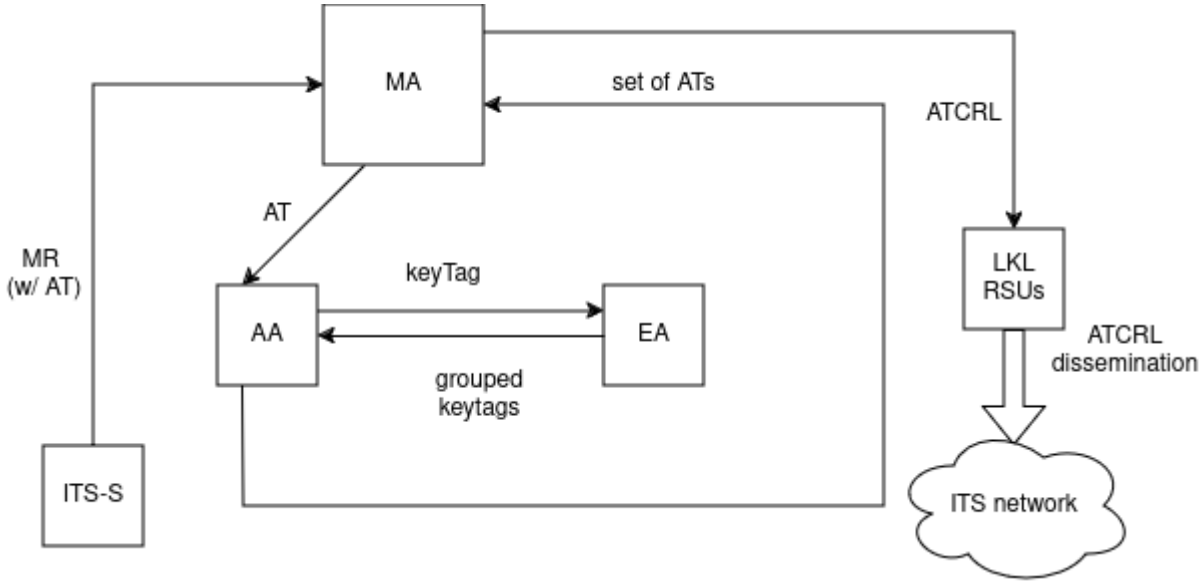


Figure 3.3: Active Revocation algorithm - decentralized approach

The algorithm has the following steps:

1. An ITS-S reports another ITS-S by sending a Misbehaviour Report (MR) to the MA, containing the AT associated with the misbehaviour situation.
2. The MA analyses the MR and decides that the ITS-S is compromised.
3. The MA initiates the revocation process:
   (a) Contacts the AA sending the AT authorizing the compromised message.
   (b) The AA sends the keytag associated with the AT to the EA.
   (c) The EA links the keytag with the EC of the compromised ITS-S.
4. The EA sends back to the AA all the grouped keytags associated with the compromised ITS-S Enrolment Credential (EC).
5. The AA sends to the MA the list of ATs associated with the keytags.
6. The MA adds the new entries corresponding to the ATs to the ATCRL and sends the (updated delta) ATCRL to the LKL RSU for transmission to its neighbour RSUs.
7. RSUs disseminate the list through ITS-G5.

3.2.2.B Notes

A new, faster, decentralized Traceability Algorithm can be induced from the decentralized approach, with a single step. The AA sends the keytag to the right EA, who then links the keytag to the ITS-S EC and by consequence, to its canonical identity.

3.3 Security and Communications Requirements

3.3.1 Communication Paths

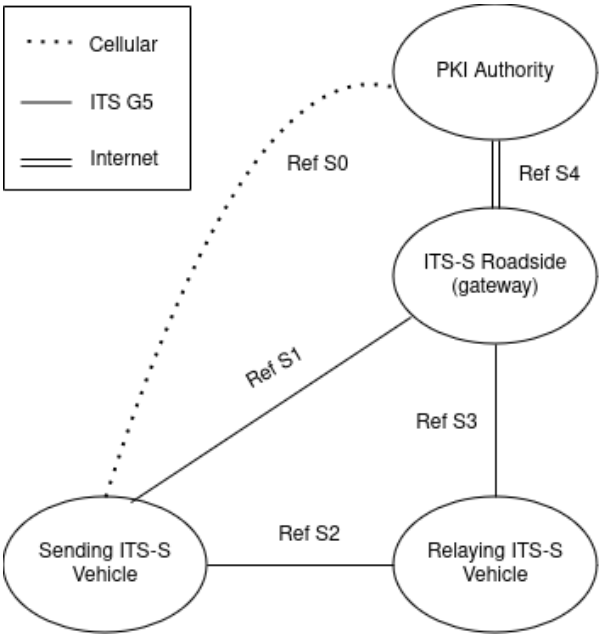


Figure 3.4: Communication paths for ITS-S communication with the PKI

Figure 3.4 presents three possible options for ITS-S communication with the PKI, in order to support security management services. Three communication paths are presented, one path via cellular network (reference point S0) and two alternative paths via ITS G5 to the ITS infrastructure (reference point S1 or reference points S2 and S3) using a relaying ITS-S roadside gateway to communicate with PKI authorities through the Internet (reference point S4).

ETSI ITS defines specific ITS-G5 (IEEE 802.11p) frequency channels for Security management services (supplementary channels can also be used when available). The allocated channels for Security Management messages are shared with Road Hazard Warning messages, such as DENMs. Cooperative road safety messages such as CAM are not shared in the defined channels nor in the specified supplementary channels [15, 16, 19, 20]. Table 3.1 shows the frequency ranges and intended usage to be used for cooperative ITS within the European Union.

	Frequency range [MHz]	Usage
ITS-G5D	5 905 to 5 925	Future ITS applications
ITS-G5A	5 875 to 5 905	ITS road safety related applications
ITS-G5B	5 855 to 5 875	ITS-non safey applications
ITS-G5C	5 470 to 5 725	RLAN (BRAN, WLAN)

Table 3.1: ITS-G5 frequency bands and intended usage [19]

RSUs should use the allocated channels for security management services (ITS-G5A frequency band, channels G5-SCH1 and G5-SCH2 [19]) or the supplementary channels when available (G5B to G5D [19]) for distribution of the ATCRL in the ITS network. For communication between the reporting ITS-S and the MA via ITS-G5 (reference points S1, S2 and S3), the specified channels for security management purposes should also be used.

3.3.2 Communication Profiles and Protocols

Several communication profiles are possible, depending on the path chosen for communication and the entities involved. As defined in ETSI TS 102 941 [16] for the security management messages of enrolment and authorization, in all communications using IP protocol (directly, over the reference points S0 and S4, or after forwarding, via the reference points S1 or S2 and S3) the protocols HTTP over TCP/IP should be used.

3.3.2.A Communication Profiles

Figure 3.5 to Figure 3.8 specify the layered set of communication protocols that are required to support communications between the sending ITS-S and other ITS stations and PKI authorities, using the example of request messages for instance requesting an EC (or AT) certificate to the EA (AA).

Figure 3.5 specifies the communication protocols that should be used between an ITS-S and PKI authorities when cellular network is used. The figure shows the mapping to ITS-S Communication layers represented in Figure 2.2. This figure specifies the reference point S1 of Figure 3.4.

The protocol stack of fig. 3.5 should be used in step 1 of the developed algorithms, the direct communication between the ITS-S and the MA, represented in Figure 3.4 by reference point S0. The access technology used can be upgraded to 5G.

Communications between PKI entities and between PKI entities and RSUs (step 1 to 7 of the Algorithms) use the seven layer OSI model with the same protocols as in Figure 3.5. In this type of communications, cable access technologies, such as fiber optics, can be used, since the entities are stationary, taking advantage of factors such as faster and more reliable speeds, lower latency and higher bandwidth when compared to cellular networks.

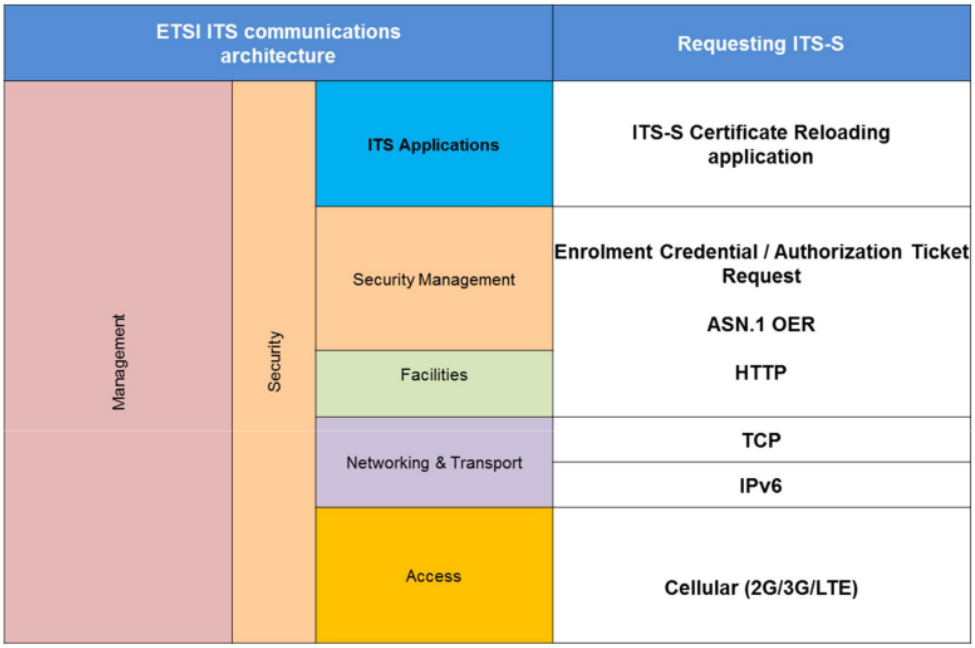


Figure 3.5: Communication protocols between the ITS-S and PKI authorities [16]

Figure 3.6 to Figure 3.8 depict the possible communication stacks when communication is based on ITS-G5 media, represented by the reference points S1, S2 and S3 in Figure 3.4. These figures specify alternative communication stacks available on ITS-G5 and the required security services (specified in ETSI TS 103 097 [17]) that should be applied for message authentication.

In the Active Revocation algorithms, all communication stacks can be used depending on the communication scenarios, when using an indirect path to communicate with PKI authorities, by communicating via ITS G5 to a relaying ITS-S roadside gateway.

In step number 1, instead of sending the MR directly to the MA (using a cellular connection and the protocol stack in Figure 3.5), the reporting ITS-S sends the MR to an ITS-S Roadside Gateway, via ITS-G5, who then forwards the report to the MA. This scenario is represented by reference points S1 and S4 in Figure 3.4. In this situation, the protocol stack to be used is represented in Figure 3.8, using Ipv6 over G5. This scenario is used for example when the sending ITS-S, who wishes to report the MR to the MA, does not have access to cellular internet and relaying RSUs are within the ITS-G5 5,9 GHz radio range.

NOTE: If the reporting ITS-S would to be answered back by the MA, the ITS network protocol GeoNetworking would be needed to send the answer back to the ITS-S via ITS G5. In this case, the protocol stack in Figure 3.6 would have to be used instead. This situation is not considered, since the sending ITS-S is merely reporting a suspicious behaviour to be further evaluated by the MA, not expecting an answer back.

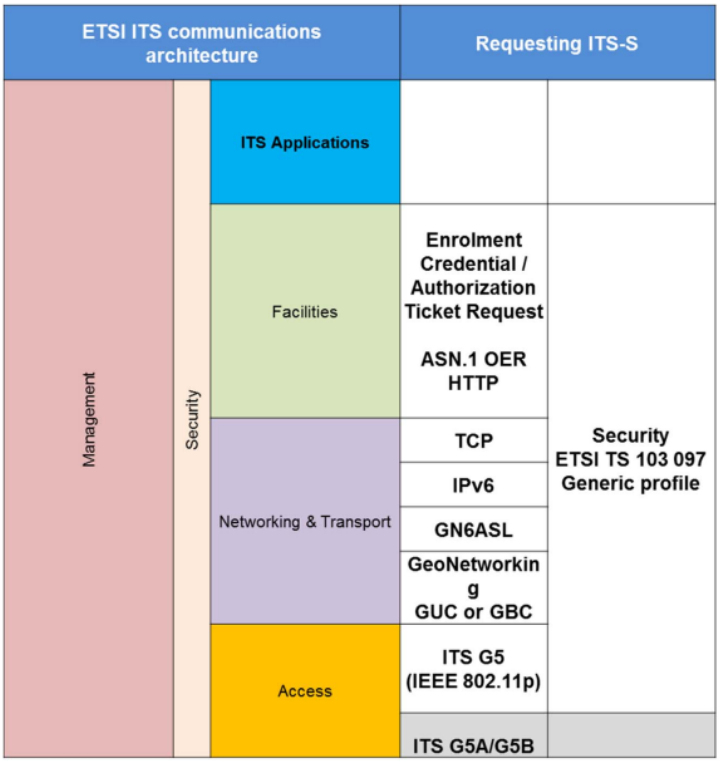


Figure 3.6: Communication protocols between an ITS-S and an ITS-S Roadside Gateway using Ipv6 over GeoNetworking [16]

Another situation can occur, a message is sent to another ITS-S vehicle who then forwards it to the ITS-S Roadside Gateway. This situation is represented in fig. 3.4 by the referencing points S2, S3 and S4. In this case, the reporting ITS-S would send the MR to another vehicle ITS-S who would then forward it to the relaying ITS-S Roadside Gateway to be sent to the MA. The protocol stack to be used is represented in figure Figure 3.6, using Ipv6 over GN. This situation can occur when the sending ITS-S does not have access to Internet via cellular communication and RSUs are not within the ITS-G5 5.9 GHz radio range, so it has to communicate via a relaying ITS-S vehicle.

For the dissemination of the ATCRL (step 8 of the Active Revocation algorithms), the protocol stack to be used is the one of Figure 3.7, using the ITS transport and network protocols BTP over GN.

3.3.3 Security in Communications

The developed Traceability and Active Revocation algorithms have the following security requirements:

3.3.3.A Confidentiality

- Messages are encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES) as defined in ETSI TS 103 097 [15];

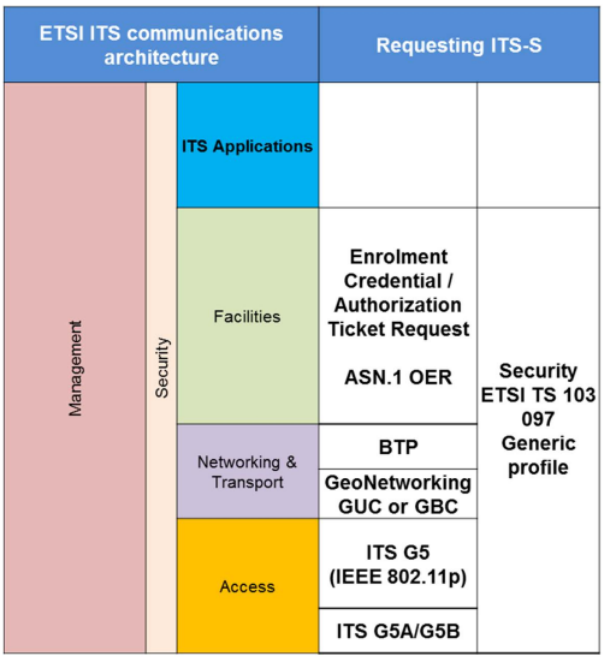


Figure 3.7: Communication protocols between an ITS-S Vehicle and an ITS-S Roadside Gateway using GN/BTP protocol [16]

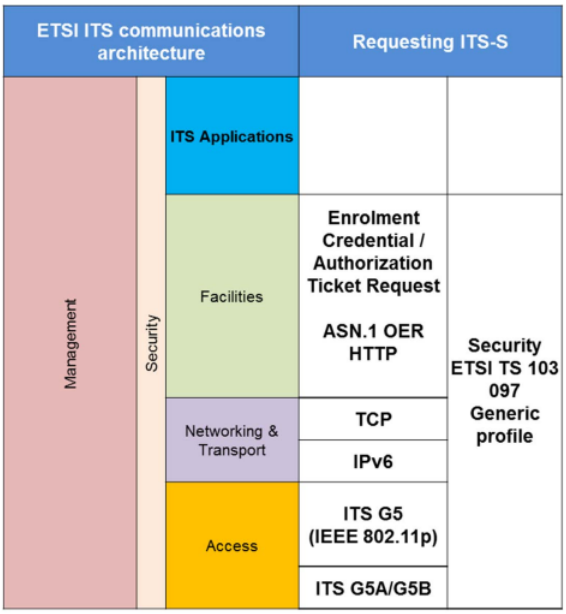


Figure 3.8: Communication protocols between an ITS-S Vehicle and an ITS Roadside Gateway using Ipv6 over G5 [16]

- Messages are encrypted with the public key of the receiving PKI authority certificate;
- All messages, except the ATCRL dissemination messages, shall be encrypted;

- No supplementary cryptographic layer such as TLS is required over HTTP;
- The ATCRL should be publicly accessible, thus not encrypted.

3.3.3.B Authentication and Integrity

- Messages are signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in ETSI TS 103 097 [15];
- Messages are signed using entities certificates:
  - ITS Stations sign using the Authorization Tickets (ATs) issued for the effect, i.e. with Security Management permissions;
  - PKI authorities sign with their private keys associated to their public keys.
- All messages must be signed;
- When forwarding messages in ITS-G5, no additional cryptographic procedures are needed, such as a new signature over the signed message.

3.3.4 Secure Message Data Structures

Messages contents are to be incorporated in ETSI TS 103 097 [17] secure message data structures introduced in Appendix A, namely in the field `tbsData.payload.content` of the `EtsiTs103097Data-Signed` data structure. The ITS-AID used for the active revocation service should be distinct from the other application service IDs.

4

Performance Evaluation

Contents

4.1 Overview 40
4.2 Data Dimensions, Cryptographic Operations and Access Rates 40
4.3 Formulas 43
4.4 Configuration scenarios 46

4.1 Overview

In this chapter, a study of the Active Revocation (AR) algorithms is conducted. This study includes a performance evaluation in multiple scenarios and a comparison between the two AR algorithms versions, the centralized and the decentralized version. For the analyses conducted, the data dimensions, cryptographic operations features and access rates presented in the next section are used.

4.2 Data Dimensions, Cryptographic Operations and Access Rates

4.2.1 ATCRL

The ATCRL is composed by the ATs entries, each containing the AT identifier and the respective validation period, by a sequence number and a `nextUpdate` field, plus a flag `isFullList` to indicate if the list is a full or delta list. Figure 4.1 illustrates the contents of an ATCRL.

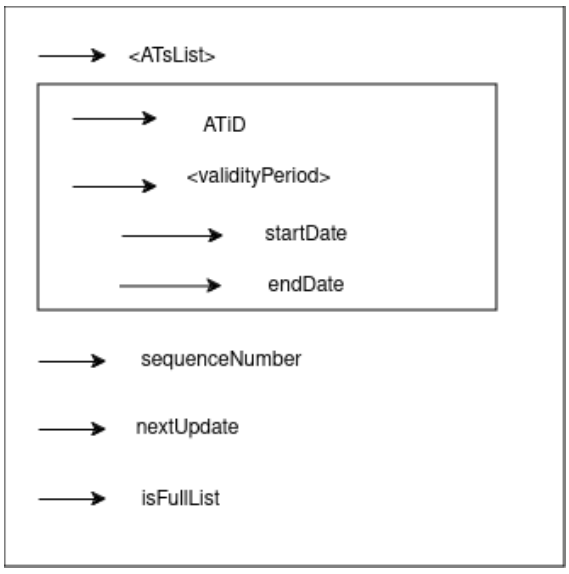


Figure 4.1: ATCRL components illustration

4.2.2 Messages Content dimensions

Table 4.1 represents the various messages contents of the Active Revocation Algorithms and their dimensions, together with common ITS messages, such as CAM and DENM, that may be sent as evidence in the Misbehaviour Report to the MA. The MR dimension was estimated containing long CAMs or DENMs and the respective ITS-S AT certificate for the message application, plus an extra space for the report message with the AT of the reporting ITS-S [21]. The eaId was estimated as a typical URL

Message content	Data dimension
short CAM	190 bytes [22]
long CAM	300 bytes [22]
DENM	300 bytes [22]
AT certificate	132 bytes [23]
Misbehaviour Report (MR)	1 kbyte
keyTag	16 bytes [16]
eaID	75 bytes

Table 4.1: Messages contents and respective dimensions

ATCRL component/field	Dimension
AT identifier (SHA-256)	32 bytes
startDate	4 bytes
endDate	4 bytes
sequenceNumber	2 bytes
nextUpdate	4 bytes
isFullList	1 bit

Table 4.2: ATCRL components dimension

address size. Table 4.2 represents the contents of an ATCRL and the respective data dimensions.

4.2.3 Cryptographic Operations

The following section presents the cryptographic information for signing and encrypting messages with the cryptographic operations presented in section 3.3.3. Table 4.3 shows the cryptographic operations data and respective dimensions. table 4.4 presents the ciphertext to plaintext ratio of an ECIES with a key length of 512 bits, the key length of ITS entities encryption key (public key) used to encrypt messages. table 4.5 presents the execution time in milliseconds for the SHA-256 hashing algorithm, used to digest messages for signing with the ECDSA. table 4.6 presents encryption and decryption rates using an ECIES [24] with the ITS entities private key size of 256 bits for decryption and the associated public key size of 512 bits for encryption.

Cryptographic Operation Data	Dimension
public key	64 bytes [23]
private key	32 bytes [23]
certificate	132 bytes [23]
certificate identifier (SHA-256 hash)	32 bytes
signature	69 bytes [23]

Table 4.3: Cryptographic Operations data and dimensions

From Table 4.4 we can conclude the overhead added by the encryption process is negligible when encrypting more than 1 kB of information [24].

In Section 3.3.3, we can observe the times taken by the SHA-256 operation increase with the in-

Plaintext (bytes)	Ciphertext (bytes)	Ratio
16	225	14.06
32	241	7.53
64	273	4.27
128	337	2.63
265	465	1.82
512	721	1.41
1024	1233	1.2

Table 4.4: Cryptogram lengths and ratio for different plaintext sizes with an ECIES 512 bits key [24]

Text File (kB)	SHA-256 (ms)
877	55.478
1653	82.523
3758	187.98
5071	229.215
10,021	436.442
14,034	647.784
21,854	932.596

Table 4.5: SHA-256 execution times [25]

crease of the input data in an almost linear way. For calculations, we used the linear characteristic of the SHA-256 execution times with the input data to calculate the time taken by the SHA-256 over the messages of the algorithm, adjusting the linear factor to the messages dimensions.

Operation	Key Length	Rate
Encryption	512 bits	0.08 ms / byte [24]
Decryption	256 bits	0.0167 ms / byte [24]

Table 4.6: Encryption and Decryption rates for ITS entities public and private key sizes with ECIES

With respect to the ECDSA for signature of messages, the times for signature generation and signature verification over the SHA-256 hash of messages were calculated using the ECIES rates presented in Table 4.6. Signature generation uses private key encryption and signature verification uses public key decryption. The rates of encryption and decryption using ECIES are equal for the same key length [24]. The resulting times are presented in table 4.7.

The total times for signature generation and verification of a message are calculated by adding the SHA-256 execution time of the message plus the respective signature operation time over the 256 bits hash.

4.2.4 Access Technologies

The access technologies indicated in Figure 3.4 and used in the Active Revocation algorithm in the different communication paths, between PKI entities communication and to RSUs, and for RSUs message

Cryptographic Operation	Time
Signature generation over 256 hash	0.53 ms
Signature verification over 256 hash	2.56 ms

Table 4.7: Signatures operations time over the SHA-256 hash of a message

broadcast dissemination to the ITS network, are presented in Table 4.8 with the typical average data rates. Fiber Optics rate is a common data rate for professional fiber optics connections such as the ones in use.

Access Technology	Typical Data Rate
ITG-G5	6 Mb/s [19]
Cellular upload	12 Mb/s [26]
Fiber Optics	1 Gb/s

Table 4.8: Active Revocation algorithm Access Technologies data rate

4.3 Formulas

The equations used for calculation of the times taken by the two algorithms approaches (centralized and decentralized) are presented in this section, where each expression represents the time taken for the transmission of the messages for each access technology used. These equations use the general form of time calculation, represented by:

$$time = \frac{data}{accessRate} \tag{4.1}$$

For the three different communication access technologies used in the Active Revocation algorithms, we have the following three equations for calculation of the time taken by each communication technology over its respective links, using the data rates presented in Table 4.8:

$$cellular = \frac{data}{6\ Mb/s} \tag{4.2a}$$

$$fiberOptics = \frac{data}{1\ Gb/s} \tag{4.2b}$$

$$ITS\text{-}G5 = \frac{data}{12\ Mb/s} \tag{4.2c}$$

Before dividing into the two Algorithms time equations, there is a number of general expressions common to both algorithms we can define.

First, we start by defining the number of ATs belonging to the compromised ITS-S to be revoked with the active revocation algorithms by $n0$ and the number of ATs present in the ATCRL before the addition of the new AT by $n1$. Having in account the defined variables, we can present the general expressions common to both AR algorithms.

The dimension of the ATCRL is calculated using the following general equation:

$$ATCRL = (n0 + n1)(ATiD + validityPeriod) + sequenceNumber + nextUpdate + isFullList \Leftrightarrow$$
$$ATCRL = (n0 + n1)40 + 7\ bytes \tag{4.3}$$

The grouped keytags and set of ATs are calculated using the expressions:

$$groupedkeytags = n0 \times keytag \tag{4.4}$$
$$setofATs = n0 \times AT \tag{4.5}$$

The path chosen for communication between the reporting ITS-S and the MA is the direct path, using cellular networks, represent by reference point S0 in Figure 3.4. This is the most common path to be used.

For both versions of the Active Revocation algorithms, the time taken by communications over cellular and ITS-G5 access technologies is the same, since there is no changes between the algorithms over these access communications connections. The cellular rate is calculated for the best case scenario, considering that there are no other messages shared in the available cellular rate. As for the ITS-G5 link, security messages are distributed in the specified channels, presented in section 3.3.1. In the scenarios considered, no background messages, such as DENM, are estimated to be shared in the available channels at the time of the ATCRL distribution, since this is the common scenario due to the sporadic and non regular nature of the messages. The ATCRL is broadcast by RSUs to ITS stations vehicles.

We have the following two expressions for the communication time over cellular networks and ITS-G5 in the Active Revocation algorithms:

$$cellular = \frac{MR}{cellularUploadRate} = \frac{1\ kbytes}{12\ Mb/s} = \frac{1000 \times 8\ bits}{12 \times 1000000\ b/s} \approx 0.67 \times 10^{-3}\ s \tag{4.6}$$

$$ITS\text{-}G5 = \frac{ATCRL}{ITS\text{-}G5rate} = \frac{(n0 + n1)40 + 7\ bytes}{6\ Mb/s} \tag{4.7}$$

For the distribution of the ATCRL to the last known locations RSUs, the MA sends the list to a specific central LKL RSU, who then disseminates the ATCRL to its neighbours RSUs in a pre-defined radius. The variable representing the number of RSUs receiving the ATCRL from the LKL RSU is $RSUs$.

Having the general expressions, the calculus of each algorithm time over the fiber optics links is presented in the following two equations, each related to one version of the active revocation algorithm, centralized and decentralized. The differences between the two approaches are present in the fiber optics link connections, since the decentralized version needs fewer connections between entities to

achieve the same output, having the counter of less control over the algorithm by the MA.

The time taken by the centralized active revocation algorithm (CARA) messages sent over the fiber optics links is calculated with the following expression:

$$fiberOptics = \frac{AT + (keytag + eaID) + keytag + n0keytags \times 2 + n0AT + ATCRL + ATCRL \times RSUs}{fiberOpticsRate} \tag{4.8}$$

The time taken by the decentralized active revocation algorithm (DARA) approach is calculated with the following expression:

$$fiberOptics = \frac{AT + keytag + n0keytag + n0AT + ATCRL + ATCRL \times RSUs}{fiberOpticsRate} \tag{4.9}$$

We can see the decentralized version of the algorithm requires less exchange of messages, resulting in less data being exchange between entities over the fiber optics links.

For simplification, we consider the Round Trip Time (RTT) between each entity present in the algorithm the same and equal to the average RTT in the same country, considered Portugal:

$$RTT = 15\ ms \tag{4.10}$$

The transport layer algorithm used in the algorithm communications is TCP, requiring an initial RTT for establishing a session between the communication parties before the sending of a message. As described in section 3.3.2, TCP is chosen for reliability purposes, since the messages involved in the algorithm are critical and sequential, all messages require a confirmation of reception from the destination entity, given in the TCP protocol at the transport layer. For the calculus of the time taken by each message sent in the Algorithm, the RTT with the TCP slow start are considered.

All communications employ TCP except the last, the dissemination of the ATCRL in the ITS network through ITS-G5, using the protocols detailed in 3.3.2. In this step, the RTT is not considered. For the transmission of the ATCRL from the LKL RSU to its neighbours RSUs, the RTT is considered ($RTT = 3\ ms$) since the entities are close to each other.

As for the headers of the diverse protocols corresponding to the protocol stack of a message, the following values are considered:

The dimensions represented in Table 4.9 are added to the messages when calculating the time taken by each message sent with the fiber optics links. The protocols headers sizes are fixed, except the HTTP protocol, where the typical header size for the type of services employed in the algorithms

Protocol	Header Dimension
Ethernet	26 bytes
IPv6	40 bytes
TCP	20 bytes
HTTP	500 bytes

Table 4.9: Protocols headers sizes

(without cookies and user agent extended features) is considered.

For the cellular connection, the protocols headers are included in the cellular rate measure by Speedtest [26], except the HTTP protocol, since it measures the rates at the application layer using TCP. The HTTP header size is added to the cellular message (the MR) dimension for the time calculation. For the ITS-G5 dissemination, the transport and network protocols used are BTP over GeoNetworking (GN), as indicated in section 3.3.2. The sizes of these protocols are considered negligible in the calculation of the time taken by the message, since the message (ATCRL) size is of a much bigger dimension than the size of the protocols headers, which are around the TCP and IP protocols dimensions.

4.4 Configuration scenarios

The changeable (configurable) variables in the different scenarios for the employment of the algorithm are the following:

- Number of ATs belonging to the compromised ITS-S stations to be revoked ($n0$);
- Number of ATs present in the ATCRL before the addition of new ATs ($n1$);
- Number of RSUs in the pre-defined radius receiving the ATCRL from the LKL RSU to broadcast it into the ITS network ($RSUs$).

Having these variables defined, we have configured the scenarios that follows.

4.4.1 Scenario 1 - Base Scenario

Configuration:

Variables	Values
$n0$	100
$n1$	0
$RSUs$	20

Table 4.10: Variables configuration for scenario 1

In this scenario, there is no ATs previously present in the ATCRL and the number of ATs to be revoked is the maximum number of active ATs an ITS-S can hold at the same time [18]. A number of 20 RSUs was

considered for the initial area in which the ATCRL is to be disseminated. For the considered scenario, we have obtained the following results for the two Active Revocation (AR) algorithm approaches:

Communication	AR centralized	AR decentralized
Cellular	23.5 ms	23.5 ms
Fiber Optics	427.5 ms	397.5 ms
ITS-G5	5.3 ms	5.3 ms
Total	456.3 ms	426.3 ms

Table 4.11: Active Revocation algorithms transmission times

With the results of table 4.11, we can observe the difference between the use of the centralized and the decentralized versions of the Active Revocation algorithm. There is a difference of 97.5 ms, representing the fewer number of messages needed by the decentralized AR algorithm version.

4.4.2 Scenario 2 - Increase in RSUs

In this scenario, we maintain the values of scenario 1, increasing the number of RSUs receiving the ATCRL from the LKL RSU for disseminating it into the network, thus comparing the impact in time with the increase of RSUs in the pre-defined area. We will compare three cases ($RSUs = 20, RSUs = 100,$ and $RSUs = 1000$).

In this scenario, we have the following values:

Variables	Values
$n0$	100
$n1$	0
$RSUs$	20, 100, 1000

Table 4.12: Variables configuration for scenario 2

Since there is no difference in this step of the two AR algorithms, we will use the faster version, the decentralized AR algorithm, for testing the impact of the number of RSUs in the pre-defined area receiving the ATCRL to broadcast it. The results obtained are shown in Table 4.13.

Communication	$RSUs = 20$	$RSUs = 100$	$RSUs = 1000$
Cellular	23.5 ms	23.5 ms	23.5 ms
Fiber Optics	397.5 ms	1237.5 ms	10687.5 ms
ITS-G5	5.3 ms	5.3 ms	5.3 ms
Total	426.3 ms	1266.3 ms	10716.3 ms

Table 4.13: Decentralized AR algorithm time increase with RSUs

As expected, the number of RSUs ($RSUs$) in the pre-defined area receiving the ATCRL from the neighbour LKL RSU for disseminating it to the network, has a significant impact in the total time of the AR algorithm. The use of a high RTT value of 3 ms ($RTT = 3ms$) plays an important role in the times

presented, due to the close proximity between the RSUs. The value of the RTT could be reduced, even considered negligible in some situations, such as the distribution of the list in a sequential manner from RSU to RSU with direct links between them. If the Round Trip Time (RTT) would be considered 1 ms, the time taken by the distribution of the ATCRL through the RSUs in the pre-defined area would decrease in a proportional manner of 1/3.

4.4.3 Scenario 3 - Use of delta ATCRLs

In scenario 3, we test and compare the difference in time between the use of a delta ATCRL and the full ATCRL. The scenario was thought of having an ATCRL with 1000 ATs. If each compromised ITS-S holds 100 ATs to be revoked, it is the equivalent of having the ATs of 10 compromised ITS-Ss in the list. For the adding of ATs to the ATCRL, the maximum number of active ATs an ITS-S can hold, 100 ATs, is considered. For the number of RSUs, 100 RSUs were chosen, representing a larger area than in scenario 1.

For this scenario, the values of the defined variables are represented in Table 4.14.

Variables	Values
n0	100
n1	1000
$RSUs$	100

Table 4.14: Values of variables for scenario 3

We test two options:

a) No delta ATCRL is used and the full ATCRL is transmitted over ITS-G5 by RSUs.

b) A delta ATCRL is used, containing only the updated entries in relation to the last issued ATCRL, which will be 100.

The goal of this scenario is to analyse the difference in the use of a delta ATCRL instead of the full ATCRL. Once again, the fastest algorithm, the decentralized version, was used, obtained the results in Table 4.15.

Communication	delta ATCRL	full ATCRL
Cellular	23.5 ms	23.5 ms
Fiber Optics	521.2 ms	6278.3 ms
ITS-G5	5.3 ms	59.5 ms
Total	550 ms	6361.3 ms

Table 4.15: Decentralized AR algorithm times with the use of a delta ATCRL and the full ATCRL

The difference in the total times is due to the size of the ATCRL transmitted through the algorithm, with the full ATCRL being significantly bigger and taking more RTTs to transmit from one entity to another

(from the MA to the LKL RSU or between the RSUs in the pre-defined area). The difference in ITS-G5 is not so noticeable, since the RTT is considered zero due to the proximity between the vehicles receiving the ATCRL and the RSUs. With this result, the benefits in terms of time of using delta versions of the ATCRL become evident, also having the benefit of transmitting less data, which is easier to transmit and less prone to errors.

It is important that algorithms for active revocation of ATs have a reduced time. If a given compromised ITS-S holds active ATs, the compromised ITS-S can use those ATs to send messages to the ITS network. These messages can potentially be compromised and endanger the ITS functioning and the life of users. It is of vital importance to have an active revocation algorithm with a reduced time for a fast ATCRL dissemination, in order for ITS-Ss to discard messages coming from the compromised ITS-S.

NOTE: There are security measures specific to applications to handle possible misleading ITS messages coming from the compromised ITS-S. Examples are CAM comparison to other CAMs received and the reception of one-hop DENMs within a valid (possible) GeoNetworking protocol dissemination distance from the source location [27].

4.4.4 Scenario 4 - Addition of cryptographic operations

So far, in the scenarios considered, we have not measured the processing time of the cryptographic procedures over the various communication messages of the Algorithm.

As detailed in section 3.3.3, all messages except the ATCRL are signed, encrypted and decrypted, and the signature verified, in every communication exchange in the Active Revocation algorithm. The ATCRL is signed by its issuing entity, the MA, and its forwarding by the RSUs does not require any additional cryptographic operations, such as re-signing the ATCRL.

The total time taken by a message exchange in the algorithm is computed as follows:

$$\begin{aligned} Total\ time = {} & Message\ generation + Message\ signature + Message\ encryption \\ & + Message\ transmission + Message\ decryption + Message\ signature\ verification \end{aligned} \quad (4.11)$$

The message generation step is done at the application layer and can be considered negligible when comparing to the cryptographic processes times of signature and encryption as more computer power is required for the computation of the cryptographic procedures, as stated in Vieira et al. [13].

Using the information in tables 4.3 to 4.7, we computed the behaviour of the Algorithm when cryptographic measures are applied. The times of the algorithms including the cryptographic security processing operations are presented in Table 4.16, together with the times without security processing for comparison. The scenario contemplates the revocation of 100 ATs of a reported compromised ITS-S and the use of a delta ATCRL ($n0 = 100$ and $n1 = 0$), the same values considered for Scenario 1 without

security operations. The number of RSUs considered in the pre-defined area to disseminate the ATCRL is 100 ($RSUs = 100$).

Communication	DARA w/ security	DARA w/o security	CARA w/ security	CARA w/o security
Cellular	145.15 ms	23.5 ms	145.15 ms	23.5 ms
Fiber Optics	3129.6 ms	1237.5 ms	3341.46 ms	1267.5 ms
ITS-G5	7.96 ms	5.3 ms	7.96 ms	5.3 ms
Total	3282.71 ms	1266.3 ms	3494.57 ms	1296.3 ms

Table 4.16: AR algorithms times with security operations

From the results, we can observe the influence of the cryptographic operations of encryption and decryption, signature generation and signature verification of messages over the Algorithm. Since the cryptographic procedures are very computational demanding, requiring high computer power, they are also very time consuming, making for most of the time taken by the Active Revocation algorithm. This can be observed from the difference of the AR decentralized total algorithmic times in Table 4.16.

Another outcome can be observed from the table results, the difference between the two algorithm versions, CARA and DARA, has increased. This increase is natural, since the centralized version has more connections (messages exchanges) between entities and due to the addition of the cryptographic processing times for message exchange, the difference between the two algorithms became larger. This difference is shown at the fiber optics times and we can observe that, even though it is more representative with the inclusion of the security times, it is not very significant.

4.4.5 Scenario 5 - Alternative paths

Figure 3.4 shows three alternative paths for the message exchange between the reporting ITS-S and the MA, the sending of the MR.

So far, in the scenarios considered, we have used the most normal and common path to be used, the direct path between the two entities using cellular networks.

In the case of the reporting ITS-S not having access to cellular internet, two alternative paths using ITS-G5 are given. In one path, represented by the reference points S1 and S4 in Figure 3.4, the ITS-S sends the report to a relaying RSU, which then forwards the MR to the MA. This path adds an additional communication exchange, impacting the total time of the algorithm. The time for sending the MR with this option is given by the following formula:

$$time = \frac{MR}{ITS\text{-}G5rate} + \frac{MR}{fiberOpticsRate} \tag{4.12}$$

The third option is for the case when the relaying RSU is not in ITS-G5 communication distance reach. In this case, the reporting ITS-S sends the MR to a neighbour ITS-S vehicle, which then forwards

the MR to another vehicle or in the case it is in reach, to the relaying RSU, which forwards it to the MA. This option is represented by the reference points S2, S3 and S4. The time taken for this communication path depends on the number of hops, and can be calculated using the following formula with the number of hops represented by $nHops$:

$$time = \frac{MR}{ITS\text{-}G5rate} \times nHops + \frac{MR}{fiberOpticsRate} \tag{4.13}$$

Considering a scenario of 3 hops ($nHops = 3$), two relaying ITS-S vehicles and a relaying RSU, we can compare the times taken by the three alternative paths to send the MR from the reporting ITS-S to the MA. The results are shown in the following table:

Path	Direct	w/ relaying RSU	w/ relaying vehicles and RSU
Time for MR communication	145.15 ms	146.27 ms	150.72 ms

Table 4.17: Communication time over the various communication paths for sending the MR

From the Table 4.17, we can observe the increase in time between the three communication path options. Since the number of hops in the ITS network to reach a relaying RSU is predicted to be relatively low, as the example 3 hops, the change of the path chosen to send the MR to the MA will not have a time impact in the algorithms.

5

Conclusion

Contents

5.1 Synthesis of the work 53

5.2 Results and Conclusions 54

5.3 Future work 54

5.1 Synthesis of the work

In this work, a study of ITS security management was conducted, resulting in a survey of the ETSI standards applicable across the globe. In this survey, the security model of ITS messages is detailed, presenting how ITS stations send authenticated and authorized messages in the network, encrypted when needed, while keeping the privacy of ITS users. An important requirement to hold about ITS stations is the protection of their identities with the use of pseudonym certificates, the ATs, keeping the identity of ITS-S secret while having the possibility of messages to be traced back to the sender by a responsible and certified authority for the effect. The security management system was presented, named Cooperative-ITS Security Certificate Management System or C-ITS Trust Model, presenting the Certificate Authorities (CAs) of the ITS PKI, that build the certificate chains in which ITS stations base to trust other ITS-Ss messages. Certificate Trust Lists (CTL) and Certificate Revocation Lists (CRL) containing the certificates of the CAs are distributed throughout the network, through RSUs, in order to keep the list of trusted CAs updated to ITS-Ss.

A problem with the revocation of ATs was detected. The revocation of ATs is conducted with passive revocation, not issuing more ATs to compromised ITS-SS. Even though ATs have a short validity period, the time period between an ITS-S is classified as compromised and the end of the validity of its ATs leaves the possibility of the compromised ITS-S to communicate in the network. For solving the problem, an active revocation algorithm was proposed based on an Authorization Tickets Certificate Revocation List (ATCRL) to be distributed in the network and used by ITS-Ss to discard messages coming from the compromised ITS-S, discarding messages signed with the revoked ATs present in the list. For the development of the active revocation algorithm, a traceability algorithm was developed, to trace back the active ATs held by a compromised ITS-S from one of its messages sent together with the respective message application AT. After the traceability process, the active revocation of ATs begins, with the MA gathering the ATs of the compromised ITS-S and adding them to the ATCRL. The ATCRL is then distributed through RSUs to the ITS network, when vehicle ITS stations receiving the list can compare the ATs associated with the incoming messages against the ATCRL, discarding messages which ATs are present in the list.

Two approaches for the active revocation algorithm were developed, a centralized approach, where the MA has the total control of the algorithm process, and a decentralized approach, were the role of the MA as centralized authority is reduced, having less control over the algorithm. Throughout the development, the requirements and notes of the algorithms were detailed, including future strategies for distribution and scalability problems of the ATCRL that may arise.

Several scenarios were built to analyse the algorithms, testing the differences between the two active revocation algorithms versions, the use of a larger number of RSUs to distribute the ATCRL, the use of a delta ATCRL instead of the full ATCRL, the impact of the necessary cryptographic operations and the

use of alternative paths for sending the MR to the MA. For each scenario, conclusions were drawn, as shown next.

5.2 Results and Conclusions

From Scenario 1, we concluded that the use of the decentralized active revocation algorithm is faster than the centralized approach, being the preferred choice. With Scenario 2, we saw the increase in time with the increase in RSUs to distribute the ATCRL. In Scenario 3, we could observe the benefit in using delta versions of the ATCRL to update the revoked ATs in the ATCRL, instead of sending the full ATCRL to ITS stations every time the list is updated. In Scenario 4, we observed the high impact on time of the cryptographic operations for signature and encryption of messages, necessary in the algorithms. In Scenario 5, we compared the difference in time between the use of the different communication paths to send the MR to the MA, understanding the low impact on time of the use of alternative paths through ITS-G5 to send the MR when the sending ITS-S does not have access to cellular networks.

5.3 Future work

Several strategies can be adopted for distributing the ATCRL from the MA to RSUs to be disseminated in the ITS network. A first strategy, consists in the division of the ATCRL in geographic areas, and the distribution of the respective lists in those areas. A second strategy, is the incremental increase of the defined area to distribute the ATCRL, with the movement of the compromised ITS-S outside of the defined perimeter. Lastly, a third strategy could be the definition of more than one central LKL to distribute the ATCRL, in a pre-defined area around them. To optimize the algorithm, the ATCRL could be distributed from RSU to RSU instead of a centralized manner, from the LKL RSU to the others.

More studies can be done in the algorithms, simulating them and exploring possible optimizations, such as the mentioned routing between RSUs or other software optimizations. The ATCRL is developed because the ATs belonging to an ITS-S cannot be linked to each other, so there is not a way to link an AT of a compromised ITS-S to the other ATs (thus the necessity of a list). If an active revocation algorithm is developed in which the ATs of an ITS-S can be linked to each other, perhaps based on a constant only to become public in case of ATs revocation, the necessity of a list would be reduced. This optimization strategy would have to be implemented at the moment of creation (and issuing) of the ATs to ITS stations, and would be a way to optimize the developed algorithm, by decreasing the load of the ATCRL.

An implementation of the algorithms can be conducted, in a real system or in a simulation environment, testing the models defined in this work and the performance evaluation conducted. Moreover,

we propose that future work explore the described optimization strategy of linking the ATs, keeping the privacy requirements of ITS stations of pseudonymity and unlinkability of ATs, including between the EA and AA at the enrolment and authorization process.

Bibliography

[1] ETSI, “En 302 665 - v1.1.1 - intelligent transport systems (its); communications architecture,” 2010.

[2] ——, “En 302 636-4-1 - v1.4.1 - intelligent transport systems (its); vehicular communications; geonetworking; part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; sub-part 1: Media-independent functionality,” 2020.

[3] B. Hinden and D. S. E. Deering, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 2460, Dec. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2460

[4] ETSI, “En 302 636-6-1 - v1.2.0 - intelligent transport systems (its); vehicular communications; geonetworking; part 6: Internet integration; sub-part 1: Transmission of ipv6 packets over geonetworking protocols,” 2013.

[5] ——, “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,” 2017.

[6] J. Postel, “User Datagram Protocol,” RFC 768, Aug. 1980. [Online]. Available: https://www.rfc-editor.org/info/rfc768

[7] ——, “Transmission Control Protocol,” RFC 793, Sep. 1981. [Online]. Available: https://www.rfc-editor.org/info/rfc793

[8] ETSI, “En 302 637-2 - v1.4.1 - intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service,” 2019.

[9] ——, “En 302 637-3 - v1.3.1 - intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service,” 2019.

[10] ——, “Ts 103 301 - v1.2.1 - intelligent transport systems (its); vehicular communications; basic set of applications; facilities layer protocols and communication requirements for infrastructure services,” 2018.

[11] ——, “Tr 103 562 - v2.1.1 - intelligent transport systems (its); vehicular communications; basic set of applications; analysis of the collective perception service (cps); release 2,” 2019.

[12] ——, “En 302 890-1 - v1.2.0 - intelligent transport systems (its); facilities layer function; part 1: Services announcement (sa) specification,” 2018.

[13] E. Vieira, J. Almeida, J. Ferreira, T. Dias, A. Vieira Silva, and L. Moura, “A roadside and cloud-based vehicular communications framework for the provision of c-its services,” *Information*, vol. 14, no. 3, 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/3/153

[14] C-Roads, “The platform of harmonised c-its deployment in europe,” last access on 01/2024. [Online]. Available: https://www.c-roads.eu/platform.html

[15] ETSI, “Ts 102 940 - v2.1.1 - intelligent transport systems (its); security; its communications security architecture and security management; release 2,” 2021.

[16] ——, “Ts 102 941 - v1.4.1 - intelligent transport systems (its); security; trust and privacy management,” 2021.

[17] ——, “Ts 103 097 - v2.1.1 - intelligent transport systems (its); security; security header and certificate formats; release 2,” 2021.

[18] E. Comission, “Certificate policy for deployment and operation of european cooperative intelligent transport systems (c-its),” 2018, last access on 02/2024. [Online]. Available: https://cpoc.jrc.ec.europa.eu/data/documents/c-its_certificate_policy-v1.1.pdf

[19] ETSI, “En 302 663 - v1.2.0 - intelligent transport systems (its); access layer specification for intelligent transport systems operating in the 5 ghz frequency band,” 2012.

[20] ——, “Ts 102 724 - v1.1.1 - intelligent transport systems (its); harmonized channel specifications for intelligent transport systems operating in the 5 ghz frequency band,” 2012.

[21] ——, “Ts 103 759 - v2.1.1 - intelligent transport systems (its); security; misbehaviour reporting service; release 2.”

[22] L. M. Lopez, C. F. Mendoza, J. Casademont, and D. Camps-Mur, “Understanding the impact of the pc5 resource grid design on the capacity and efficiency of lte-v2x in vehicular networks,” *Wireless Communications and Mobile Computing*, vol. 2020, 2020.

[23] C2C-CC, “Survey on its-g5 cam statistics,” 2018.

[24] V. G. Martínez, L. H. Encinas, and A. Q. Dios, “Security and practical considerations when implementing the elliptic curve integrated encryption scheme,” *Cryptologia*, vol. 39, pp. 244–269, 7 2015.

[25] H. Hashim, A. R. Alzighaibi, A. F. Elessawy, I. Gad, H. Abdul-Kader, and A. Elsaid, “Securing financial transactions with a robust algorithm: Preventing double-spending attacks,” *Computers*, vol. 12, 9 2023.

[26] “Speedtest global index – internet speed around the world – speedtest global index,” date accessed: 27/05/2024. [Online]. Available: https://www.speedtest.net/global-index

[27] ETSI, “Ts 103 831 - v2.1.1 - intelligent transport systems (its); vehicular communications; basic set of applications; decentralized environmental notification service; release 2,” 2022.

[28] ——, “Ts 102 965 - v2.1.1 - intelligent transport systems (its); application object identifier (its-aid); registration; release 2,” 2021.

A

Standard Data Structures and Authorization Request Message

A.1 Signed and Encrypted Data Structures

The present document assumes the definition of the data structures specified in ETSI TS 103 097 [17].

Especially the following TS103097 data structures shall be used for encrypted/signed messages specified in the present document:

- `EtsiTs103097Data-Signed`;
- `EtsiTs103097Data-Encrypted`;
- `EtsiTs103097Data-SignedAndEncrypted`;
- `EtsiTs103097Data-SignedExternalPayload`.

The `EtsiTs103097Data-SignedAndEncrypted` structure is composed of an `EtsiTs103097Data-Encrypted`

structure containing an encrypted EtsiTs103097Data-Signed structure.
The EtsiTs103097Data-SignedExternalPayload is used to sign digest (hashed) messages.

All signed data structures contain a headerinfo which itself includes a PSID/ITS-AID. This PSID/ITS-AID is mandatory and shall be used for the certificate management CRL and CTL services with value as assigned in ETSI TS 102 965 [28].

A.2 Authorization Request Message

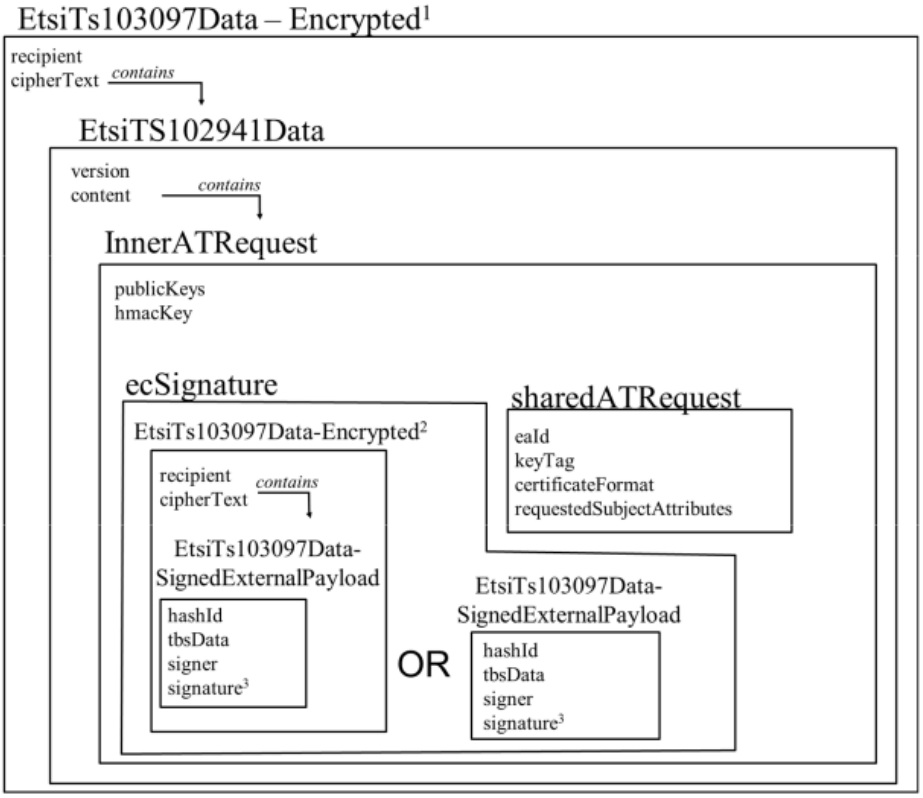
To create an authorization request, the ITS-S shall follow this process:

- An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the AT.
- Optionally, an ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the AT.
- A random 32 octets long secret key (hmac-key) is generated.
- A tag using the HMAC-SHA256 function is computed using the previously generated hmac-key, on the concatenation of the serialization of verificationKey and encryptionKey elements (encryptionKey is optional); this tag is truncated to the leftmost 128 bits and named keyTag. By including the tag in the SharedATRequest structure the integrity as well as the non-repudiation of the verificationKey and encryptionKey elements is ensured. The use of an HMAC function ensures that the tag can only be verified by the instances that are in possession of the hmac-key. By this means the AA can verify that the HMAC value of the public keys match the given keyTag and the EA is not able to draw conclusions on the keys requested by the ITS-S.
- A SharedATRequest structure is built, with:
  - the eaId identifying the EA certificate of the EA that can be contacted for validation;
  - the calculated keyTag;
  - the certificateFormat which specifies the version used for the certificate format specification;
  - the desired attributes(requestedSubjectAttributes).
- An EtsiTs103097Data-SignedExternalPayload structure is built containing: hashId, tbsData, signer and signature:
  - the hashId shall indicate the hash algorithm to be used;

- in the tbsData:
  - the payload shall contain an extDataHash with the hash of SharedATRequest;
  - in the headerinfo:
    - the psid shall be set to ”secured certificate request”;
    - the generationTime shall be present;
  - the signer declared as a digest referencing the hashID8 (SHA-256 without the eight least significant bytes) of the EC certificate;
  - the signature over tbsData computed using the private key corresponding to the EC's verification public key.
- [ITS-S_WithPrivacy] An EtsiTs103097Data-Encrypted structure (encryptedEcSignature) is built with:
  - the component recipients with one instance of RecipientInfo of choice certRecipInfo, containing:
    - the HashedId8 of the EA certificate in recipientId; and
    - the encrypted data encryption key in encKey; the public key to use for encryption is the encryptionKey found in the EA certificate referenced in recipientId;
  - the component ciphertext containing the encrypted representation of the EtsiTs103097Data-SignedExternalPayload structure;
  - [ITS-S_NoPrivacy] For special purpose ITS-Ss which do not require privacy and are allowed to be re-identified by the AA, the message structure shall omit the encryption of the signer information and signature by omitting the previous step.
- An InnerATRequest structure is built, containing:
  - the publicKeys: a verificationKey requested for certification and an optional encryptionKey to be placed in the same certificate;
  - the generated hmac-key;
  - the SharedATRequest structure;
  - [ITS-S_WithPrivacy] the encrypted detached signature containing the EtsiTs103097Data-Encrypted structure (encryptedEcSignature);
  - [ITS-S_NoPrivacy] the not encrypted detached signature containing the EtsiTs103097Data-SignedExternalPayload.
- An EtsiTs102941Data structure is built, with:
  - the version set to v1 (integer value set to 1);
  - the content set to the previous InnerATRequest structure.

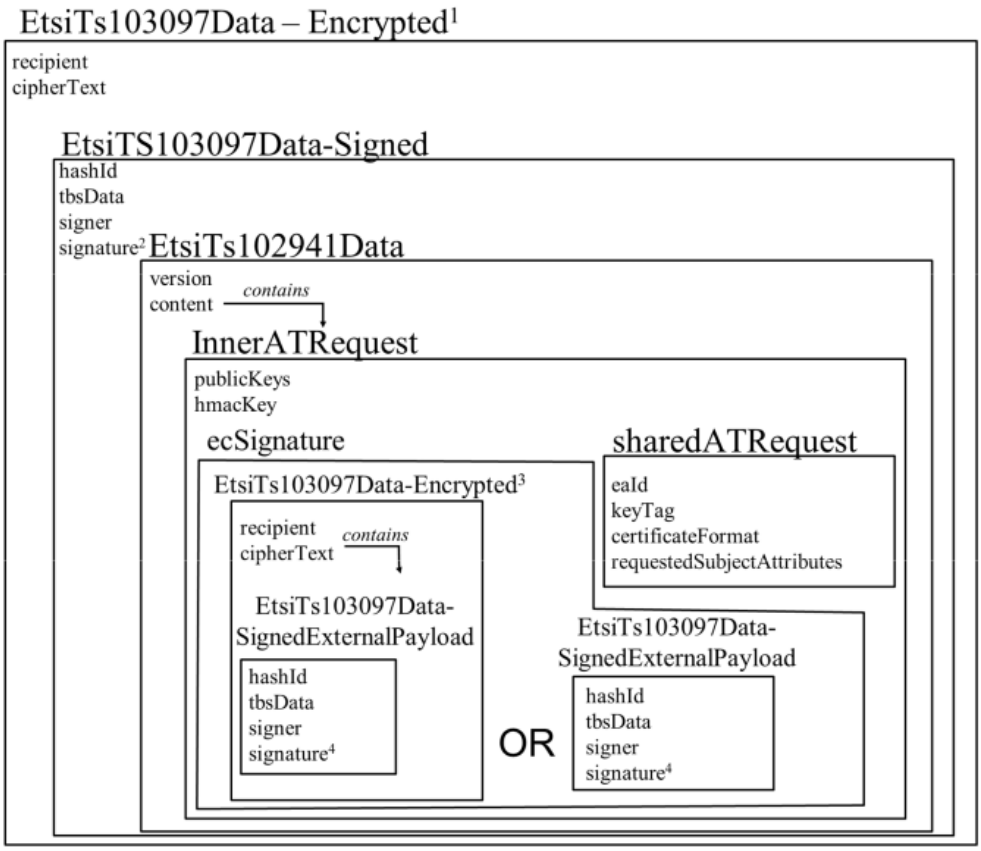
The Prove of Possession (POP) signature is optional. That is why there are two types of messages for the authorization request: AuthorizationRequestMessage and AuthorizationRequestMessageWithPop. The use of this signature is recommended since it is an important security mechanism to ensure the trustworthiness of the ITS-S. It ensures that the requesting ITS-S is in possession of the corresponding private key. If present, this `EtsiTs103097Data-Signed` contains a signature providing a proof of possession of the ITS-S verification key that is provided to the AA for certification. This component is an `EtsiTs103097Data-Signed` structure containing (see Figure A.2) the `hashId`, the `tbsData`, the `signer` and `signature`:

- The `hashId` shall indicate the hash algorithm to be used;
- In the `tbsData`:
  - the `payload` shall contain the previous `EtsiTs102941Data` structure;
  - in the `headerinfo`:
    - the `psid` shall be set to ”secured certificate request”;
    - the `generationTime` shall be present;
  - The `signer` declared as `self`.
  - The `signature` over `tbsData` computed using the private key corresponding to the verification public key `verificationKey` to be certified and provided in the ATRequest.
  - An `EtsiTs103097Data-Encrypted` structure is built, with:
    - the component recipients containing one instance of `RecipientInfo` of choice `certRecipInfo`, containing:
      - the hashedId8 of the AA certificate in `recipientId`; and
      - the encrypted data encryption key in `encKey`, the public key to use for encryption is the `encryptionKey` found in the AA certificate referenced in `recipientId`;
    - the component `ciphertext` containing the encrypted representation of the previous `EtsiTs103097Data-Signed` structure if the POP signature is present otherwise the `EtsiTs103097Data` unsecured envelope containing the `EtsiTs102941Data` structure.



NOTE: [1] Encryption is done with ECIES using the public encryption key of the AA.
[2] Encryption is done with ECIES using the public encryption key of the EA.
[3] Signature computed using currently valid private key corresponding to the EC's verification public key.

Figure A.1: AuthorizationRequest message [16]



NOTE: [1] Encryption is done with ECIES using the public encryption key of the AA.
[2] Signature computed using the private key corresponding to the verification public key to be certified.
[3] Encryption is done with ECIES using the public encryption key of the EA.
[4] Signature computed using currently valid EC private key corresponding to the verification public key.

Figure A.2: AuthorizationRequestMessageWithPop [16]