C-ITS Platform

WG5: Security & Certification

Final Report

ANNEX 1: Trust models for Cooperative - Intelligent Transport System (C-ITS)

An analysis of the possible options for the design of the C-ITS trust model based on Public Key Infrastructure in Europe

v1.1

Contents

Executive Summary

In the overall context of the EU C-ITS platform the topic security & certification has been concentrated in working group five and this technical report elaborates the basis for the in depth discussion of the security topic for C-ITS Introduction in Europe with the members of the working group and hereby defines the available options of a future solution in European and worldwide C-ITS markets.

The objective of this technical report is to identify and analyse the main Trust Models for Cooperative-C-ITS based on a Public Key Infrastructure (PKI). While other cryptographic techniques could also be used (e.g., symmetric cryptography), this report focuses specifically on PKI. The report identifies the potential PKI-based trust models from literature and other case studies and assess them on the basis of the specific features of C-ITS and metrics of evaluation based on high level requirements.

The report describes similar case studies, which could provide input to the analysis for the C-ITS trust model both from existing running systems and from standardization activities. Case studies outside ITS are also considered.

The report identifies the main trust models based on PKI and the main requirements areas, which are used to evaluate the trust models. An analysis for each requirement area is provided. The set of analysis is used to provide final recommendations for the most appropriate trust model in C-ITS for Europe.

1 Scope

The objective of this technical report is to identify and analyse the main Trust Models for Cooperative-C-ITS based on a Public Key Infrastructure (PKI). While other cryptographic techniques could also be used (e.g., symmetric cryptography), this report focuses specifically on PKI. The report identifies the potential PKI-based trust models from literature and other case studies and assess them on the basis of the specific features of C-ITS and metrics of evaluation based on high level requirements. The report also presents similar case studies based on PKI from existing deployed systems (PKI for the European Digital Tachograph application, Australian Gatekeeper) and from current standardization activities (Car to Car and Connected Vehicles in USA).

The main objective of this report is not to identify new security requirements for C-ITS or to conduct a new risk analysis in addition to the work already done in European research projects and the standardization activity in Car to Car. For these aspects, this technical report will use the work already published.

This technical report will present a qualitative analysis of the expert members in the security working group of the trust models rather than quantitative work. While, some hard evidence could be used to support an analysis for specific aspects (e.g., performance for the validation of the certificates or price range of crypto-processors), the analysis will be mainly based on the expertise of the participants and contributors of the Working Group 5 of the C-ITS Platform.

2 Introduction

Cooperative Intelligent Transport Systems and Services (C-ITS) enables communication between vehicles and traffic infrastructure C-ITS stations on the basis of the exchange of information in terms of standardised message sets. C-ITS can support a wide range of new applications to improve road safety by avoiding accidents and reducing injury severity, increased efficiency by supporting a consistent traffic flow, foresight driving and enhance driving comfort.

The success of the C-ITS network as a whole will also depend on the provision of appropriate levels of trust and the related security properties: availability, confidentiality, authentication, integrity, authorization and non-repudiation.

The implementation of appropriate levels of security is essential to provide a level of trust among the main elements of the C-ITS architecture: vehicles, road side infrastructures, drivers personal ITS stations, road authorities, service providers and so on.

In comparison to other domains (e.g., electronic commerce, government services), C-ITS has specific features, which must be taken in consideration. For example, the cooperative aspect implies that mutual trust among the elements of the architecture must be supported, the importance of safety applications means that security requirements are high to protect the lives of the citizen, the high speed of the vehicles implies that real-time exchange of secure information is needed, the huge size of the automotive market spanning many nations entails complex organization and technical dependencies. These and other features are described in detail in the rest of this technical report.

Historically, cryptography is the approach that has been used to secure communications and devices. Two main cryptography approaches are commonly used:

- Symmetric cryptographic system, where a secret key is used to encrypt the message is the same one used to decrypt a message.
- Asymmetric cryptographic system, keys come in pairs—each message sent contains one half of this key pair, and the receiving node has the other key.

In this technical report, we will focus on the Asymmetric cryptographic system and the Public Key Infrastructure concept, which is needed to support the deployment of Asymmetric cryptographic in C-ITS. A Public Key Infrastructure (PKI) is the key management environment for public key information of a public key cryptographic system. In addition, this report will discuss the cryptographic or security solutions, which are complementary to the PKI as described in the Car to Car technical deliverables.

Note that the overall system supporting a trust model in a specific jurisdiction (e.g., European member state) can be wider than the PKI implementation and deployment and it may include organizational and process aspects. For this reason, the term C-ITS Credential Management System (CCMS) can also be used to include both, the PKI system and the related policy, organizational structures and processes. From this point of view, an EU-wide C-ITS trust model or EU CCMS can be defined in the following way (from [52]):

"Any communications system needs to provide a mechanism to allow communicating partners to trust each other. In large systems, this is typically accomplished by cryptographic protection for individual communications, along with cryptographically secured credentials and a centralized credential management system with responsibility for ensuring that credentials are issued only to parties that are entitled to them. Each credential management system typically has a small number of nodes that serve as trust anchors, which can make statements themselves about the trustworthiness of end-entity nodes or delegate the ability to make trust statements to other management nodes"

The structure of the report is as follows: the section Public Key Infrastructures and C-ITS describe the main concepts of PKI and the context of C-ITS for the specific aspect of the trust model based on Public Key Cryptography. Then, the main examples of PKIs already deployed and in standardization activities are described in section Current PKI infrastructures in road transportation. The section includes a description of the Car to Car security design. The purpose to provide this background information is to identify potential gaps for the PKI design. The Section Trust Models for C-ITS identifies the potential Trust Models for C-ITS based on PKI, which are evaluated in section 9 where the metrics for the evaluation are identified and described. Finally, the section Conclusions provides the conclusions of the technical report.

3 References

[1].	Hunt, R. (2001). Technological infrastructure for PKI and digital certification. *Computer communications*, *24*(14), 1460-1471.
[2].	López Millán, G., Gil Pérez, M., Martínez Pérez, G., & Gómez Skarmeta, A. F. (2010). PKI-based trust management in inter-domain scenarios. Computers & Security, 29(2), 278-290.
[3].	Skarmeta, A. F. G., Pérez, G. M., Reverte, S. C., & Millán, G. L. (2003). PKI services for IPv6. Internet Computing, IEEE, 7(3), 36-42.
[4].	BerkovC-ITS, S., Chokhani, S., Furlong, J. A., Geiter, J. A., & Guild, J. C. (1994). Public key infrastructure study. NATIONAL INST OF STANDARDS AND TECHNOLOGY

	GAITHERSBURG MD.
[5].	Hesse, P., & Lemire, D. (2002, February). Managing Interoperability in Non-Hierarchical Public Key Infrastructures. In NDSS.
[6].	Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. IEEE Internet Things J, 1(1), 10-21.
[7].	Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. Computer Communications, 44, 1-13.
[8].	NHTSA, (2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.
[9].	Information technology — Security techniques — Evaluation criteria for IT security ISO/IEC 15408-1
[10].	X.509 standard
[11].	Adams, C., & Lloyd, S. (2003). Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional.
[12].	Gatekeeper PKI Framework, Gatekeeper Public Key Infrastructure Framework, February 2009.
[13].	Gatekeeper PKI Framework, Security Profile, February 2009.
[14].	Gatekeeper PKI framework Core Obligations policy, February 2009.
[15].	Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU PP), Compliant to EU Commission Regulation 1360/2002, Annex I(B), App. 10., BSI-CC-PP-0057
[16].	Common Criteria Protection Profile, Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, BSI-CC-PP-0070.
[17].	Digital Tachograph System European Root Policy Version 2.1, JRC 53429
[18].	ERCA Certification Practices Statement v1.0 - S.P. I.04.178.
[19].	Digital Tachograph home page: http://dtc.jrc.ec.europa.eu/
[20].	R. Kroh, A. Kung, and F. Kargl. SeVeCom Deliverable 1.1, version 2.0: Vanets security requirements final version. Technical report, 6th Framework Programme, 2006
[21].	A. Kung. SeVeCom Deliverable 2.1, version 2.0: Security architecture and mechanisms for V2V/V2I. Technical report, 6th Framework Programme, 2007.
[22].	PREparing SEcuRe VEhicle-to-X Communication Systems, Deliverable 1.3, V2X Security Architecture v2, Janury, 2014.

[23].	PREparing SEcuRe VEhicle-to-X Communication Systems Deliverable 1.1 Security Requirements of Vehicle Security Architecture, June 2011.
[24].	ETSI TS 102 940 Intelligent Transport Systems (C-ITS); Security; C-ITS communications architecture and security management, v1.1.1, June 2012.
[25].	ETSI TS 102 941 v1. 1.1-intelligent transport systems (C-ITS); security; trust and privacy management," Standard, TC C-ITS, 2012.
[26].	ETSI, TR 102 893:" Intelligent Transport System (C-ITS), Security, Threat, Vulnerability and Risk Analysis (TVRA).
[27].	ETSI TS 103 097 Intelligent Transport Systems (C-ITS); Security; Security header and certificate formats, v1.1.1, April 2013.
[28].	ETSI TS 102 731 v1. 1.1-intelligent transport systems (C-ITS); security; security services and architecture. Standard, TC C-ITS. 2010.
[29].	Federal Register Vol. 79 Friday, No. 60 March 28, 2014, Electronic Logging Devices and Hours of Service Supporting Documents; Proposed Rule
[30].	Raya, Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. "Securing vehicular communications." IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications 13.LCA-ARTICLE-2006-015 (2006): 8-15.
[31].	U.S. Department of Transportation, Privacy Impact Assessment, Federal Motor Carrier Safety Administration (FMCSA), Electronic Logging Devices, Supplemental Notice of Proposed Rulemaking
[32].	Security Credentials Management System (SCMS) Design for the Connected Vehicle System, Primer for Harmonization Task Group #6, January 15, 2014
[33].	S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETs): status, results, and challengeg Telecommun. Syst., 50 (4) (2012), pp. 217–241.
[34].	A. Dhamgaye, N. Chavhan Survey on security challenges in VANET, Int. J. Comput. Sci., 2 (2013), pp. 88–96 ISSN 2277-5420.
[35].	Perlman, R., "An overview of PKI trust models," Network, IEEE , vol.13, no.6, pp.38,43, Nov/Dec 1999
[36].	Rao, A.; Sangwan, A.; Kherani, A.A.; Varghese, A.; Bellur, Bhargav; Shorey, R. "Secure V2V Communication With Certificate Revocations", 2007 Mobile Networking for Vehicular Environments, On page(s): 127 - 132
[37].	Mingchu Li; Yizhi Ren; Zhihui Wang; Jun Xie; Hongyan Yao "A New Modified Bridge Certification Authority PKI Trust Model", Pervasive Computing and Applications, 2006 1st International Symposium on, On page(s): 23 - 26

[38].	Koga, S.; Sakurai, K. "A merging method of certification authorities without using cross-certifications", Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on, On page(s): 174 - 177 Vol.2 Volume: 2, 29-31 March 2004.
[39].	Lloyd, S., Fillingham, D., Lampard, R., Orlowski, S., & Weigelt, J. (2001, March). CA-CA Interoperability. In PKI Forum TWG.
[40].	Alterman, P. (2001). The US federal PKI and the federal bridge certification authority. Computer Networks, 37(6), 685-690.
[41].	Polk, William T., and Nelson E. Hastings. "Bridge certification authorities: Connecting b2b public key infrastructures." PKI Forum Meeting Proceedings. 2000.
[42].	William E. Burr and William T. Polk, A Federal PKI with Multiple Digital Signature Algorithms, PKS98 Conference, April 1999
[43].	Linn, J. (2000). Trust models and management in public-key infrastructures. RSA laboratories, 12.
[44].	TeleTrusT European Bridge CA. https://www.ebca.de/fileadmin/docs/publikationen/2015-TeleTrusT-Info_EBCA_EN.pdf
[45].	Bridge/Gateway Certification Authority (BGCA). http://ec.europa.eu/idabc/en/document/2318/5927.html
[46].	EUROPEAN COMMISSION – Enterprise DG. A bridge CA for Europe's Public Administrations Feasibility study. PKICUG PROJECT. Final Report 2002. Publicly available at http://ec.europa.eu/idabc/servlets/Doc257e.pdf?id=17267.
[47].	Sean Lancaster, David C. Yen, Shi-Ming Huang, Public key infrastructure: a micro and macro analysis, Computer Standards & Interfaces, Volume 25, Issue 5, September 2003, Pages 437-446, ISSN 0920-5489.
[48].	Bundesamt fur Sicherheit in der Informationstechnik (BSI), Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued by EU Member States, Ver. 2.1, Technical Guideline TR-03139, Bonn, Germany, 2013
[49].	Antonia Rana, Luigi Sportiello, Implementation of security and privacy in ePassports and the extended access control infrastructure, International Journal of Critical Infrastructure Protection, Volume 7, Issue 4, December 2014.
[50].	ETSI: Provision of harmonized Trust Service Provider (TSP) status information, Technical Specification TS 102 231,
[51].	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework IETF RFC 3647. https://tools.ietf.org/html/rfc3647. Last accessed 10/07/2015.
[52].	HTG6 Co-Operative Credential Management System Functional Analysis

4 Glossary

Abbreviation	Synonym	Description
API	Application Programming Interface	Programming interface available to developers to create applications
Accountability		Responsibility of an entity for C-ITS actions and decisions (ISO 27000)
Authenticity	Security property	Property that an entity is what it claims to be (ISO 27000.
AA	Authorization Authority	Authority that provides an C-ITS-S with permission to invoke C-ITS applications and services (ETSI TS 102 941, [25])
EA	Enrolment Authority	Authority that validates that an C-ITS-S can be trusted to function correctly (ETSI TS 102 941, [25])
Authorities and prospective roles: CMA/Enrolment CA, CIA, Auditors, Root CA, etc.)	Roles in the security infrastructure	Credentials Management Authority CMA, Certificates Issuing Authority CIA, Root keys Certification Authority, Auditors are examples of the entities and actors physically constituting the organization of the system trust chain.
CA	Certificate Authority	The CA is a trusted party, which authenticates entities taking part in an electronic transaction. To authenticate an entity, the CA issues a digital certificate. This certificate is a digital document which establishes the credentials of the entities participating in a transaction.
CAM	Cooperative Awareness Message	The Cooperative Awareness Messages (CAMs) are distributed within the C-ITS-G5 (802.11p) network and provide information of presence, positions as well as basic status of communicating C-ITS stations to neighbouring C-ITS stations that are located within a single hop distance.
CAMP	Crash Avoidance Metrics Partnership	A public–private research consortium working with NHTSA to develop technology that will help cars, trucks, buses and other vehicles avoid crashes by communicating with nearby vehicles and roadway infrastructure, including traffic signals, dangerous road segments and grade crossings.
Certificates	Security material	A set of data that uniquely identifies an entity, contains the

		entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity.
Certification	Process	The process of ensuring that a system component or interface meets an established standard or technical specification. According jurisdiction and policies, this can be performed by authorized certification bodies (accredited labs) or industry can self certifies a product line.
COI	Community of Interest	Specific group of entities with similar properties or roles
Confidentiality	Security property	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 27000)
Connected		Connected means that data/information will be sent to and from vehicles/drivers (or broader road users) by all communication means but mainly by cellular 3/4G/LTE (for information and advice) and for specific critical services by short range Wifi-p (warnings). The information received in the vehicle will be used by the drivers themselves.
Cooperative		Cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) by all communication means but mainly by short/range Wifi-p (control and warnings) and less by cellular 3/4G/LTE (for less critical services). In the "cooperative" situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (eg CACC).
Cooperative C-ITS (C-ITS)		C-ITS systems that can bring intelligence for vehicles, roadside systems, operators and individuals, by creating a universally understood communications "language" allowing vehicles and infrastructure to share information and cooperate in an unlimited range of new applications and services.
Cooperative Services		Cooperative services concerns the (fast) exchange of data/information with DSRC/wifi-p form V2X to support or automatically take-over the tasks of driver.
CP	Component Personaliser	Personaliser of electronic components used in the Digital Tachographs like a tachograph card, vehicle unit or motion

		sensor.
CRL	Certificate Revocation List	List of identifiers of the certificates that have been revoked.
CSP	Certification service provider	Provider of certification service.
DCM	Device Configuration Manager	
DENM	Decentralized environmental Notification Message	C-ITS facility layer message providing Road Hazard Warning related information.
Device	Piece of hardware part of an C-ITS system.	
DoS	Denial of Service	Attack where the provision of a service by a service provider is denied.
EAL-X	Evaluation Assurance Level	The Evaluation Assurance Level (EAL1 through EAL7) of an Information Technology product or system (for example a telematics device used in road vehicle) is a numerical grade (i.e., X) assigned on the basis of the completion of a specific Common Criteria security evaluation.
ECC	Elliptic Curve Cryptography	
Enforcement		Operational verification and measures to ensure that a regulation-law in force is effectively and correctly applied in the field of operations (this is typical role of police forces and road authorities).
EOI	Evidence of Identity	
Equipment	Set or subset of devices	
ERCA	European Root Certification Authority	It is the root CA for the Digital Tachograph application in Europe.
ETSI	European Telecommunications Standards Institute	It is an European standardization body.

Flexibility/Scalability/Maintainability		Capacity of a system to adapt to changes (technological or political), to evolve, and to maintain C-ITS characteristics, and to recover from accidents
FMCSA	Federal Motor Carrier Safety Administration	
FOT	Field Operational Test	Test executed in the field.
Function		The action(s) a device is designed to perform
G5A	C-ITS road safety communication (802.11p)	Frequency band between 5.875 GHz and 5.905 GHz - reserved in Europe for C-ITS road safety communication
G5B	C-ITS non-safety communication (802.11p)	Frequency band between 5.855 GHz and 5.875 GHz - reserved for C-ITS road non-safety communication
G5C	C-WLAN	5GHz WLAN communication (802.11a)
Harmonization		Efforts and measures to adopt harmonized and compatible 'systems' between jurisdictions. It encompasses hardware aspects (devices) but also organizational (PKI, policies, privacy regimes) and requires flexibility to adapt and adjust.
I2I		Infrastructure-to- Infrastructure Communication between multiple infrastructure components like roadside C-ITS stations
I2V and I2C		I2C Infrastructure-to-Vehicle Communication between infrastructure components like roadside C-ITS stations and vehicles.
ICS		C-ITS Central Station
Information Security		Preservation of confidentiality, integrity and availability of information NOTE In addition, other properties, such as authenticity (2.6), accountability, non-repudiation, and reliability can also be involved. (ISO 27000)
Infrastructure		A collection of equipment interconnected to the cooperative system interacting with a transportation system and/or other institution (authorities and public supervision systems, private

		services entities, etc.)
Integrity		Property of protecting the accuracy and completeness of assets (ISO 27000)
Interoperability		The ability of a system to communicate with other systems to provide the same service in different physical locations. It is also the ability of one system (or component) to replace another without degrading or affecting the service being provided.
IRS	C-ITS Roadside Station	
ISM	Australian Government Information and Communications Technology Security Manual	Compliance with the PSM and ISM is required as a minimum standard for Gatekeeper Accreditation
C-ITS	Intelligent Transport Systems	Intelligent Transport Systems (C-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).
C-ITS Application		A functional definition of a service provided to an end user, which fulfils specific needs of a user (for example, forward collision warning)
C-ITS Station		A collection of (functional) equipment that participate in the provision of C-ITS services at a particular location. An C-ITS Station may exist in a vehicle, at the roadside, in a central location such as a Traffic Management Centre, or in a mobile device. It has two meanings: an actual physical device and/or a functional set of services.
IVS	C-ITS Vehicle Station	
Jurisdiction		Entity where rules, laws, regulation, policies are managed by the same authority.
KDR	Key Distribution Request (for motion sensor master keys)	It is the distribution request for the motion sensor master key.
Km		Motion sensor master key in the Digital Tachograph

KmVU		Motion sensor master key inserted in vehicle unit
LOP	Location Obstruction Proxies	Proxy to obscure the location information to support privacy.
LTC	Enrolment Credential	Long-Term Certificate
LTCA	Enrolment Authority (EA)	Long-Term Certificate Authority
LTCA	Long Term Certification Authority	Certification authority for the long term Certificates.
Misbehavior detection		Automatic detection of misbehaving device or equipment, possibly resulting in automatic revocation.
MS	Motion Sensor	This is the motion sensor in the truck used to record the driving time of the drivers.
MSA	Member State Authority	
MSCA	Member State Certification Authority	It is the Certification Authority at European Member State level. It is equivalent to NCA.
NA	National authority	Representative of an European member state.
NCA	National Certification Authority.	It is the Certification Authority at National level in Europe. It is equivalent to MSCA.
Non-repudiation	Security property	Ability to prove the occurrence of a claimed event or action and C-ITS originating entities (ISO 27000).
OBD		On Board Diagnose
OEM		Original Equipment Manufacturer
OCSP	Online Certificate Status Protocol	
Origin	Defined source of data or messages	
OTAR	Over the air interface	Over the Air Interface which can be used to distribute certificates to the ITS stations.
PC	Pseudonym Certificate	
PCA	Pseudonym Certification	Certification authority for the pseudonym Certificates.

	Authority	
PKCS	Public Key Cryptography Standards	A set of cryptographic standards, published by RSA Security LLC.
PKI	Public Key Infrastructure	A public key infrastructure (PKI) is the combination of software, cryptographic technologies, processes, and services that enable an organization to secure C-ITS communications and business transactions.
Policies		Rules, practices, regulations, laws, official texts governing specific activities, organizations, agreements.
Privacy/Data protection		Set of rules and policies in a jurisdiction, aiming at protecting sensitive personal data belonging to individuals.
Pseudorandom certificates		Techniques to randomly and periodically change security certificates to mitigate the risks of a device (and C-ITS owner) of being tracked or linked.
PSM	Commonwealth Protection Security Manual	Compliance with the PSM and ISM is required as a minimum standard for Gatekeeper Accreditation
PS-OBU	Public Safety On Board Unit	
RA	Registration Authority	A RA is responsible for the interaction between clients of a C-ITS and CAs.
RAES	Registration Authority Extended Services	
RCA	Root Certification Authority	
Resilience	Security Property	Capacity of a system to resist to perturbations, and to recover from accidents with an acceptable rate.
Revocation		Action to render security credentials no more valid and therefore no more trustworthy.
RSA	Rivest, Shamir, Adleman	RSA is an asymmetric cryptographic scheme, named after their inventors Rivest, Shamir and Adleman and widely used in many IT scetors.

R-C-ITS-S	Roadside C-ITS Station	Roadside C-ITS Station, or R-C-ITS-S
SCMS	Security Credentials Management System	Security system design for cooperative vehicle-to-vehicle and vehicle to infrastructure applications
Security material		Collection of cryptographic material (keys, certificates, algorithms, credentials, identifiers) that need to be created, embedded, activated, deactivated and eventually discarded at the end of life of a device.
Security material lifecycle		The description of processes and procedures accompanying the management of security material during operations and after.
SHA	Secure Hash Algorithm	
SK	RSA secret key	
Sustainability		Capacity to remain operational and viable on a long term
TCA	Transport Certification Australia	TCA (Transport Certification Australia) is a federal governmental organisation in Melbourne Australia managing the Australian National Telematics Framework with the C-ITS like IAP (Intelligent Access Program) for Goods Transport as its first service.
TF		Task Force
Tracing		Action to track and trace a connected device, recording e.g. PVT parameters (position, velocity, time).
TRO	Threat/Risk Organization	
TTP		Trusted Third Party
Type approval	Process	Final result of a multi-steps certification process (e.g. functional, interoperability certifications) resulting in the deliverance of a type approval certificate for a product. In some cases such a certificate is mandatory for any new product to enter the market.
Unlinkability		Ability of a user to make multiple uses of resources or services without others being able to link these uses together (ETSI TS 102 941).

V-C-ITS-S	Vehicle C-ITS Station	Vehicle C-ITS Station, or V-C-ITS-S
V2I	Vehicle to Infrastructure	Vehicle to Infrastructure communications
V2V	Vehicle to Vehicle	Vehicle to Vehicle communications
V2X	Vehicle to X	Combination of Vehicle to Vehicle communications and Vehicle to Infrastructure communications.
VU	Vehicle Unit	It is the main computing and recording platform in the vehicle for the European Digital Tachograph application

5 Public Key Infrastructures and C-ITS

5.1 Public Key Infrastructures and Services

In this section, we describe the generic main PKI components and services.

A Public Key Infrastructure (PKI) is the key management environment for public key information of a public key cryptographic system. Detailed information on PKI concepts can be found in [11] and [4] and some of the content described in this section is derived from these references.

We identify the following main components in a PKI system:

- A certificate authority (CA) that both issues and verifies the digital certificates. This is main chief of trust. CA can have a hierarchical structure.
- A registration authority which accepts and verifies the identity of users requesting information from the CA. Once the user's identity has been authenticated the request is then forwarded to the CA. The CA will in many cases trust requests received via the RA without further validation.
- A central directory or certificate repository, which is a secure location in which to store and index keys/certificates.
- Certificate Distribution System, to distribute the certificates.
- Policies. There are policies defined for the management of the PKI system or the generation and distribution of certificates. These can be subcategorized into Certificate Policies, which put requirements on the end-entities that must be met in order to obtain certificates, and Certification Practice Statements, which are statements by a CA operator about the practices they will follow to ensure correct outcomes. More details on the definition of policies are in 8.2.
- PKI enabled applications, which uses the PKI system.

The following list identifies the main services usually offered by a PKI system. Not all the PKI systems can offer these services. Some PKI systems only offer a subset of the services listed in the table**:**

Where the definition of PKI services and components is from based on [11]**:**

Certification Repository. Repository of keys and certificates.

Certificate Revocation. When a key is not used or acceptable any longer (e.g., security breach), there must be a way of alerting the users that it is no longer acceptable to use *this* public key for *that* identity. This alerting mechanism in a PKI is called *Certificate Revocation.* Two main mechanisms are usually employed for this purpose: Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP). The former enables the publication of lists with revoked certificates, while the latter provides a method to check online the current status of a given certificate.The first solution is easier to install and maintain, but has drawbacks in the reaction time for a breached certificate, the second one is faster in reacting but needs ITS stations to be “always online” to work effectively.

Key Backup. Backup of private keys.

Key Recovery. Recovery of private keys.

Key Update. This is the service to update the keys. This function is needed to replace obsolete keys, in case of a security breach or when the evolution of the system, requires new set of keys. This function can be automated or manual. The Key update is both for private and public keys even if the update process can be quite different.

Key History Management. The concept of key update, whether manual or automatic, implies that, over the course of time, a given user will have multiple "old" certificates and at least one "current" certificate. This collection of certificates and corresponding private keys is known as the user's key history. For decryption keys, keeping track of the entire key history is very important because data that an user has encrypted in the past cannot be decrypted with his current private decryption key. This service is used in the migration process. Basic rules for the key history management need to be included in the overall policy of a PKI infrastructure.

Cross-Certification. If we have a number of independently developed PKIs, it is inevitable that at least some of them will need to be interconnected over time. The concept of cross-certification has arisen in the PKI environment to deal with precisely this need for forming trust relationships between formerly unrelated PKI installations.

Support for Non-repudiation. Nonrepudiation is the case where the purported creator of a document making a statement will not be able to successfully challenge the validity of the document. A PKI cannot by itself provide true or full non-repudiation; typically, a human element is needed to apply discretion and judgment in weighing the evidence and to provide the final decision. However, the PKI must support this process by providing some of the technical evidence required, such as data origin authentication and a trusted attestation of the time the data was signed. Another way to think about non-repudiation is that it gives the receiver of a message the power to prove to a third party that the creator was involved in creating it.

Secure Time Stamping. That is, the time source must be trusted, and the time value must be securely conveyed. In addition, time stamping is needed to ensure that the expiration date of the certificates is accurate.

Notarization/Data Certification.
The PKI-enabled service of notarization is defined to be synonymous with data certification. That is, the notary certifies that data is valid or correct, in which the meaning of correct necessarily depends on the type of data being certified.

Validation Service.
A validation service enables to compute certification path construction and certification path validation. This service may implement the cross-certification functionality in scenarios where cross-certification is used.

This service can be either run locally or delegated to an external server via protocols like the Server-Based Certificate Validation Protocol (SCVP).

5.2 Generic deployment C-ITS architecture

This section describes the generic C-ITS deployment model for the generation and distribution of cryptographic material.

Note that this is only a high-level view, which is not directly linked to a proposed or deployed system, but it is only used for common information purposes of this report.

The overview of C-ITS security is described in Figure 1:

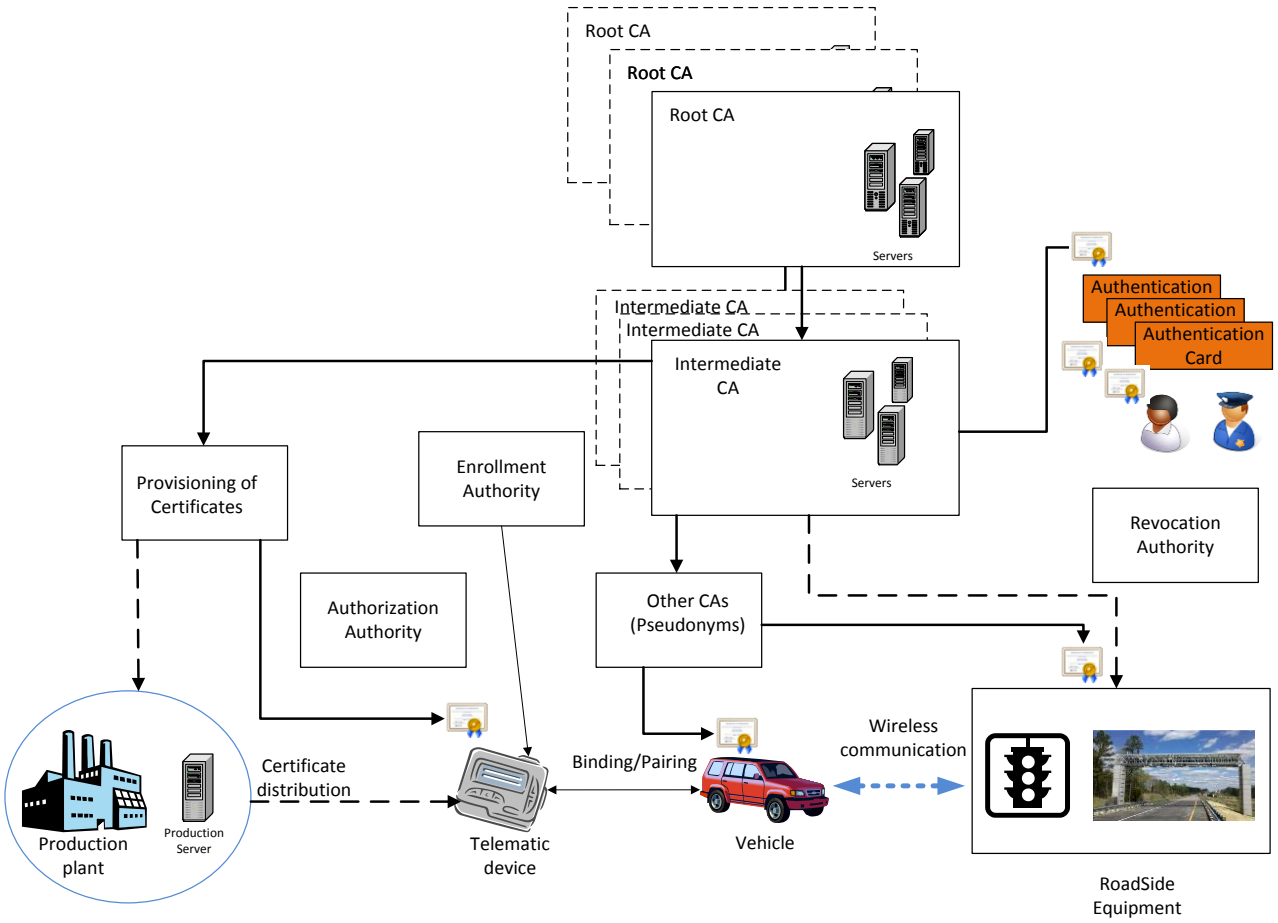

Figure 1: C-ITS elements for trusted communications based on PKI

The main components of this concept are:

1. One or more Root CAs (i.e., to support different jurisdictions or set of applications)
2. Intermediate CAs can be present when the organizations need an additional layer in order to work together efficiently. For example, this is the case in Europe for the Digital Tachograph application, where each European member state is related to a specific intermediate CA.

3. The Provisioning component has the function to distribute the certificates to the C-ITS device. The enrolment can be executed in a manufacturing plant or a workshop directly into the telematics device. Note that the telematics device may not be operational yet because the Enrollment/Registration of the devices has not been completed yet.
4. The Enrollment/Registration authority ensures that the telematics device is registered in the overall C-ITS system. Part of the registration phase could also be the binding/pairing of the C-ITS device with other components in the vehicle. For example, a telematics device can be paired with a specific sensor in the vehicle as in the case of the Digital Tachograph application.
5. The Authorization authority grants the permission to the telematics device to become fully operational and authorized to interact with the other components of C-ITS.
6. The Revocation authority is responsible for the revocation of the certificates associated to specific telematics devices with the consequence that operational devices may go back to previous states (e.g., enrolled)

Note that this is a simplified version of the architecture, which can be more complex and include other components like misbehaviour analysis modules and so on. An important aspects, which is not addressed in this figure is the distribution of new certificates in case of changes of the C-ITS PKI architecture (e.g., addition of a new CA or removal of a CA) or trust failures (e.g., compromise of a CA). This may include the presence of distribution channels beyond the one identified in the figure (i.e., the manufacturing plant). An important distribution channel is an Over The Air (OTAR) channel, which must be secure. In addition, entities like workshops could also be used as distribution channels guaranteed that some security conditions are met.

Other CAs could be present to support specific functions. For example, to create temporary pseudonym certificates to support privacy protection in car to car or car to infrastructure communication.

Not all these components may be present in the specific PKI architectures described below. For example, the Intermediate CA may not be necessary in some context or there may be only one Root CA.

Various types of stakeholders are present in this C-ITS scenario. In this technical report, we will adopt the list of types identified in [28] .

From a security point of view, different types of stakeholders may have different levels of access to C-ITS services and data. For example, law enforcer can have access to C-ITS services with a higher priority then normal stakeholders. The details on the level of access to specific C-ITS services and data is dependent on the regulatory frameworks defined in each domain. It is out of scope of this report to define all the potential access levels. On the other side, the capability of the trust model to support different levels of access will be addressed in this technical report. This may require a specific authentication process associated to different cryptographic materials. For example, the PKI may generate different types of certificates for the different levels of access. For example, in the Digital Tachograph application, there are four types of stakeholders: drivers, law enforcers, companies and workshops. Similar roles could also be defined in the C-ITS framework.

The entities described in this section participate to the different phases of the lifecycle of a telematics device, which are described in the following section.

5.3 Lifecycle

In this section, we describe the aspects related to the lifecycle of the main elements of the deployed system for Connected Vehicle/C-ITS applications and how they relate to the PKI concepts.

In this technical report, we deliberately focus on the operational phases for the deployment of ITS stations (which can be a telematic equipment in a vehicle or a roadside component) in the field, which are equipped with C-ITS devices and capabilities. The production/development phases of vehicles are not considered in this section, but they are addressed in the metrics definition in section 9 (for example under the CAPEX costs).

We can identify the following main phases and operations related to the ITS station lifecycle. In some cases, some operations apply in a different way for the telematics equipment in the vehicle or a roadside component and Table 1 provides a summary of the differences.

The main phases are:

1. Unprovisioned: The ITS station does not have any of the crypto material or certificates necessary to interact with other ITS stations or entities of C-ITS in a trustworthy fashion.
2. Provisioned and Unenrolled: The device has the crypto material and root certificates necessary to communicate with Enrolment entities. At this stage the ITS station is still not part of C-ITS and cannot in trustworthy fashion interact with other ITS stations.
3. Enrolled and Unauthorized: The device has all the material it needs to communicate with Authorization entities. It still cannot trustworthy interact with other ITS stations in trustworthy fashion.
4. Operational: The device has all the material it needs to communicate with ITS stations and C-ITS management entities.
5. End-of-Life: The device is unable to communicate with any entities in C-ITS.

The main operations are:

1. *Bootstrap*: This is the initial setup of the vehicle and/or telematics devices for the deployment in the field. For example, the telematics device (e.g., DSRC wireless communication device) should be configured and equipped with a long term certificate, which can be used for a considerable time (e.g., 2-3 years or more) to support other security functions (e.g., set-up of a Virtual Private Network) and/to download of sensitive content or other cryptographic material through the Over the air interface. In the bootstrap phase, security requirements are even higher than normal operations because the system may be compromised from day one for all the other security functions or operations. As a consequence, the distribution of the long term certificates should be implemented and executed in a secure environment. For example, through dedicated links protected at the physical level. The bootstrap phase includes all the different operations, which are needed to bring a C-ITS device or C-ITS station from the initial unprovisioned state to the final operational state. These operations are:
    a) Provision of certificates or simply provisioning. For example, a C-ITS device or C-ITS station not equipped with cryptographic material and just out of the manufacturing plan must be equipped with security certificates as initial step.

b) Enrolment/Registration of the C-ITS device with a registration authority. For example a roadside unit is registered with the central roadside authority according to the overall and agreed and implemented system policies and processes.

c) Authorization of the registered C-ITS device by a central authorization authority to be part of the C-ITS overall system and exchange data with other authorized C-ITS stations.

Some of these operations can be performed together or they may include other phases/operations. For example the Linking/Pairing (described in the next bullet) can be part of the Enrolment.

2. *Linking/Pairing*. This phase includes the secure linking of the main secure devices in the vehicle or the roadside infrastructure to ensure that the internal communications are operational and secure once the system is deployed in the field. For example, a secure sensor in a vehicle can be installed with specific keys/certificates in the bootstrap phase, but this phase is needed to ensure that the secure sensor and the other secure components in the vehicle are linked to support mutual trust (often for all the lifetime of the vehicle, or till a possible migration phase).
3. *Operation/Monitoring*. This phase is characterized by the regular and correct interactions of all C-ITS related nodes in the overall network which communicate which each other using the basic security principles and implemented technical elements of the respective stakeholders, in order to be fully interoperable in one C-ITS market region (E.g. Europe or USA). This phase includes regular monitoring of active C-ITS stations according to the developed domain policies.
4. *Migration.* This phase is related to the changes in the security components of the system including PKI and how it impacts the overall C-ITS/Connected Vehicle domain. For some secure elements, this phase may be unavoidable. For example, certificates usually have a shorter life (e.g., 3-5 years) than the lifetime of the cars or trucks. In addition, the implementation and deployment of new C-ITS applications can require changes to the PKI architecture/elements, which require a migration from the previous processes or cryptographic material to the new ones. Migration is usually related to a significant change in the PKI (Identify some examples of migration, like a new version of the security infrastructure and partners, or new algorithms to implement).
5. *Set to End of life.* Each element of the PKI or the C-ITS/Connected Vehicles systems has a specific lifetime and it is bound to be replaced or removed from the system at one point in time. In this phase, the PKI and systems administrators must ensure that cryptographic material or information are not disclosed, that important dependencies are not broken and so on.
6. *Periodic Maintenance/Calibration.* This phase is related to the periodic maintenance of the component of the systems, which may include calibration. In some cases, sensitive sensors must be checked or replaced at the workshops. In this phase, it is important that maintenance of sensitive components (e.g., containing cryptographic material) is executed with well-defined processes to avoid creating vulnerabilities in the system of the components of the PKI. For example, seals, which protect sensitive components could be damaged.
7. *Recall.* This phase is related to the forced recall of the car/trucks/roadside equipment because a hardware or software failure has been identified. As in the case of periodic maintenance, it is important that the handling of sensitive components is executed with well-defined processes to avoid creating vulnerabilities.

Each of these phases impacts the various PKI services and components of C-ITS systems in a different way. For example, workshops are obviously used in the Calibration/Recall and probably the Bootstrap phase as well.

Table 1 Lifecycle phases for ITS stations

Phase/Operation	C-ITS telematics equipment in vehicle	C-ITS telematics equipment in the infrastructure
Bootstrap (Provisioning)	Applicable	Applicable
Bootstrap (Enrolment)	Applicable	Applicable but combined with Bootstrap
Bootstrap (Authorization)	Applicable	Applicable but combined with Enrolment
Linking	Applicable	Not Applicable
Set to end of life	Applicable	Applicable
Maintenance/Calibration	Applicable	Applicable
Recall	Applicable	Applicable

6 Security context for C-ITS

6.1 Specific features of C-ITS and C-ITS applications for security

The C-ITS domain has specific features regarding security and privacy, which must be taken into consideration in the development of security solutions including cryptographic systems and PKI.

Various references have identified the specific features of C-ITS (e.g., car to car, connected vehicles) and future C-ITS applications in general.

In this section, we will review some of the contributions from literatures: government, academic and standardization.

Requirements for Car to Car are identified from the FP7 Preserve project [23] and ETSI technical specifications [24], [27], which identify the following key challenges:

- Scalability. The security solutions must be scalable to support tens of millions of cars and trucks in each geopolitical area (e.g., Europe, Asia).
- Heterogeneity of applications in the C-ITS domain. The security solution must be flexible to support various C-ITS applications both current and future.
- On-board end-point vulnerabilities. A malicious attacker may select to tamper with data (e.g., velocity, location, status of vehicle parts) at their source or the end-points of the wireless connection rather than breaking the encryption of the connection itself.

Requirements for the provision and validation of the main security properties (availability, confidentiality, authentication, integrity, authorization and non-repudiation) are heavily dependent on the type of application supported by C-ITS. For example, depending on the type of information transmitted among the C-ITS nodes (e.g., C-ITS stations), the level of requested confidentiality can be higher or lower.

For example, for the Co-operative Awareness Message, the following requirements are identified from [24]. It is also described how the requirements are addressed.

	Cooperative awareness (CAM)	**Static local hazard warnings**	**Dynamic local hazard warnings**	**Area hazard warnings**
Authentication and Authorization	• Basic CAM authorization, • Advanced CAM authorization • Authorization to claim priority rights for emergency vehicles • Authorization to state regulatory orders such as speed limits and road closures	In general the requirements for Authorization and Authentication are similar to CAM. In the subsequent unicast sessions, the local policies of the participating partners may require additional authorization and/or authentication.	In general the requirements for Authorization and Authentication are similar to CAM. In the subsequent unicast sessions, the local policies of the participating partners may require additional authorization and/or authentication.	Authorization could be granted at several levels depending on the capabilities of the vehicle.
Confidentiality	CAMs are broadcasts to any possible receiver but some CAM messages can be still considered personal data and local data protection laws apply. Pseudonyms are used to protect privacy.	Depends on application and the related information to be exchanged	Depends on application and the related information to be exchanged.	No confidentiality services are required
Privacy	CAMs are sent periodically many times a second and pseudonyms are used to protect privacy.	As the nature of the service is broadcast and the sender is a static RSU, no confidentiality or privacy requirements apply	Depends on application and the related information to be exchanged.	No confidentiality services are required

Beyond the requirements for specific applications, high level requirements can also be defined from the performance, organizational and processes point of view. The FP7 PRESERVE project addresses the challenges of secure and privacy-friendly communication between vehicles. Deliverable 1.1 specifically investigates and identifies the security requirements of vehicle security architecture [23]. The deliverable provides an extensive threats analysis in section 3.2 and identifies key requirements for vehicular communications in 3.3, which are summarized here:

- Time requirements for the signing and verification of messages.
- Low latencies.
- Simple processes for the distribution, installation, revocation of cryptographic material,
- Flexibility of the security architecture and proposed solutions to support the appearance of new applications in the lifetime of the car. It is reminded that a car lifetime can be usually from 5 to 15 years.
- Cost effectiveness. The price of the solutions cannot exceed the market constraints.
- Harmonization at global level. Proprietary security solutions should be avoided and global approaches should be supported to facilitate telematics and vehicle manufacturers.

Beyond Car to Car requirements, from section IX of reference [8] (research report from US NHTSA published in 2014), we can extract the following needs/requirements.

Note, that these requirements are provided only for informational purpose.

The suggested security infrastructure should:

- Not require the identity of the participating parties and, accordingly, supported the goal of appropriately preserving privacy;
- Be fast enough to fit within the bandwidth constraints of DSRC (5.9 GHz in Europe) and the processing constraints of the V2V on-board equipment;
- Fit within the constraints of DSRC bandwidth and size of the BSM in the message payload; and
- Support non-repudiation.

Then reference [8] provides a detailed study on the various security approaches (symmetric cryptography, public key, other security solutions).

From research literature, we can also identify similar set of requirements.

For example, reference [30] identifies the following specific challenges for vehicular networks:

- Delay-Sensitive Applications. Many applications and especially safety applications in C-ITS are delay sensitive: messages must be transmitted, received and authenticated in a very short timeframe.
- Scalability. The security solutions must be scalable to support tens of millions of cars and trucks in each geopolitical area (e.g., Europe, Asia).
- Heterogeneity of applications in the C-ITS domain. The security solution must be flexible to support various C-ITS applications both current and future.
- On-board end-point vulnerabilities. A malicious attacker may select to tamper with data at their source or the end-points of the wireless connection rather than breaking the encryption of the connection itself.

Additional papers, which identify similar security requirements are [32], [33] and [34].

In this technical report, we do not aim to identify the specific requirements for all the applications, which could be supported by C-ITS. As discussed above, these requirements have been already identified in many other references. Our objective is to identify the high level requirements at technical, organizational and economical level, which can be used to evaluate the different options for the Trust Models for PKI. From this point of view, the requirements are used as evaluation metrics and they are defined in detail in section 9.

7 Current PKI infrastructures in road transportation

7.1 European Root Certification Authority (ERCA) for the Digital Tachograph

This section describes the ERCA for the Digital Tachograph. While this regulated application is not fully part of C-ITS, the description of its trust model based on ERCA represents an useful case study for the deployment of a trust model in C-ITS. In particular, the new version of the Digital Tachograph based on 165/2014 regulation introduces the remote communication function, where the integrity security requirement must be validated. The number of trucks involved in the Digital Tachograph regulations is in the order of millions of units (around 5 millions in 2014 and likely to grow in the future).

The Digital Tachograph is a mandatory intelligent recorder of the professional drivers' activities (rest and driving hours). It provides trustworthy information to EU enforcers controlling compliance with Social Regulation (EC) No 561/2006.

The original tachograph (often referred to as the analogue or chrono tachograph) has been in existence for many years and its origins can be traced back to the era of the Jones Recorder of 1912. Whilst the instrument has increased in sophistication since first introduced, concern increased regarding the instrument's ease of use, its susceptibility to misuse and fraudulent operation, and its ability to offer an effective and secure system for the recording and monitoring of drivers' hours and vehicle activity.

In the early days (70's) there were mechanical tachographs, which progressed to the early electronic models, introduced around 1985. The advent of digital electronics, the growing power of computing and C-ITS ever-increasing cost effectiveness, resulted in increased pressure to update the chrono tachograph. Following a proposal from the European Commission and opinions expressed by the Economic and Social Committee a decision was taken to replace the current system with a digital version – a digital tachograph. The Digital Tachograph was clearly less vulnerable to illegal acts by users to distort the data. The new system also allowed for easier and better control of driver's hours by operators and the enforcement authorities.

From May 2006 all new vehicles over 3.5 tonnes except for those exempt have had to be supplied with a Digital Tachograph in Europe.

It has been generally acknowledged that fraudulent activities in road transport create the potential for reducing safety and disadvantaging those that do respect the rules in their day-to-day activities.

The purpose of the DT is, therefore, "to put an end to the most common abuses of the present system" by introducing new "advanced recording equipment fitted with an electronic device for storing relevant information and a personal driver card, so ensuring that the data recorded are retrievable, intelligible when printed out, and reliable, and that they provide an indisputable record of the work done by both the driver over the last few days and by the vehicle over a period of several months."

The recorder unit in the truck is called Vehicle Unit and it is connected to a Motion Sensor (MS), which is used to calculate the travelled distance in relation to time. Smartcards are used to access data of the Digital Tachograph.

From the security point of view, the Digital Tachograph system is based on a PKI, where the main root CA (also called ERCA) is the responsibility of the Joint Research Centre of the European Commission.

ERCA provides support for two cryptographic mechanisms:

1. Symmetric-key cryptography for pairing of the Vehicle Unit with the Motion Sensor.
2. Public-key cryptography for VU and Cards interaction and Data Download function.

The overall view of the European DT PKI is presented in Figure 2 and a more detailed view is presented in Figure 3.

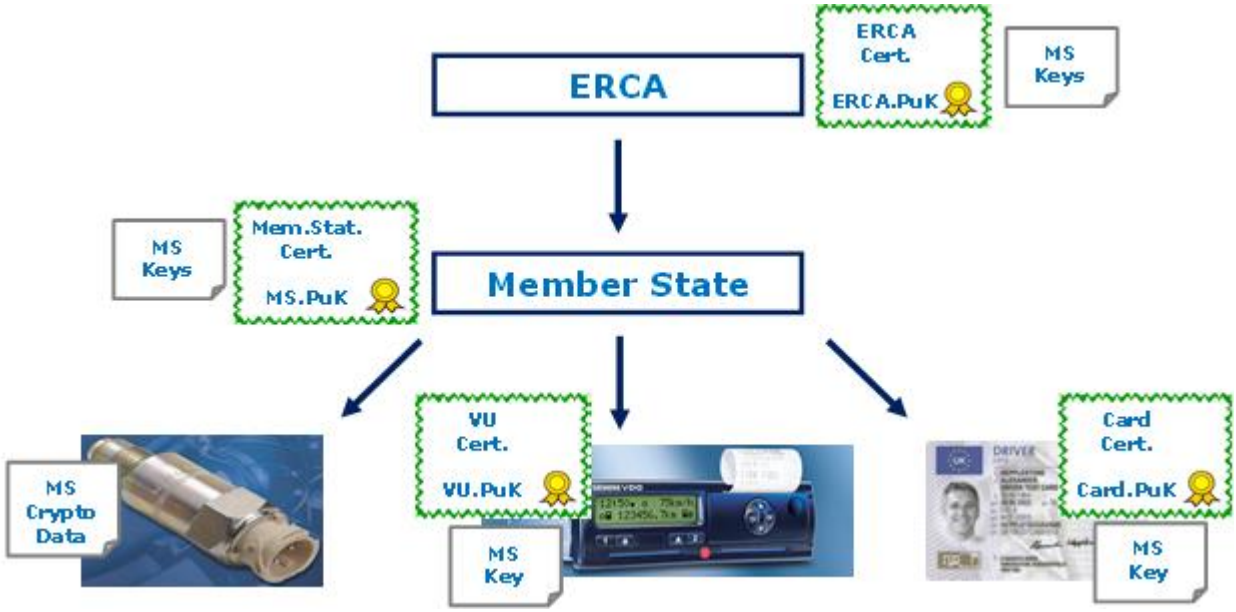

Figure 2 Structure of the European Root Certification Authority for the European Digital Tachograph

The PKI is based on three layers organisational scheme: 1) the European Root Certification Authority (ERCA) maintained by the Joint Research Centre of the European Commission, 2) The Certification Authority in each European member states and 3) the devices themselves (smartcard, VUs) in the truck.

The entities depicted in Figure 3 are the ERCA certification service provider (CSP); a member state certification authority (MSCA) also called National Certification Authority (NCA); and the two types of component personaliser (CP): tachograph card or vehicle unit manufacturing; and motion sensor manufacturing.

The process to get or update the keys is through ERCA sessions in the JRC, which are scheduled every ~2 weeks. The staff involved to maintain and operate ERCA is around 5 JRC employees.

The actors on JRC site are:

- National CA trusted courier, who is responsible for getting the keys at the level of European member state.
- JRC ERCA Administrator and Officer, who is responsible for the management of the ERCA system.
- JRC Security Auditor, who is responsible for the auditing of the ERCA system.

In the Digital Tachograph, system, four cards are used:

1. the Law enforcer card used by law enforcers to access the data concerning the driving time of the drivers.
2. The workshop cards used for first installation, pairing and periodic calibration.
3. The company card used by the companies owning the vehicle.
4. The driver card owned by the driver and which must be inserted by the driver in the Digital Tachograph when the driver is driving the truck.

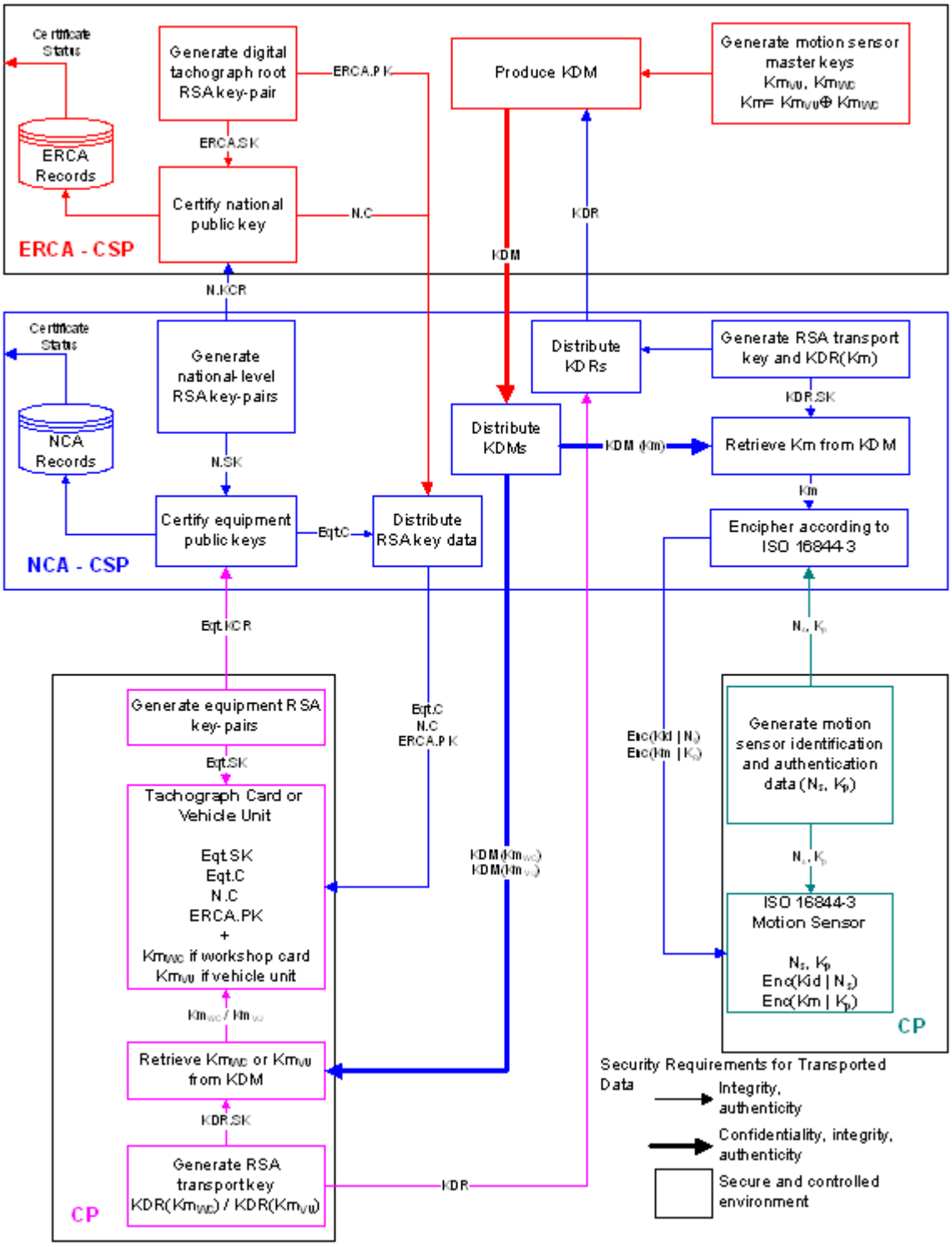

Figure 3 European Root Certification Authority architecture

The complete list of procedures for all the ERCA services are described in [17].

The bootstrap process in the Digital Tachograph is the initial installation of keys in the motion sensor and the vehicle unit. In the Digital Tachograph, symmetric keys are used in the bootstrap phase instead of keys generated by the PKI. The flow for the bootstrap is shown in the right side of Figure 3. The linking/pairing

between the vehicle unit and the motion sensor is implemented in a workshop through a workshop card to ensure an additional level of security: only authorized personnel in the workshop can execute the linking/pairing operation.

Every two years, the trucks are requested to be calibrated again at the workshop. The calibration procedure is recorded and made available to the law enforcers to support auditing and cross-checking of data to detect misbehavior.

The regulation for the Digital Tachograph is currently being revised and new functions are going to be added to the new version of the Digital Tachograph. In particular, a Dedicated Short Range Communication (DSRC) wireless communication device will be added to support targeted roadside check by law enforcers. The data transported over the DSRC link must be signed and encrypted and similar considerations to the other systems based on wireless communications presented here (Car to Car, Connected Vehicles) can be applied.

At the same time the general functionality of the Digital Tachograph except the added data interface remains unchanged and therefore the overall complexity is much lower compared to the C-ITS network and their ITS stations in the various domains with the different categories of stakeholders and final users involved. How far this has an impact on the security topic and the related trust models will be further analysed in chapter 9.

7.2 TCA National Telematics Framework incorporating Gatekeeper

TCA has, as a public authority actively involved in managing goods transport flows in Australia, as part of C-ITS National Telematics Framework, implemented the Gatekeeper PKI Framework for C-ITS telematics applications that require the use of PKI from lorries.

The Gatekeeper PKI Framework consists of policies, standards and procedures governing the use of PKI in Government for organisations, individuals and non-person entities (devices, applications and computing components). The structure of the Gatekeeper Public Key Infrastructure Framework is presented in [12]. Public Key Infrastructure (PKI) is a system of cryptographic technologies, standards, management processes and controls governing the use of digital certificates. The Australian Gatekeeper PKI Framework governs the use of PKI in government, where adopted, for the authentication of internal and external clients (Organisations, Individuals and other entities). Where a government agency uses PKI, it is mandatory that it uses the Gatekeeper Framework. The Strategy enables a whole-of-government framework that delivers integrity, interoperability, authenticity and trust for Agencies and their Clients. This is a framework that provides flexibility to support different user needs and is extensible. It should be noted that while Gatekeeper PKI Framework provides a framework that can be adopted, the implementation for the intended application must be defined by the user and operationally defined.

The Australian approach for the definition of a PKI architecture in the C-ITS domain is quite different from the European approach. In Europe, the PKI architecture was a government initiative and the ERCA is maintained by a part of the European Commission (DG JRC). In Australia, any organizational entity can become an accredited PKI service provider if it fulfills the requirements, obligations and processes defined in [12]. References [13] and [14] define the main features/services and levels of assurance of the Gatekeeper, which are directly relevant to this technical note.

Under the Framework, CAs will be able to operate as “service bureaus”, responsive to Agencies (either directly or via Gatekeeper Accredited RAs) and issue digital certificates on request via standard Public Key

Cryptography Standards (PKCS) protocols. Each Agency will enroll Subscribers for defined PKI-enabled applications according to scheme or program-specific business rules.

An Accredited Service Provider must use security products that have undergone an appropriate evaluation against approved protection profiles, such as the Common Criteria evaluation. International recognition under Common Criteria applies.

The primary characteristics of the Gatekeeper PKI Framework are:

Interoperability	Digital certificates issued by Gatekeeper Accredited Service Providers will be capable for use across jurisdictions.
Transparency	Gatekeeper Policies and Criteria will be publicly available.
Accessibility	Service providers that meet the relevant Gatekeeper Accreditation requirements are able to participate.
Standards-based	Accreditation/Recognition processes are, as far as possible, based on national and international standards (where processes are not yet standardised, Gatekeeper will define C-ITS requirements).
Privacy-centred	Protection of the privacy of personal and corporate data will be a major consideration with mandatory compliance with the *Privacy Act 1988*.
Security-focused	Mandatory compliance with Government security standards.
Risk-based	Agency/business selection of certificate types will be based on a thorough risk assessment of the type of online transactions that are to be facilitated (based on AS/NZS 4360).
Accountability	Accredited and Recognised Service Providers are accountable to the Gatekeeper Competent Authority for compliance with Gatekeeper Policies and Criteria.
Trust	Accreditation processes will provide end users with a sufficient degree of trust in the operations of the service provider and the PKI products used.
Light-touch	• Gatekeeper documentation has been rationalised to reduce the paper burden on Service Providers and streamline the Accreditation process. • Accreditation focuses on security requirements rather than business and legal aspects with commercial and legal aspects managed between Service Providers and Agencies.
Access and Authorisation	Enrolment of certificate holders (i.e. provision of access and authorisation entitlements) is the responsibility of Agencies and businesses. Guidelines on access and authorisation are available from the AGAF Access and Authorisation Guide.
Digital Certificates	• Are based on the X.509 V3 standard. • Provide authentication, confidentiality, integrity and non-repudiation (as required by the PKI domain). • Will accommodate the inclusion of certain attributes in non-critical extensions.

Figure 4 Main features of the Gatekeeper PKI (from [12])

Digital certificates issued under the Gatekeeper PKI Framework will:

- provide authentication, confidentiality, integrity and non-repudiation;
- meet X.509 Standards; and as appropriate
- be able to accommodate inclusion of the Australian Business Number (ABN). An ABN is a unique identifier assigned to each company established in Australia.

Digital certificates issued by Gatekeeper Accredited/Recognised CAs require verification of the identity of the Key Holder to meet the Gatekeeper Binding requirements. The Gatekeeper can provide both Individual and Organizational Certificates in three categories: Special Category, General Category and High Assurance Category. It also defines the concept of Community of Interest (COI).

A COI is a set of Individuals and/or Organisations which agree to transact according to a defined set of rules. A COI may range from a single Relying Party (Relationship Organisation) with multiple Subscribers to multiple Relying Parties and Subscribers. This concept of a COI provides a mechanism to enable trust between organisations for a specific purpose or application.

The Gatekeeper Public Key Infrastructure Framework enables an Organisation to establish its internal identity verification and management processes as equivalent to Gatekeeper Evidence of Identity (EOI) requirements (i.e. a face-to-face evidence of identity check including photographic and signature verification) by means of an independent threat and risk assessment. Under the Framework, an Organisation can be Listed as a Threat / Risk Organisation (TRO) if it is able to demonstrate via a Threat and Risk Assessment that its internal EOI processes are equivalent (from a risk perspective) to Gatekeeper EOI Policy; and managed in accordance with TRO Listing Requirements.

TROs are introduced to reduce the administrative burden and cost to applicants for digital certificates by removing the requirement for a face-to-face EOI check at the time an application for a digital certificate is submitted. The TRO approach provides a further opportunity for those Organisations which do not meet Gatekeeper's requirements for a Known Customer Organisation but whose internal data holdings are risk assessed as adequate.

TROs will not be required to undergo a formal accreditation process under Gatekeeper but must be listed under Gatekeeper. Listing will be a formal acknowledgement that the Organisation has satisfied specific Gatekeeper requirements and will provide the necessary assurance to Relying Parties and Subscribers.

In the transport domain TCA has gained experience since 2005 through the establishment of the IAP Intelligent Access Program for the government by the administration of a National Telematics Framework which provides a nationally-agreed, sustainable environment for the use of telematics and related technologies in trucks.

The Framework is premised on a multi-provider, multi-application environment, which leverages the capability of the market and core elements of the Framework have been recognised and adopted internationally through ISO 15638 - Framework for Collaborative Telematics Applications for Regulated Commercial Freight Vehicles. For the C-ITS domain this means that certified or "regulated", public applications e.g like access to inner city networks for low emission vehicles, are operated in parallel to

market driven applications on the same in vehicle units. For the security aspects of this PKI solution please refer to chapter 9.

7.3 Car-to-Car Communication Consortium and European Telecommunications Standards Institute

The PKI architecture presented in this note is based on references [22] and [23] which are deliverables of the PRESERVE project. This PKI design of the Car-to-Car Communication Consortium is following the architecture specified by the European Telecommunications Standards Institute (ETSI) [24][27].

The Security Infrastructure that aims to protect the V2V and V2I communication (collectively called V2X in the references [22] and [23]) is based on a Public Key Infrastructure (PKI). The PKI consists of different Certification Authorities (CAs). The main components of the PKI architecture are the Root CA (RCA), Long-term CA (LTCA) and Pseudonym CA (PCA). The ETSI PKI design [24] shows the same PKI entities but uses different names. The LTCA is named Enrolment Authority and the PCA is named Authorization Authority.

One of the main components of the V2X architecture is the C-ITS station, which can represent the On Board Unit (OBU) in the car or the Roadside Unit (RSU) or a remote C-ITS center.

An important element of the security infrastructure is the protection against privacy threats, which is implemented through Pseudonyms. Pseudonymity is a mechanism to hide the real identity of the sender. However, using pseudonyms is only efficient if their lifetime is limited. Therefore, the pseudonyms must be changed during the vehicles' lifetime. The frequency of the changes has an impact on the overall architecture.

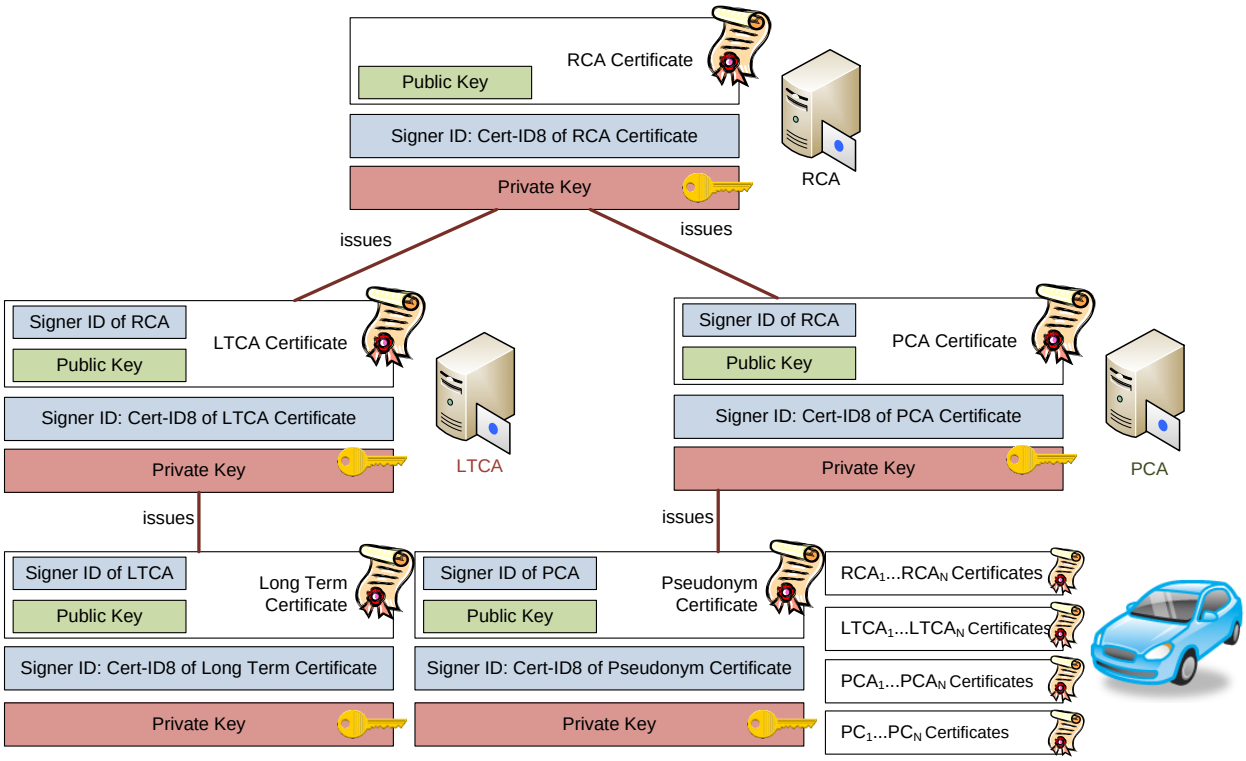

Figure 4 Overall architecture of CAR2X

The general PKI architecture is described in Figure 4. It consists of:

1. The Root CA, which is the trust anchor of the PKI. The certificate of the RCA is signed by itself. The RCA certificate consists mainly of a public key plus additional information such as validity and permissions. With a hash function a digest of the certificate is created that is used subsequently as cert-ID. As previously mentioned, the RCA certificate is self-signed, that is why the certificate contains no signer ID. Fitting to the public key, a private key created by the Root CA is used to sign other CA certificates or certificates for other PKI entities such as CRL signer. The RCA certificate and the cert-ID are public and must be available to all C-ITS stations in the network.
2. The LTCA, which is responsible for enrolment of the C-ITS stations and management of long term certificates that contain identifying information. The long-term certificates are used to identify the C-ITS in PKI requests. However, to provide privacy against the PCA, the long-term certificate has to be transmitted encrypted to the PCA, such that only the LTCA is able to decrypt the message. Then, the identity of the C-ITS station is hidden from the PCA and the privacy of a C-ITS station is preserved, if the LTCA and PCA are separated on an organizational and technical level and if the do not collude.
3. The PCA is responsible for issuing pseudonym certificates that do not contain any identifying information and are reduced to a minimum of size. The number of created pseudonyms per C-ITS station has to be balanced between security, privacy and cost concerns. Providing more certificates to an C-ITS station reduces the security, because an attacker may potentially extract more valid pseudonym certificates with corresponding private keys and hence, forge messages from different senders. The privacy is increased with the number of pseudonyms, because more pseudonyms are available to cycle through in each validity period. However, increasing the number of pseudonym increases also the cost factor of the C-ITS station and also of the PKI, because more certificates have

to be stored by the C-ITS station and more computational power is required by the PKI to sign the certificates

In order to issue CA certificates by the RCA, the LTCA and PCA create independently public and private key pairs. The public key is transmitted to the RCA where an appropriate certificate is generated. The permissions of the LTCA and PCA as well as the public key are stored in the unsigned certificate format. Subsequently, the RCA adds C-ITS own certificate-ID or certificate as signer information and signs the certificate with C-ITS private key. The signed certificate is then returned to the respective CA. Equally to the Root CA, the LTCA and the PCA create a certificate-ID out of their own certificate and publish the certificate afterwards. The private key must be protected particularly in order to avoid misuse of the PKI.

An .important difference with other PKI architectures like the European ERCA is the sporadic availability of the communication channel between the car, the road infrastructure and the control centres, which also include the CA. This communication channel which can provide a moderate degree of availability and moderate data rate connectivity is essential to support various CA services, like the update of the keys and related certificates in an appropriate short timeframe. The C-ITS stations can preload pseudonym certificates for future use in order to allow longer timeframes without connectivity to the CA.

The support of the network for the security functions is visible in Figure 5.

The message payload and parts of the network header are signed by the security layer. The resulting security header contains the secured payload, the signer information such as the certificate of the sender or C-ITS certificate-ID, the signature and additional information such as a secure timestamp or information about the generation location. The basic network header is not part of the secured message as it contains mutable information that changes if the packet is transmitted over multiple hops.

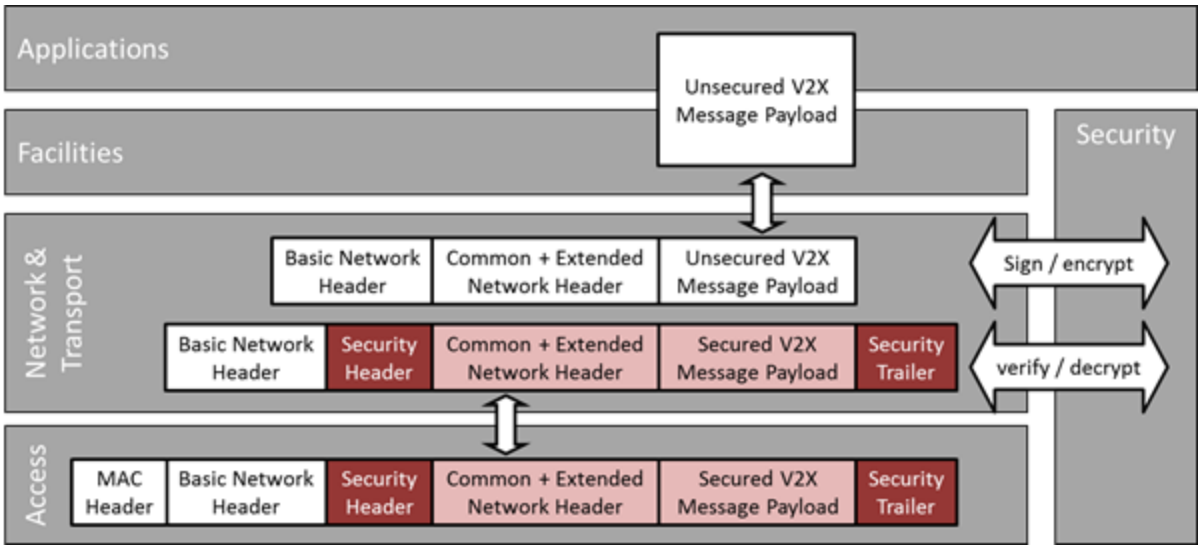

Figure 5 Security processing and communication in CAR 2 CAR (from [24])

With this basic design principles the overall high number of active units are combined with a high level of privacy through the regular exchange of short term certificates pre-installed in the vehicle units. The more detailed comparative assessment of all aspects will be performed in chapter 9.

7.4 Connected Vehicle System – United States

Security Credentials Management System (SCMS) designed by Crash Avoidance Metrics Partnership (CAMP)

The core functions of the Public Key Infrastructure developed for connected vehicle are the same as most other PKI systems. A Root Certificate Authority (Root CA) is the source of trust for all other entities, an enrolment CA provides a long term certificate for users to request short term certificates for interacting with vehicles and devices on the road, a CA generates short term digital certificates for users, while a Registration Authority (RA) distributes the certificates to users.

What makes this system different is that some of the functionality of the typical Certificate Authority and Registration Authority are split into additional entities. Some of these entities are common to recent PKI systems but there are also new functions with new entities all with the intent to protect the privacy of users as well as enhancing security. Figure 5 illustrates a recent version of the SCMS architecture which is still evolving.

Table 2 calls out the additional entities and their primary purpose.

Table 2. SCMS Entities

Basic PKI entities	Added for security	Added for privacy
Root CA	Intermediate CA	Pseudonym CA
Enrolment CA	Certification Lab	Device Configuration Manager
Registration Authority RA	Request Coordination	Location Obscurer Proxy
CRL Broadcast mechanism	Misbehaviour Authority	Linkage Authority 1
	SCMS Manager	Linkage Authority 2

These entities use private asymmetric keys to sign their messages and decrypt received messages and public asymmetric keys to encrypt and distribute symmetric keys amongst themselves. They will use their symmetric keys to encrypt messages between entities internal to the SCMS.

In the current design, user devices in vehicles will use certificates in bundles of 20-40 that are good for a 2 week period. The certificates are used for randomly variable short periods on the order of minutes and reused randomly throughout the 2 weeks. Then they expire and the on-board unit (OBU) activates a new bundle. Whether the OBU will download these bundles in batches to cover a year or more, or periodically top off the certificate store is still under discussion. The details of certificates for roadside equipment (RSE) are still being worked out as well. Expect that the batch sizes and lifetime of V2V certificates and V2I certificate to be different.

The SCMS entities can be looked at in terms of 3 different kinds of functionality: Governance, Bootstrap and Pseudonym Operations.

7.4.1 Governance

The SCMS Manager is the entity that will provide policy and governance for the SCMS and perhaps it's supporting industry. It will give and withdraw permission for operating entities within the SCMS. It decides

on the policies and industry-wide practices like auditing and standard operating procedures as well as the technical requirements that govern the operation of SCMS entities and users. Some kind of central administrative body is anticipated but the details of the SCMS Manager are still to be determined. Also not determined is whether this role will be performed by the private sector with something like a volunteer industry consortium or by a quasi-public organization or a legal/regulatory body.

7.4.2 Bootstrap

A new user enters the system through the Bootstrap functions. They provide the OBU a long term digital certificate that it can use to request the short term certificates it needs to interact with other devices as well as trust credentials (certificates) for other components of the SCMS.

The bootstrap functions are listed below in the order in which they would become engaged to respond to a certificate request:

- Device Configuration Manager (DCM)
- Enrolment Certificate Authority (ECA)
- Certification Lab

7.4.3 Pseudonym Operations

The remaining entities provide the short term certificates the device needs to be trusted by other devices in the connected vehicle environment and the mechanism for recognizing and revoking misbehaving devices. These short term certificates are called "pseudonym" certificates because they contain no identifying information about users. So the users can be anonymous in the system yet still trusted as long as their certificates have not been revoked. The pseudonym functions that create, manage, distribute, monitor, and revoke these short-term certificates for vehicles and devices are listed below in two groups. First, the entities that establish the chain of trust all user certificates rely on and second, the entities that are involved with the short term certificates in the order by which they engage upon a request for certificates.

Trust chain entities

- Root Certificate Authority (root CA)
- Intermediate Certificate Authority (intermediate CA)

Pseudo-certificate entities

- Location Obscurer Proxy (LOP)
- Registration Authority (RA)
- Request Coordination
- Linkage Authority (LA)
- Pseudonym Certificate Authority (PCA)
- Misbehaviour Authority (MA)

This presentation is at a conceptual level because the SCMS is still being designed. Therefore, exactly how most of the IT level requirements of the Common Criteria will be implemented is still to be determined. What of these details the designers will decide, and what the SCMS Manager will decide during implementation, is also still to be determined.

Further details are in [8].

7.5 Comparison among the Case Studies for Intelligent Transport Systems

This section provides a qualitative comparison among the case studies. Note that this comparison is valid at the moment of drafting this technical report (February 2015) and it is only for informational purpose. All the identified case studies are subject to evolution and changes. As a consequence, this comparison table can change in the future.

	Europe / Digital Tachograph	**USA / Connected Vehicles**	**Australia**	**Europe / Car to Car**
Certification Authority	Yes, ERCA	Yes (different levels: Root CA, Enrolment CA, Intermediate CA and PCA)	Yes, CAs can be added using the Gatekeeper framework.	Yes (different levels: RCA,LTCA and PCA)
Key Backup	The ERCA RSA private key and the motion sensor master keys shall be backed up, stored and recovered only by personnel in trusted roles using at least dual control in a physically secured environment. Backup copies of the ERCA RSA private key and the motion sensor master keys shall be subject to the same level of security controls as the keys in use. One backup copy of the ERCA RSA private key and the motion sensor master keys shall be maintained off-site	Yes	Yes, it is the responsibility of the subscriber.	Yes
Key History Management	Supported in the new version of the Digital Tachograph for migration aspects.		Yes. This has been confirmed however specific details are not known.	Yes for CAs and enrolment keys (Long term certificate) of the C-ITS at the LTCA. The PCA is not able to manage a pseudonym certificate key history

				as pseudonyms cannot be linked. LTCA can only store how many pseudonyms are issued but has no access to the pseudonym keys.
Authentication	Manual authentication	Yes. Message authenticated with digital signature. Users authenticated in the Enrolment process, details TBD	Through the Formal Identity Verification Model and the Registration Authority (RA).	Yes, all PKI processes require authentication of the end entities. Automatic authentication of enrolled C-ITS stations.
Secure Time Stamping	Yes, ERCA and through the GNSS module in the truck in the revision of the digital Tachograph.	Yes. Either GPS or to an NIST clock (TBC)	Possible – application specific. Secure time-stamping using evaluated time-stamping server.	Yes, through GNSS synchronized time
Certification Repository	Yes, ERCA	Secure onboard storage in the OBU.	Yes – Repository is available for the different supported applications as required by the application	Public repository of CA certificates and keys at RCA. Secret internal repository of long term certificates and public keys at LTCA. No repository of pseudonym certificates and keys at PCA. Secure onboard storage in the OBU.
Key Recovery	Yes, see [8]. Recovery in the following cases: a) compromise or theft of the ERCA root key and / or the motion sensor master keys; b) loss of the ERCA root key and / or the motion sensor master keys;	TBD	Yes, it is the responsibility of the subscriber.	Yes, even if it is not fully described in the references. Recovery of CA keys. No recovery of keys owned by the C-ITS station such as long term private key and pseudonym private

	c) IT hardware failure			keys.
Cross Certification	Not supported	TBD	Yes, through Cross-Recognition as described in [12].	Not supported Cross-certification of RCAs is to be discussed.
Integrity	Yes.	Yes	Yes	Yes, all PKI processes require integrity protection of transmitted data. Even platform integrity is supported through the Platform Integrity Module (see [22][23]).
Notarization/Data Certification	Yes, through the signature of the logged data.	Digital signature authenticates the message and proves integrity (not tampered with) but the data in the payload could be wrong from the source, like a bad sensor. Data not certified but could be subject to plausibility checks at the receiver, or even just before transmission.	TBD	Data plausibility checks at the sender and receiver. Sending C-ITS station checks data consistency and plausibility of sensor information. Receiver performs data plausibility checks of received data using time and location information from internal sources.(Note that the sensor information could be still wrong even if the security integrity is respected)
Certificate Revocation	Revocation of the certificates is done manually but the status of the certificates can be consulted on-line	Yes. Automated scheme with CRL devised. CRL tells users what messages not to trust. Misbehavers are removed when their request for new certificates is rejected. Misbehavior detection and details of the revocation process	Yes. It is not clear if it is manual or automatic.	Yes, CA certificate revocation with CRL. No active revocation of pseudonym certificates but reject of pseudonym certificate update requests if C-ITS station is revoked.

		TBD.		
Cryptographic material (e.g., Key or certificates) Update	The key update is only manual. No automatic key update is provided.	Yes if this is covered by the certificate renewal process. Otherwise, not sure.	Manual however may be automated for specific applications	Yes and it is both dynamic and automatic.
Client Software	This is the client software of the DT application.	This is the client software or application of the user/	This is the client software or application of the subscriber. This can be anything required by the application	Yes. It is present in the OBU of the C-ITS station
Confidentiality	Yes	* Requests and certificates are encrypted for transmission. * Data for applications without latency requirement can be. * Low latency real-time app data is not encrypted. * Where latency is not critical, encryption is left for the app to decide.	Yes	- Yes, for the communication with the PKI. - Optional, for the communication between C-ITS stations.
Non-repudiation support	This is done through a combination of authentication and integrity	Yes. Being able to decrypt a message or signature with the sender's public key proves it is from their private key.	Yes (Within the defined COI for special category)	Yes, through a combination of authentication and integrity
Privacy	Yes, through access control mechanism.	Yes, through pseudonyms, linkage values, organizational separation of functions.	No	Yes, through the pseudonyms and separation of LTCA and PCA.

7.6 Additional Case Studies

7.6.1 Trust model for electronic passports in Europe

Machine readable travel documents (MRTD) support advanced security mechanisms for the protection of the data stored in the MRTD. One of these mechanisms is the extended access control (EAC). If data stored in a MRTD is protected by EAC a terminal must be authenticated by the MRTD and must prove its right to the MRTD before the terminal can access the data.

This common Certificate Policy provides a common set of minimum requirements upon which each Members State shall base a National Certificate Policy for use of certificates for border control purposes. The terminal authentication to be performed before reading protected data out of a MRTD is based on CV certificates which can be verified by a MRTD. The access rights given to a terminal are coded within the CV certificate. After verifying the CV certificate the MRTD grants access to its data according to the access rights coded in the CV certificate. A public key infrastructure for the generation and distribution of these CV certificates is outlined in [48]. Within the EAC-PKI each member state operates its own root CA called country verifying CA (CVCA). The second level of the EAC-PKI is formed by CAs called Document Verifier (DV). Each DV is associated to the national CVCA of its own country. The DV gets its own CV certificate from that national CVCA and generates the CV certificates for inspection systems (IS) within its sphere of influence.

As described in [49], the PKI design is basically cross-certification among the country verifying CAs. Each country sets up a single point of contact (SPOC) system, essentially an interface between the country and other countries. All inter-country communications are conducted through their SPOCs, which are connected to the Internet. A SPOC collects certificate requests from each domestic document verifier, sends them to the SPOCs of the destination countries, which, in turn, forward the requests to their CVCAs. A certificate generated by a CVCA (or a failure notification) is returned along the same path, in reverse order, up to the document verifier that originated the request. Thus, a SPOC, on one hand, collects and forwards internal document verifier requests directed at foreign CVCAs and, on the other, collects and forwards foreign requests addressed to its domestic CVCA.

7.6.2 Bridge CAs in Europe

In this section we describes two main Bridge CAs in Europe:

- The European Bridge CA is a privately run initiative of Deutsche Bank and Deutsche Telekom, and is a “pure” implementation of the bridge model, providing a central CA which cross-certifies with each CA domain. It has provided interoperability among a few major EU companies [44]. The European Bridge CA is an example of large Bridge CA. The European Bridge CA operates a virtual Directory Service. Certificates of participants from different companies can be called up via this Directory Service. For this the LDAP-queries of the Bridge-CA are forwarded to the repositories of the connected organisations.

- Bridge/Gateway Certification Authority (BGCA). The EU IDABC Bridge/Gateway is a model for bridge CA, which can be operated by the European Commission and it allows interoperability between the PKIs of EU governments and their agencies. The model assumes that in each Member State there will be a national CA that operates that government’s PKI. Civil servants in national public administrations that participate in IDABC networks must use electronic certificates from the IDABC PKI for security of communications, encryption and electronic signature.

There are two main reasons for this. The first is due to interoperability problems. The second is that there is no way, at present, for trust to be established in an electronic certificate from a certification authority other than one's own.

For national public administrations to use electronic certificates, issued by their national CAs (i.e. the CAs contracted to provide certification services to their national public administrations) in IDABC networks or in trans-European (i.e. cross-border) communications with other Member States' administrations, a mechanism must be found whereby trust and confidence can be established between these CAs. Such a mechanism is a 'bridge' or 'gateway CA'. IDABC was charged, at the request of the Member States, to carry out a study, (an action of the 2001 work programme) to examine the feasibility of establishing a bridge or gateway CA to act as an intermediate trust infrastructure between the PKIs of Europe's national public administrations (from [45]).

8 Trust Models for C-ITS based on PKI

8.1 Introduction

In this section, we discuss the potential trust models for C-ITS based on PKI concepts. We start from the taxonomy of trust models provided in [35] by Pearlman. While this is an essential reference, it is a bit dated (1999) and we will integrate it with additional trust models not mentioned in [35].

The main element of the PKI trust model is the CA. The Root CA is the "Trust Anchor" for the whole PKI. The PKI and all users / end users shall trust the operator of the Root CA over the whole lifetime of a service. This trust model includes agreed processes, policies and rules, which must be followed for the Root CA and its underlying CAs and which should be correctly in place and audited from accredited authorities.

We can have a PKI design based on a hierarchy with a single Root CA (as in the case study of the Digital Tachograph) or with many CAs, which are cross-certified. The concept is Cross certification is described in the following paragraph.

8.2 Concept of Domain

In the rest of the technical report, we will use the term *domain* to identify an area with the same security policies. The concept of domain is an essential element of the analysis presented in this trust model, so it is described in detail in this section.

The concept of domain is based on the security domain from ISO/IEC 15816:2002-02-01, where a security domain is defined as a collection of users and systems subject to a common policy. An important element of the policy is the definition of the credential (a credential is an attestation of an individual's identity by a third party) management systems with the responsibility for ensuring that credentials are issued only to parties in the domains, which are entitled to them. Because the scope of the analysis of this report is the implementation of trust model through PKI, a credential can be linked to a digital certificate. Another important element is the cryptographic algorithms used to generate the credentials and digital certificates.

The concept of domain can be refined on the basis of the presence of jurisdictional or political authorities (e.g., a member state), so that we can different layers of domains, which are identified here:

- A C-ITS **security** domain is defined as a system under the control of a single authority which the entities therein trust. There is one security policy in place in a security domain and it is defined by the domain authority.

- A C-ITS **trust** domain is made up from multiple security domains belonging to different authorities, but with the same **certificate** policy in place. The authorities **trust certificates issued in all security domains**.

- A **federated** C-ITS **trust** domain is made up from multiple trust domains belonging to different authorities, with different **certificate** policies, but with the same security goal. After appropriate trust extensions, the authorities **trust certificates issued in all trust domains**.

The analysis in section 8.4 for the trust model options is specific for the trust domain where the same certificate policy is in place. In the rest of the document the term C-ITS domain is generically used to represent all the layers, even if most of the times, it will be specified to which layer we refer.

The concept of policy can be refined to differentiate between security policy, certificate policy and Certification Practice Statement (CPS).

- **Security policy:** rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems, particularly those which impact the systems and associated elements (ISO/IEC 21827:2008-10-15).

- **Certificate policy (CP):** - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. (IETF RFC 3647, [51]).

- In addition, the **Certification Practice Statement (CPS):** A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. (IETF RFC 3647, [51]).

The relationships between CP and CPS is clearly defined in [51]:

"A CP sets forth the requirements and standards imposed by the PKI with respect to the various topics. In other words, the purpose of the CP is to establish what participants must do. A CPS, by contrast, states how a CA and other participants in a given domain implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the participants perform their functions and implement controls.

An additional difference between a CP and CPS relates the scope of coverage of the two kinds of documents. Since a CP is a statement of requirements, it best serves as the vehicle for communicating minimum operating guidelines that must be met by interoperating PKIs. Thus, a CP generally applies to multiple CAs, multiple organizations, or multiple domains. By contrast, a CPS applies only to a single CA or single organization and is not generally a vehicle to facilitate interoperation".

Examples of Security Policies including CP and CPS in the road transportation sector can be found in [14] for the Australian Gatekeeper (see section 7.2), and [17],[18] for the European Digital Tachograph (see section 7.1). On the basis of IETF RFC 3647 and the cited references ([14], [17],[18]), the following elements are part of the Certificate policy (CP) and Certification Practice Statement (CPS):

Certificate Policy:

- Key Generation includes the minimum length for the public key and private key pairs. It also includes the cryptographic algorithms used to generate the keys.
- Participants of the trust model based on PKI and their role. This includes certification authorities, registration authorities, subscriber relying parties. It also includes the processes for users enrolment.
- Certificate revocation and suspension to define requirements on who has the authority to issue revocation and suspension and the associated procedure.
- Certificate use, which describe the authorized and prohibited certificate uses.
- Legal issues, such as liability, that might arise if the CA becomes compromised or is used for something other than its intended purpose.

- Private key management, including the requirements for the storage on physical devices (e.g., ITS stations).

Certification Practice Statement (CPS)

- Policies, procedures, and processes for issuing, renewing, and recovering certificates
- Physical, network, and procedural security for the CA. This is about the physical protection of the networks and infrastructures supporting the CA.
- Management and Operational controls including the processes for audits of the PKI and the CA servers, archival of records and compromise and disaster recovery. Note: this an important element to support the mutual trust of the PKIs in cross-certification models. Some implementations of RFC 3647 do not include auditing of CA in the CPS, but we decided in this analysis to include in the CPS all the management and operations processes to support mutual trust.

These elements override other elements defined in the security policy, which can be a wider document, defining processes and organizational structures beyond the PKI itself. For example, the training of the personnel could be defined in the security policy rather than the CPS unless it directly impact the trust of the PKI.

The domain concept (whatever is the level of the layer) can be developed in three dimensions:

1. *Space*. A jurisdiction where a common set of security policies or certificate policies for road transportation is defined. For example, Europe and USA or different member states in Europe.
2. *Time (meant as changes in the regulatory framework)*. Policies, technologies or trust frameworks can change in time. A domain can modify C-ITS features as a consequence of any of these changes. As a consequence a new domain is created, but road equipment may support both old and new domains. An example is the revision of a regulatory framework like the Digital Tachograph from the old version to the new version defined by regulation 165/2014.
3. *Applications*. A domain can be defined by a set of applications or by a single application, whose trust model can be based on policies, security requirements, design and technologies are quite different among each other. For example, the application of mobile advertising for road transportation can have different security features from the applications of collision avoidance or hazards notification. These applications could coexist independently in the road transportation market or they could interoperate to support a more complex application. In the latter case, mutual trust should be ensured to support secure interoperability among the applications. Example of applications can be Traffic signal priority request by designated vehicles or Traffic jam ahead warning, which can involve both V2V and V2I.

8.3 Security Interoperability: Trust extension

Extending Trust is needed to enable end-users (C-ITS-Stations) of one PKI to trust certificates issued in another PKI. One relevant method to extend trust is cross-certification. When two CAs are cross-certified, they agree to trust and rely upon the digital certificates issued by them. It allows easy and scalable trust management between certified entities.

Cross-certification is the act of one CA issuing a certificate to another CA, which is also stated in X.509 standard [10]: “Cross certificate – This is a certificate where the issuer and the subject are different CAs. CAs issue certificates to other CAs either as a mechanism to authorize the subject CA’s existence (e.g. in a

strict hierarchy) or to recognize the existence of the subject CA (e.g. in a distributed trust model). The cross-certificate structure is used for both of these."

We can have three models of cross-certification (see [2],[39]):

1. Intra-domain cross-certification, which defines trust relationships between CAs inside the same administrative domain. This can be used in case the C-ITS Trust model is based on a Federation of Root CAs
2. Peer-to-Peer cross-certification, which defines trust relationships between two autonomous (either standalone or hierarchical) CAs. This is also called inter-domain cross-certification. This is necessary for any C-ITS Trust Model, since Europe has borders with other future potential C-ITS domain(s).
3. Bridge CA (BCA) model, representing a trustworthy independent node, which establishes trust relationships with several non-related CAs. This approach can be used both as intra-domain as well as inter-domain cross-certification.

We can have variations on these models. We can also have unidirectional or bi-directional cross-certification.

In the case of bi-directional cross-certification, a reciprocal relationship is established between the CAs - one CA issues a cross-certificate for the other, and vice versa. Unilateral cross-certification simply means that one CA generates a cross-certificate for another CA, but the inverse is not true.

The advantages of intra-domain cross-certification are:

- One of the primary advantages associated with cross-certification is that each PKI domain retains C-ITS autonomy. That is, external trust relationships can come and go without affecting the internal trust relationship between the relying parties and their trust anchor within a given PKI domain [34].
- The model is more flexible because a new organization (e.g., a new member state) or a new C-ITS application with C-ITS own PKI could be inserted in the model without the need to update all the cryptographic materials or change the PKI structure. This is facilitated by the fact that the technology and the domain is the same in this specific case.

The disadvantages of intra-domain cross-certification are:

- A protocol for the exchange of information must be established to guarantee a level of trust among the CA. This protocol could be quite complex to establish even if there are already a number of case studies.
- The control on many different CAs can be less strong than the case of a single CA. One of the CAs could be compromised and this will impact the entire PKI. It is easier to control a single CA than a number of CAs.

Other possible options for cross-certification, which are discussed below are:

1. Certificate Trust List model (see [50]) which makes available trust service status information such that interested parties may determine whether a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

2. the delegate CA Trust model, where already configured CAs can sign certificates authorizing other CAs to grant certificates [35].
3. The Pretty Good Privacy (PGP) model, where each user is responsible for configuring some trust anchors [35].

In order to provide the required level of functionality and reliability to cross-certification, each domain has to implement a minimum set of certification services, building and validation algorithms, and issue public key certificates with some extensions requirements.

One of the main services that need to be offered to an entity (e.g. end user, device or software process) is the possibility to determine whether the certificate provided by any other entity can be trusted or not. This decision will be based on the existence of a valid certification path between the target certificate and a trust anchor that may belong to different domains. The infrastructure has to ensure that the path can be built and validated in real time and several services are necessary to be implemented by every organization involved in the certification path. This implies that a cross-certification model requires some extra services that might not be needed by a single PKI deployment. At least the following services are needed:

- Certification repository: repository services have to include, beside CAs and end user certificates, cross-certificates for each trust relation-ship with other domains and CRLs.
- Validation Service: the Validation Service implementing the algorithm that generates and validates certification paths should support cross-certification. This can be computed locally or delegated to an external server using protocols like e.g. SCVP.

These two services are critical in public key infrastructures in order to provide building and validation mechanisms to third trusted parties. Current solutions provide CRL-based validation mechanisms and some of them also offer advanced services like OCSP. However, neither CRL nor OCSP were designed to provide advanced certification path building and validation, but simple certificate status request. Indeed, a more suitable protocol such as SCVP has to be deployed for these cross-certification scenarios.

Regarding certificate extensions, some of them need to be included to support cross-certification. For instance, Authority/SubjectKeyIdentifier, KeyUsage and BasicConstraints can be used to help the validation service to decide between different cross-certification paths; AuthorityInfoAccess can be also used to recover information about validation services (CRL/OCSP) from cross and end user certificates; and NameConstraints can be defined to exclude certification paths. Finally, some policy extensions (CertificatePolicies, PolicyMappings, etc.) can also be specified to support policy definition. More detailed information about required certificate extensions can be found on [2].

8.4 List of options for Trust Models based on PKI

8.4.1 Introduction

This section describes the main trust model options based on PKI, which can be adopted for C-ITS. Two main categories are defined when the PKI is applied to a single Trust domain (see 8.2) based on a single certificate policy or to a Federated Trust Domain with multiple certificate policies. The first category is represented by Options 2.x, and the second category is represented by Options 3.x. Option 1 represents the security domain case with a single security policy as there is only one root CA.

8.4.2 Option 1: A single Root CA

The "single Root CA option" is the simplest C-ITS trust model. In this case, there is a single root CA in the C-ITS domain (i.e., it is a C-ITS security domain). A C-ITS-Station has C-ITS root of trust in the Root CA and has the corresponding root CA certificate securely installed. This trust model can have a single RA (as in the Digital Tachograph application) or multiple RAs (one for each member state).

The policy authority is a body recognized by all current and future C-ITS stakeholders within the C-ITS domain. It is also in charge of defining the inter-domain cross-certification requirements.

The single root CA can be operated by a single authority, which can be either public or private or based on a public-private partnership and it is based on a single security policy. While there could be a single root CA, we could have a multi-layered structure as in the case of the Digital Tachograph where below the root CA, we have intermediate CAs for each member-state.

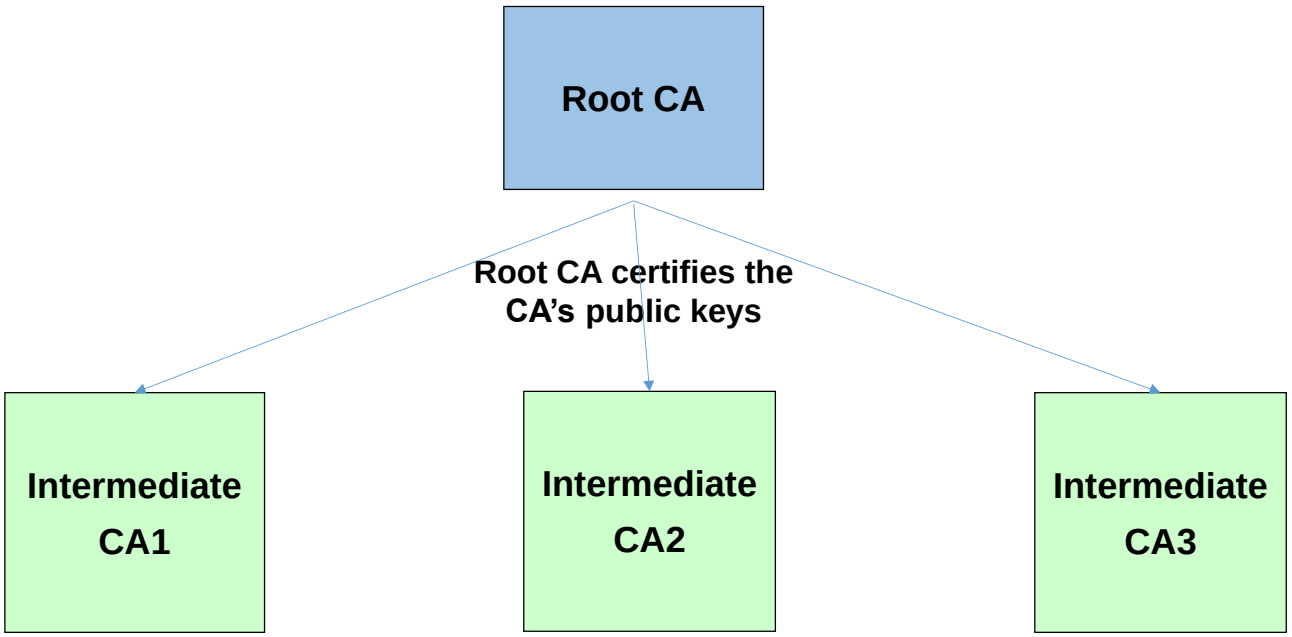

Figure 6 Hierarchical trust model based on a root CA

Organisational aspects to be considered:

- This trust model could be difficult to implement and deploy from an organizational/political point of view because all the involved organizations must trust the organization responsible for the single root CA. In the real world, this is not easy to achieve. If a single organization is given the monopoly on granting certificates in the entire C-ITS domain, there is the risk that it will have excessive power and it can use this power to charge excessive fees for issuing certificates [30]. This is why a public organization could be preferable (as in the case of the Digital Tachograph application).
- The policy authority needs to act in the interest of the stakeholders, and the stakeholders need to endorse C-ITS decisions
- Parallel, independent trust models need to be prohibited.

Technical aspects to be considered:

- One policy means simpler technical implementation. For example, a new intermediate CA (e.g., a new European member state) could be inserted in the system without the need for the ITS station to download new root certificates to interoperate with the ITS stations (e.g., roadside equipment of the new member state) related to the new intermediate CA, because the root CA will be the trust anchor.
- Cross-certification with other domains is difficult since it is challenging to find a mapping between the respective policies.

8.4.3 Option 2a: Federation of Cross-certified Root CAs in the same domain

In the *Federation of Cross-certified Root CAs in the same domain* option for the C-ITS trust model, there are multiple Root CAs in the C-ITS domain. The organizations responsible for the root CAs constitute a federation which jointly defines, maintains and updates the federation's security policies The federation can also delegate an external entity to draft the security policies.

The federation shares a single certificate policy, it can have multiple security policies but they should be harmonized to similar high level trust requirements to support the same level of trust across different authorities.

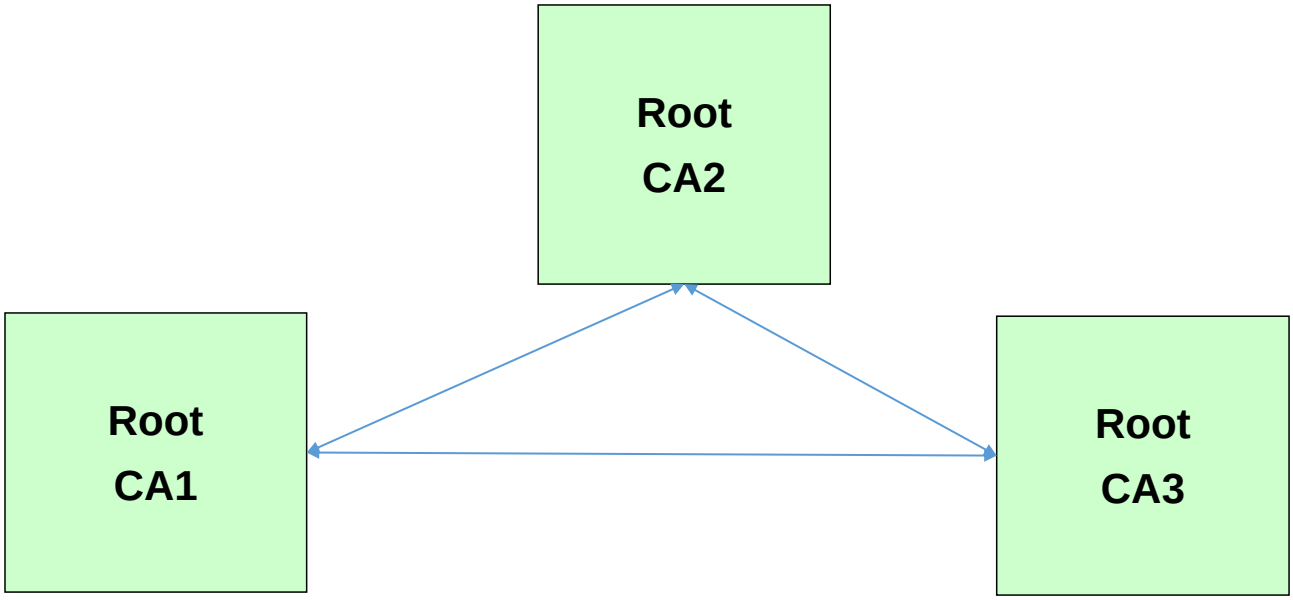

Figure 7 Federation of cross-certified root CAs

The federation acts as the policy authority. It is also in charge of defining the inter-domain cross-certification requirements.

Each Root CA is the root of trust in the PKI which is constituted by:

1. The Root CA itself
2. The EAs and AAs that received CA certificates from the Root CA.
3. The C-ITS stations that are enrolled with one of the EAs in the PKI.

The different Root CAs can be operated by different stakeholders (interest groups) and set-up within different time scales. The Root CAs are cross certified. A C-ITS station has C-ITS root of trust in one of the Root CA and has the corresponding root CA certificate securely installed.

Organisational aspects to be considered:

- The founders of the federation will define the security policy or security policies and the single certificate policy.
- Changes to the security or certificate policies needs to be agreed between all parties of the federation.
- Parallel, independent trust models need to be prohibited.

Technical aspects to be considered:

- One certificate policy means simpler technical implementation.
- Cross-certification with other domains is difficult since it is challenging to find a mapping between the respective policies.

8.4.4 Option 2b: Bridge CA in the same domain

This option is similar to option 2a, with the difference that the federation decides to set-up and operate a Bridge CA. The Bridge CA is based on a special trust model sometimes referred to as the "hub and spoke" model. Current Bridge CA initiatives use cross-certification as the basis for interoperability among PKIs parties in different areas. The Bridge CA does not operate as a root and it does not issue certificates to subordinate CAs or relying parties but it exchanges pairs of cross certificates with each participating parties. One example is the Bridge CA used by the US Federal Government to link the PKIs of different state departments and agencies [40].

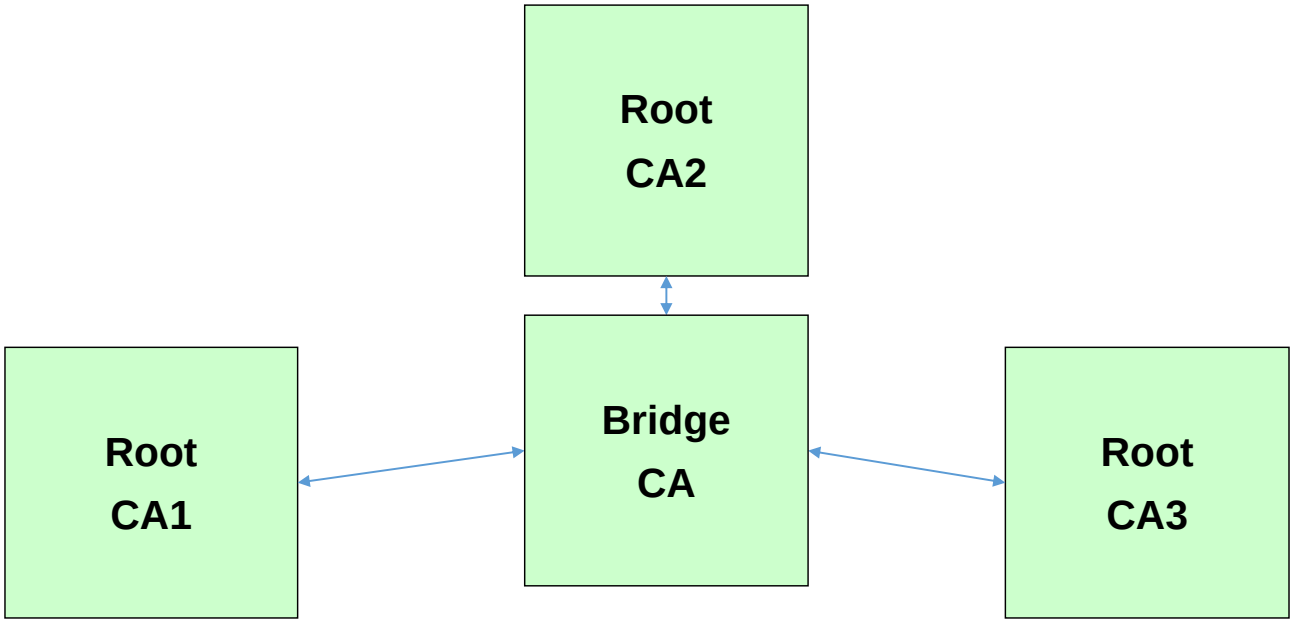

Figure 8 Bridge CA

The Bridge CA provides some important advantages in comparison to other model of cross-certification:

1) It sidesteps the political problem of trying to find a single CA.

2) It supports scalability by supporting a large number of CAs
3) From the cost point of view, it spreads the cost among the participating CAs.
4) In comparison to a mesh cross-certification, it simplify the complexity of the relationship between the different CAs.

The disadvantage is that a new entity (non-CA) must be put in place and that a cross-certification protocol must be established anyway.

We can have Bridge CAs within the same domain or across different domains and cryptographic algorithms (see [42]).

This trust model has the same certificate policy and a single security policy for the bridge CA, even if different CAs can have different security policies even if the security policies but they should be harmonized to similar high level trust requirements to support the same level of trust across different authorities.

8.4.5 Option 2c: Certificate Trust List/Independent CAs in the same domain

In the "Independent Root CAs using the same policy" option, there are multiple Root CAs in the C-ITS domain. Those root CAs use the same certificate policy and use the same security technology (e.g., cryptographic algorithms and certificate formats), which are defined by a single organization. The policy authority is a body recognized by all current and future C-ITS stakeholders within the C-ITS domain.

The different Root CAs can be operated by different stakeholders (interest groups) and set-up within different time scales.

Organisational aspects to be considered:

- The policy authority needs to act in the interest of the stakeholders, and the stakeholders need to endorse C-ITS decisions

Technical aspects to be considered:

- Multiple root CA certificates to be installed securely in the C-ITS-Station represent a challenge, especially if this needs to be done after deployment
- One certificate policy means simpler technical implementation.
- Cross-certification with other domains is difficult since it is challenging to find a mapping between the respective policies.

This trust model is also related to the Certificate Trust List (CTL) concept as an alternative concept to multiple root CA certificates being installed securely in the C-ITS-Station. In fact one or more authorities (e.g. EU national representatives) may provide to the ITS stations a list of certificates linked to the CAs. In other words, CAs do not establish a trust relationship between them and there are no certification paths in this architecture, but only certificates. Entities must maintain a list of CAs that they trust.

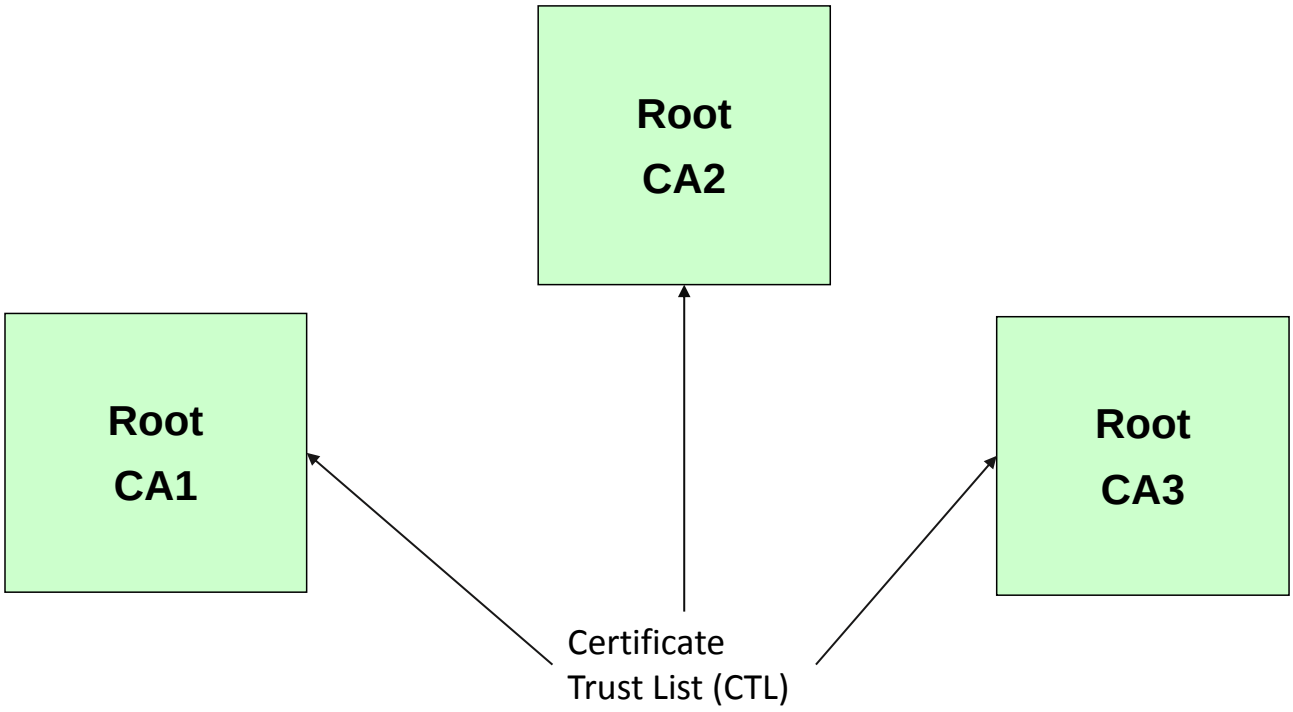

Figure 9 Certificate Trust List/Indipendent CAs

8.4.6 Option 3a: Federation of Root CAs in multiple domains

In the "Federation of Root CAs in multiple domains" option for the C-ITS trust model, there are multiple Root CAs across different domains. Those Root CAs constitute a federation which jointly defines, maintains and updates rules for cross-certification of security and certificate policies. It is also in charge of defining the inter-domain cross-certification requirements.

This means that the Root CAs may choose their certificate policies and use the security technology (e.g., cryptographic algorithms and certificate formats) within a framework established by the federation to achieve a common security goal

The different Root CAs can be operated by different stakeholders (interest groups) and set-up within different time scales. Each Interest group also acts as the policy authority.

The Root CAs are cross certified (see intra-domain cross-certification). A C-ITS-Station has C-ITS root of trust in one of the Root CAs and has the corresponding root CA certificate securely installed (the "home" PKI).

Organisational aspects to be considered:

- The founders of the federation will define the framework for the Root CA policy. Newcomers to the federation will have to accept the common framework.
- Parallel, independent trust models need to be prohibited.

Technical aspects to be considered:

- Cross-certification with other domains is possible within the federation's framework
- Each Root CA is free to change certificate policy within the framework but this implies a change to C-ITS root CA certificate and new cross-certification

1. The C-ITS station must deal with various crypto algorithms and certificate format which could be an issue for telematics devices with limited capability. This might include the need to have different hardware components for the different cryptographic algorithms (e.g., crypto modules) and associated policies.

8.4.7 Option 3b: Bridge CA in multi-domains

This option is similar to option 3a, with the difference that the federation decides to set-up and operate a Bridge CA. In this option, the bridge CA is able to support multi-domains. This may require the capability to support different cryptographic algorithms or different set of security policies, which can increase considerably the complexity and management of the bridge CA. For example, the bridge CA may require different set of crypto modules to support different cryptographic algorithms. As in the previous case, the advantage is a more flexible design because the bridge CA can support various present and future applications at the expense of an increased complexity of the bridge CA itself. The security policy of the single Bridge CA must be unique, while the security policies of the participating CAs can be different.

8.4.8 Option 3c: Certificate Trust List/Independent CAs in multi-domains

This trust model option is the same of Option 2c, with the difference that the policy and algorithms can be different, which makes the implementation much complex because the entities must be able to process different cryptographic algorithms or set-up different organizational structures and processes.

If the requirements defined in the different Certificate Policies are quite different, option 3c may require that the managing entities implement completely different PKI systems and processes with very high costs both from a management and economical point of view. From a management point of view, because the personnel must design and execute different organizational processes and set-up different organizational interfaces for each domain. From an economical point of view, the deployment of different cryptographic systems will require high CAPEX (to duplicate hardware systems) and high OPEX (for the maintenance of different systems). The complexity will also be in the C-ITS stations, which must implement crypto-agility for different cryptographic algorithms. This will considerably increase the cost of C-ITS stations and it can severely hamper the successful adoption of C-ITS in Europe.

8.4.9 Option 4: Delegate CA

In this option, the established CA can sign certificates authorizing other CAs to grant certificates. This trust model may not be alternative to the other models, but actually complementary. For example, a multi-hierarchical PKI based on root CA or cross-certification can still have delegate CAs for ancillary applications or member states, which do not want to create or maintain a CA server.

This option is not viable for C-ITS and will not be further analysed.

8.4.10 Option 5: Pretty Good Privacy (PGP) model

Trust in PGP is achieved using the web of trust model. The underlying idea of this model, is that you accept the public key of a PGP user if it has been signed by one or more other trustworthy PGP users. In other words, you are relying on trusted PGP users to introduce others. Each PGP user maintains a list of public keys, called a keyring. Keyrings can be exchanged between users.

This option is not viable for C-ITS and will not be further analysed.

9 Evaluation of Trust model options

The following sections evaluate the trust model options (and the different implications of the trust model options to technical equipment such as the C-ITS station and the PKI) against high level requirements.

Aspects which are not trust-model-related are not considered, because out of the scope of this analysis (even if potentially relevant for implementations).

All the high level requirements are associated to positive metrics. In other words, a trust model option, which addresses most or all the high level requirements in a satisfactory way, will have an higher evaluation score than a trust model option which does not address the high level requirements. A score from 1 to 5 (5 maximum level) will be defined for each metric.

In the analysis, we use the word policy generically unless specifically defined. Its meaning is related to security policy or certificate policy as stated in sections 8.2 and 8.4.

In summary, Option 1 has a single security, certificate policy and single authority, Options 2.x have multiple authorities, one or multiple security policies but a single certificate policy and Options 3.x have multiple authorities, one or multiple security policies and multiple certificate policies but a single security goal.

The meaning of the score is defined according to the following table:

	Description
1	This is the lowest score. This indicates that the trust model option under analysis does not sufficiently support the requirement area or metric. For example, the implementation of this trust model would be so expensive to design and deploy, that this trust model would not be feasible from a practical point of view.
2	This score indicates that the trust model option under analysis only partially supports the requirement area or metric. For example, the implementation of the trust model is very expensive to design and deploy and its application in the C-ITS domain would be acceptable only if no other options are feasible.
3	This score indicates that the trust model option under analysis satisfies the requirement area or metric. For example, the implementation of the trust model has an average cost for design and deployment but no particular cost efficiency.
4	This score indicates that the trust model option under analysis satisfies the requirement area to a high degree and it makes this trust model option preferable to others. For example, the implementation of the trust model has limited costs for design and deployment.
5	This score indicates that the trust model option under analysis satisfies the requirement area to an optimum level. For example, the implementation of the trust model is very efficient from a cost point of view.

As written before, this section provides a qualitative analysis rather than a quantitative analysis based on the expertise of the C-ITS platform Working Group 5 Security participants. In some specific cases, supporting evidence from market and research literature is used.

9.1 Maintainability

This requirement only addresses technical maintainability of the C-ITS-Station regarding the change of Root CA certificates. The associated economic aspects due to poor maintainability are considered part of the requirement 9.13 related to the operational costs (OPEX).

Trust Model	Analysis	Score (1-5, 5 Maximum value)
Option 1	The Trust model supports easy maintenance of the C-ITS because only one Root CA certificate needs to be installed/updated in case of equipment replacement or update. Additionally the set CA certificates and CA contact information to be maintained in the C-ITS during operation is reduced.	4
Option 2a	The Trust model supports medium cumbersome maintenance of the C-ITS-S because only one Root CA certificate needs to be installed/updated in case of equipment replacement or update. Additionally the set of Root Cross-certificates, CA certificates and CA contact information to be maintained in the C-ITS during operation is extensive.	3
Option 2b	The Trust model requires a medium cumbersome maintenance of the C-ITS because only one Root CA certificates need to be installed/updated in case of equipment replacement or update. The set of Root Cross-certificates to be maintained is reduced due to the presence of the Bridge CA. Additionally the set of CA certificates and CA contact information to be maintained in the C-ITS is extensive.	3
Option 2c	The Trust model requires a medium/highly cumbersome maintenance of the C-ITS-S because all Root CA certificates need to be installed/updated in case of equipment replacement or update or also in case of addition of a new Root CA. Alternatively the CTL information can be used to install the Root CA certificates. Additionally also the set of CA certificates and CA contact information to be maintained in the C-ITS-S during operation is quite extensive.	3
Option 3a	Same as Option 2a	2
Option 3b	Same as Option 2b	2
Option 3c	Same as Option 2c	2

9.2 Scalability

Scalability is ability of a system, network, or process to handle a growing amount of work in a capable manner or C-ITS ability to be enlarged to accommodate that growth. For example, the growing amount of work can be the consequence of an increased number of stakeholders involved.

Here scalability is intended as the ability for the trust model to be able to cope with increasing numbers of stakeholders (not number of vehicles) in the C-ITS domain. In this context, scalability also includes political considerations: if there is a greater number of stakeholders or authorities, it is may be more difficult to define common policies. Scalability only analyses aspects related to the growing amount of work (interfaces, processes).

Trust Model	Analysis	Score (1-5, 5 Maximum value)
Option 1	Generally this option provides the best and simplest way to expand with the increasing number of stakeholders. On the other side, the agreement on this trust model and the definition of a single policy can be quite difficult and complex from an organizational and political point of view. The scalability of this Trust Model is dependent on the depth of the hierarchical structure under	4

	the root CA.	
Option 2a	The scalability of this trust model is average because of the need to establish cross-certification links among all the Root CAs in the federation. The number of required cross certifications is (n(n − 1)) where n is the number of Root CAs. In addition, because the policy is defined by the federation and any change to the policy must be agreed by all the Root CAs in the federation, the definition of the policy itself is not really scalable.	2
Option 2b	The scalability of this trust model is better than average because there is no need to have (n(n − 1)) cross-certifications as in 2a) and 2c) because the single Bridge CA will take care of the cross-certifications.	4
Option 2c	The scalability of this trust model is limited because the list of certificates must grow for the all the CA to be trusted. In addition, the C-ITS station must maintain the list of certificates in its memory.	4
Option 3a	Same as Option 2a	2
Option 3b	Same as Option 2b	4
Option 3c	Same as Option 2c	3

9.3 Crypto-Flexibility

Flexibility is meant as the capability of Trust model for C-ITS to support extensions of the cryptographic algorithms or features of the cryptographic design of C-ITS.

For example, today it is impossible to predict the key lengths that will be needed in X number of years. Vehicles may have a long lifetime (e.g., 10-20 years), which could be longer that the lifetime of the cryptographic algorithm, thus the need of crypto-flexibility requirement. For example, in the case of ETSI standards, ETSI TS 103 097 and TS 102 941 may be revised so to allow certificates with different key lengths and define clear long-term migration scenarios.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The Trust model support crypto flexibility according to the single policy and the standards it refers to (as implemented by the ITS-Stations). The same degree of crypto flexibility applies to signing, verification and migration operations.	2
Option 2a	The Trust model support crypto flexibility according to the common policy and the standards it refers to. The same degree of crypto flexibility applies to signing and verification operations.	2
Option 2b	As 2a	2
Option 2c	As 2a	2
Option 3a	The Trust model support crypto flexibility according to the policy framework and the standards it refers to. Each domain chooses C-ITS own level of crypto flexibility within the framework, but at least the verification operations implemented in the C-ITS shall fulfill the sum of all crypto flexibility requirements of those domains. As the CA´s are federated the take over of an algorithm as an alternative to the current one with a security breach could be easier, and therefore the best option.	3

Option 3b	As in Option 3a, but no alternative algorithm.	3
Option 3c	Each single domain has its own degree of crypto flexibility. Due to the need for of certificates of an C-ITS participating in different domains, at least the verification operations implemented in the C-ITS shall fulfill the sum of all crypto flexibility requirements of those domains	4

9.4 Trust Model flexibility

Trust model flexibility is understood as the possibility to add/update new PKI/CAs or to change the structure of the trust model due to organizational or technical changes in the context where the trust model is applied.

In engineering, maintainability is the ease with which a product can be maintained in order to:

- isolate defects or their cause,
- correct defects or their cause,
- repair or replace faulty or worn-out components without having to replace still working parts,
- prevent unexpected breakdowns,
- maximize a product's useful life,,
- make future maintenance easier, or
- cope with a changed environment.

This requirement is different from Crypto-Flexibility, which is related the support for different keys or cryptographic algorithms.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This Trust model is not flexible for the introduction of new organizations and the related PKIs or CAs as the new organization must trust the existing root CA and the existing defined policy. The addition of a new organization is not possible if this organization has already a PKI with cryptographic algorithms or a policy different from the existing root CA. The Trust model is also difficult to extend to new policies or algorithms because all the existing C-ITS stations must be re-configured. On the other side, the addition of a new intermediate CA to support a new entity (e.g. a new application or a new European member state) is easier than other options because of the presence of a root CA as trust anchor. For example, if a new intermediate CA is added for a new member state, a C-ITS vehicle (e.g., a car) does not need to download new certificates to interoperate with the fixed C-ITS in the new member state road infrastructure as the presence of the common root CA will guarantee the trust.	2
Option 2a	The trust model has a limited flexibility, because a new organization must be conform to the rules of the federation and the common policy. The acceptance of a new organization must be confirmed by all the parties of the federation. The trust model is also difficult to extend to new policies or algorithms if they are in conflict with the agreed federation rules.	3
Option 2b	The model has medium/high flexibility because a new organization need only to link to the bridge CA, which acts as an intermediary with the other	3

	existing PKIs. The new organization must accept the existing policy. This trust model is also relatively easy to extend to new policies as they can be implemented in the bridge CA even if existing C-ITS stations must be partially re-configured.	
Option 2c	The model has high flexibility because a new organization needs only to acquire a new Certificate Trust List. The new organization must accept the existing policy. This trust model is also relatively easy to extend to new policies but new Certificate Trust Lists must be distributed to all the C-ITS stations in the system.	3
Option 3a	The trust model has a medium flexibility, because a new organization must be conform to the rules of the federation and one of the federation policies. The acceptance of a new organization must be confirmed by all the parties of the federation. The trust model is difficult to extend to new policies or algorithms if they are in conflict with the agreed federation framework.	4
Option 3b	The trust model has a medium flexibility, because a new organization must be conform to the rules of the federation and one of the federation policies. In comparison to option 2a, it is slightly more flexible, because the acceptance of the new organization must only be confirmed by the policy authority rather than the federation of the existing organizations. The trust model is difficult to extend to new policies or algorithms if they are in conflict with the agreed rules and the policy of the common policy authority.	4
Option 3c	The model has high flexibility because a new organization needs only to acquire a new Certificate Trust List. The new organization can adopt one of the existing policies. This trust model is also relatively easy to extend to new policies but new Certificate Trust Lists must be distributed to all the C-ITS stations in the system.	4

9.5 Robustness

In this technical report, we use the term robustness as a combination of *reliability* and *resilience*, which are defined below.

Reliability is the ability of a system or component to function under stated conditions at and for a specified period of time, specifically under different and difficult conditions and for a long period of time. For example, reliability is understood as PKI reliability to provide C-ITS services to C-ITS stations.

In computer networking *resiliency* is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation. One of the elements of resilience is Disaster recovery (DR). DR involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Examples of disaster recovery are a) disclosure of private keys and b) technical unavailability or loss of private key.

Note that even in the case of a security failure, the C-ITS system should be still able to provide a minimum level of functionality: the normal driving functions should not be blocked.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This trust model has a limited robustness because the failure or compromise of the root CA will require the regeneration of certificates across the entire C-ITS	Reliability (3) Resilience (1)

	system. For example, compromise of the root CA private key is negative consequences for the security of its hierarchy and the availability of the C_ITS service.	= 2
Option 2a	This trust model has a better robustness than option 1 because the failure of a single root CA of the set of federated CAs has a more limited impact on the C-ITS system than a root CA: only the ITS station belonging to the affected Root CA cannot be trusted by all other ITS stations. There may be still an impact because the CAs are cross-certified but this can be handled in the validation of the chain. The ITS station belonging to the affected Root CA cannot be trusted by all other ITS stations.	Reliability (4), Resilience (4) =4
Option 2b	The trust model has a limited robustness because the bridge CA can be a single point of failure but it is slightly better than Option 1 because of the presence of many CAs. The failure or compromise of the bridge CA can generate a denial of service for cross-certifications on CAs but existing certificates could rely on the existing CAs.	Reliability (4), Resilience (2) =3
Option 2c	This trust model has a very high robustness because in case of compromise of a root CA, the C-ITS station could just be notified that a specific certificate is not valid (though a certificate revocation list).	Reliability (4), Resilience (4) =4
Option 3a	Same as Option 2a. An additional domain does not change the aspect of robustness.	Reliability (4), Resilience (4) =4
Option 3b	Same as Option 2b. An additional domain does not change the aspect of robustness.	Reliability (4), Resilience (2) =3
Option 3c	Same as Option 2c, but a higher risk that the distribution of the revocation list is performed differently in the domains	Reliability (4), Resilience (4) =4

9.6 Simplicity (Antonym to Complexity)

Complexity is generally used to characterize something with many parts where those parts interact with each other in multiple ways. The complexity of the Trust model in C-ITS can have a negative effect as a complex systems may be more expensive to build and maintain and can be less resilient. While complexity of the trust model design could be just a reflection of the organization and technical complexity of the context where C-ITS must operate, un-needed complexity should be minimized. In other words, the Trust Model should strive for simplicity.

Two requirements/metrics are defined: organization simplicity and technical simplicity.

9.6.1 Organizational simplicity

Organization simplicity is related to the set of organizational structures and processes, which must be put in place to support the trust model. In terms of organisational complexity we need to include at least the basic domains known in the C-ITS sector, which are vehicle, roadside and personal ITS stations, but also geographically existing market areas as the three regions Europe, with the member states, Usa and Asia.

9.6.2 Technical simplicity

Technical simplicity is related to the simplicity of the design, manufacturing, deployment and testing of the technologies and technological systems and devices which must be put in place to support the trust model.

Note: The scores are represented as an average of organizational simplicity and technical simplicity

Trust Model	Analysis	Score (1-5, 5 Maximum value)
Option 1	This trust model is relatively simple both from the organizations and technical point of view and hierarchical trust models based on a root CA are well known and deployed. Nevertheless the organizational complexity to establish this root CA in Europe could be high.	organizational simplicity (4) technical simplicity (4) Average = 4
Option 2a	This trust model is more complex than option 1 because there is need to establish a federation of the organizations responsible for the CAs/PKI to define a common certificate policy. This requires the definition of specific organization processes and structures. In addition, cross-certification requires the definition of mutual trust relationships between the pair of CAs.	organizational simplicity (2) technical simplicity (2) Average = 2
Option 2b	This trust model is slightly simpler than Option 2a and 2b because a central bridge CA is used to support the cross-certification of the CAs/PKIs. On the other side, the complexity of overall cross-certification system is moved to the design and implementation of the bridge CA, which can be complex from the technical point of view.	organizational simplicity (4) technical simplicity (2) Average = 3
Option 2c	This trust model is relatively simple to deploy because it just requires the distribution of the trust certificate list in the C-ITS stations in the C-ITS environment. The maintenance of the trust certificate list may be more complex to support but this is addressed in other requirements area. If the domain specific policies are well defined and accepted for all domains.	organizational simplicity (4) technical simplicity (4) Average = 4
Option 3a	The trust model is more complex than 2a because we need to support a multi domain context with different certificate policies.	organizational simplicity (1) technical simplicity (1) Average = 1
Option 3b	The trust model is more complex than 2b because we need to support a multi domain context with different certificate policies.	organizational simplicity (3) technical simplicity (1) Average = 2
Option 3c	The trust model is more complex than 3b because we need to support a multi domain context with different certificate policies. This can make the implementation of the certificate list very complex from the technical point of view. For example, it must support different cryptographic algorithms,	organizational simplicity (1) technical simplicity (1) Average = 1

9.7 Support for life cycle

9.7.1 System Lifecycle

The system lifecycle in systems engineering is an examination of a system or proposed system that addresses all phases of C-ITS existence to include system conception, design and development, production and/or construction, distribution, operation, maintenance and support, retirement, phase-out and disposal. The design of the trust model should support all the phases of the life cycle. The C-ITS-Station Security Lifecycle includes the following stages according to [25]:

- manufacture;
- enrolment;

- authorization;
- Maintenance

Which can be complemented by the stages identified in section 5.3.

NOTE: In the table below the system in focus is the C-ITS-Station

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The trust model support all lifecycle stages, under one single Root CA. But there is the risk that this stakeholder would not phase out, eliminating the own organization.	5
Option 2a	The trust model support all lifecycle stages, no matter under which root CA the stage is in. A mixture is possible, i.e. manufacture and maintenance under one Root CA, enrollment under another, authorization under yet another. Only the certificate chains are longer (cross-certificate = 1 additional certificate).	4
Option 2b	Same as option 2a	4
Option 2c	The trust model has the following life cycle restrictions: the C-ITS-Station is manufactured as belonging to one home PKI. It cannot (re-) enroll in a different PKI. It only can get authorization in the same PKI as it is enrolled to. Maintenance can change the home PKI	3
Option 3a	The trust model has the following life cycle restrictions: the C-ITS-Station is manufactured as belonging to one home PKI. It cannot (re-) enroll in a different PKI. It only can get authorization in the same PKI as it is enrolled to. Maintenance can change the home PKI only if the C-ITS-S supports all policies within the framework.	2
Option 3b	The trust model has the following life cycle restrictions: the C-ITS-Station is manufactured as belonging to one PKI. It cannot (re-)enroll in a different PKIs. It only can get authorization in the same PKI as it is enrolled to. Maintenance can change the home PKI only if the C-ITS-S supports all possible policies.	2
Option 3c	Same as option 3a	2

9.7.2 Certificate Lifecycle

Certificate lifecycle is understood as the crucial process that handles the renewal of CA and end-entity certificates, including key backup and recovery. This has implications on the maintenance of the C-ITS-Station.

The trust model options have different support for the certificate lifecycle:

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This trust module supports the certificate lifecycle in a simple way, because the certificates are all based on a root CA. The renewal of certificates is simpler because all the certificates are based on the same root CA and the same policy.	5
Option 2a	This trust module support the certificate lifecycle in a slightly more complex way than the Option 1 because of the presence of many different CAs, which are cross-certified. The renewal of a specific CA can be complex depending on	3

	the cross-certification paths defined in the C-ITS domain. Because in this trust model the definition of the policy is based on a federation, the definition of organization processes for key backup and recovery could be more complex to define and maintain.	
Option 2b	Same as option 2a as the bridge CA does not impact significantly the complexity of the support for certificate lifecycle.	3
Option 2c	Trust certification list can be more complex to manage in the certificate lifecycle depending on the length of the trust list and the involved CAs. The Trust list could be complex to manage and maintain in case of change of the trust model.	4
Option 3a	Same as option 2a but more complex because different policies must be supported.	2
Option 3b	Same as option 2b but more complex because different policies must be supported.	2
Option 3c	Same as option 2b but more complex because different policies must be supported.	2

9.8 Liabilities, contractual aspects

Liability is understood as the responsibility for the issuing of public key certificates to authorized parties and the implications of that at application level. For example, each Root CA is liable for C-ITS certificates issued by the EAs and AA it has provided CA certificates to. In case of cross-certification, the cross-certifying CA is not liable for the cross-certified CA.

In another example, the operator of the C-ITS-S is responsible for the secure installation and storage of the Root CA certificate, and private keys of the C-ITS-S.

Liability is assumed to be expressed through Certificate Practices Statements and Relying Party Agreements. Relying Party Agreements can be valid between the CA and the Service Provider (i.e. the OEM that sells the service to the end-user) or between the CA and the end-user. In this context, the policy should define a possible harmonization for liability issues among the parties/stakeholders involved in the domain.

Note that the certificate practice statement and relying party agreement puts an upper limit to the liability of some or all of the responsibilities of a party. Good practice would be that the liabilities must be less significant than the assets (money, insurance or other) of the party.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	Liability aspects are regulated by the policy authority that acts in the interest of the community. The CA can be made liable in case key material and/or services have been compromised. The best situation is when the single root CA is operated by an independent public authority.	5
Option 2a	Liability aspects are regulated by the federation that acts in C-ITS own interest but has strong links with all C-ITS stakeholders. The CA can be made liable in case key material and/or services have been compromised. The score is given assuming a single policy authority, external to the federation.	4
Option 2b	Same as option 2a	4
Option 2c	Liability aspects are regulated by the policy authority that acts in the interest of the community. The CA can be made liable in case key material and/or services	4

	have been compromised.	
Option 3a	Liability aspects are regulated by the federation that acts in C-ITS own interest but has strong links with all C-ITS stakeholders. The CA can be made liable in case key material and/or services have been compromised.	3
Option 3b	Liability aspects are defined by the operators of the single bridge CA in their own interest. Liability of CAs may be limited, with consequence to the Service Provider or end-user due to service interruption, failure and needed maintenance.	1
Option 3c	Liability aspects are defined by the operators of the trust certificate list in their own interest. Liability of CAs may be limited, with consequence to the Service Provider or end-user due to service interruption, failure and needed maintenance.	1

9.9 Support for revocation

Revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing. The word revocation here shall not directly imply the use of technical means such as a certificate revocation list, but can be achieved either by:

- active recall i.e. using a CRL
- on demand recall i.e. providing the certificate status on request of another entity , or
- passive annulment due to expiry.

In this context, the revocation is related to all the potential parties in the trust model for C-ITS. For example, the revocation could involve a CA (EA or AA, in case of a disaster), a single certificate issued to a C-ITS-Station or, a whole C-ITS station (in case of misbehaviour or compromise).

For example, authorization to send C-ITS messages should be revoked in case of misuse (misuse is to be defined) in a reasonable time.

The usage of CRLs has the drawback that they might grow over time, becoming difficult to manage. As an alternative, on demand recall protocols like OSCP can also be used to check the status of the certificates online. OSCP uses less bandwidth than CRL retrieval and it needs less processing capabilities in the client.

The table below focuses on active recall of CA or C-ITS-S certificates to ITS-S using a CRL.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The Trust model supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA	5
Option 2a	The Trust model supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA, as long as the Root CA of the AA and the C-ITS-Station is the same or are cross-certified.	3
Option 2b	The Trust model supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA. The Bridge CA could compile one complete CRL based on the single CRLs of all AAs.	3
Option 2c	The Trust model supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA, but the number of issued CRLs could be high	3
Option 3a	The Trust model supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA, as long as the Root CAs are cross-certified.	1

Option 3b	The Trust model does not supports active revocation of C-ITS-S certificates to other C-ITS-S by the issuing AA, because there is no joint policy that regulates revocation	1
Option 3c	The Trust model does not support active revocation of C-ITS-S certificates to other C-ITS-S that belong to a different Root CA, because there is no trust establishment between the Root CAs.	2

9.10 Misbehaviour detection and countermeasures

Misbehaviour detection is the requirement to detect and potential identify misbehaviours in the system and adopt specific countermeasures. For example, the implementation of the trust model can support detection of misbehaviours by analysing logs of the certificate exchanges.

For this metrics, the misbehavior detection and countermeasures refers to the ITS Stations. For example, a system based on local detection of potential misbehavior and generation of reports by C-ITS stations and reported to a central function.

Misbehaviour detection is a system based on a Misbehavior Authority (MA) that acts as the central function to process misbehavior reports and produces and publishes the certificate revocation list.

Note that in this metric, we do not address the complexity of the implementation of algorithms/systems for misbehaviour detection in C-ITS. Instead, the trust options are evaluated with regards to their support of misbehaviour detection algorithms/systems.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The Trust model supports misbehavior detection through one central misbehavior authority for example operated by the same authority that operates the Root CA.	5
Option 2a	The Trust model supports misbehavior detection through one central misbehavior authority operated by the federation for all participating Root CAs/PKIs. This MA would collect revocation reports from all C-ITS-Stations and provide the revocation information to the responsible EAs and AAs.	4
Option 2b	The Trust model supports misbehavior detection through one central misbehavior authority operated by the Bridge CA for all participating Root CAs/PKIs. This MA would collect revocation reports from all C-ITS-Stations and provide the revocation information to the responsible EAs and AAs.	4
Option 2c	The Trust model supports misbehavior detection only separately through one misbehavior authority per Root CA/PKI; C-ITS-Stations can only report to their respective MA and receive revocation information from that MA. The various MA must exchange revocation information about vehicles within their respective PKIs.	4
Option 3a	Same as Option 2a, but the score is lower because misbehavior can be differently defined and classified in the various policies.	3
Option 3b	Same as Option 2b, but the score is lower because misbehavior can be differently defined and classified in the various policies.	3
Option 3c	Same as Option 2c, but the score is lower because misbehavior can be differently defined and classified in the various policies.	3

9.11 Robustness against lack of harmonized standards

This requirement area/metric specifies the robustness against lack of harmonization in standards or the lack of adoption of those standards by CAs. Here, we mean the standards for the interface and protocols between ITS station and certification authority.

Lack of harmonisation of standards is interpreted as the fact that single PKI and their CAs may have proprietary interfaces towards the C-ITS-Station, which prevents C-ITS-S to change C-ITS "home" PKI during C-ITS lifecycle and which prevents delivering generic C-ITS stations. An interface is constituted by a set of communication protocols (protocol stack) and application messages. Different communication protocols do not constitute a major obstacle and each manufacturer of C-ITS-Stations might want to have a degree of freedom: the communication protocol(s) used may depend on options supported by the manufacturer such as update at workshop via portable medium, remote update via cellular link, local update using Wifi or G5.

Note that this requirement/area does not judge the business / commercial aspects.

On the other hand, the use of not harmonized application messages may constitute a major burden for security applications on C-ITS-Station side. Therefore the trust model options are evaluated as follows:

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The Trust model is robust against the lack of harmonized standards because the policy authority can mandate one single interface to the EA and AA	5
Option 2a	The Trust model is robust against the lack of harmonized standards because the federation can mandate one single interface to the EA and AA (provided that there is agreement among the parties of the domain.	4
Option 2b	Same as Option 2a	4
Option 2c	The Trust model is robust against the lack of harmonized standards because the policy authority can mandate one single interface to the EA and AA	5
Option 3a	Same as Option 2a, but lower score, because policies can still be different.	2
Option 3b	Same as Option 2a, but lower score, because policies can still be different.	2
Option 3c	The Trust model is not robust against the lack of harmonized standards because each Root CA can freely decide its standard, therefore you will not prevent it.	1

9.12 Cost efficiency for investment costs-(CAPEX)

This requirement is related to the cost efficiency for the initial costs (CAPEX) for the design, development and deployment of the PKI and the related security framework including the security elements in the C-ITS station. It is desirable that the initial investment costs are minimized, but some trust model options could be more expensive than others.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This trust model is the most simple to the design and deploy even if it require the definition of the single root CA, which still requires a significant initial investment. As a consequence, the initial design and deployment costs are also	4

	limited.	
Option 2a	This trust model would require the setting up and configuration of the cross-certification protocols among the root CAs. In addition, the organizational processes and structure for the definition of the federation must be created. On the other side of the coin, the trust model can be created from the evolution/adaption of existing PKIs.	3
Option 2b	The analysis of this trust model is similar to Option 2a and Option 2b with the additional consideration that the Bridge CA must also be created.	2
Option 2c	This trust model has the lowest costs because it just requires the definition of Trust Certificate Lists and their distribution to the C-ITS stations rather than the implementation CAs systems.	4
Option 3a	The analysis of this trust model is similar to option 2a, with the additional consideration that it must support different policies, which can increases considerable the initial design and deployment cost.	2
Option 3b	The analysis of this trust model is similar to option 2b, with the additional consideration that it must support different policies, which can increases considerable the initial design and deployment cost.	1
Option 3c	The analysis of this trust model is similar to option 2c, with the additional consideration that it must support different policies, which can increases considerable the initial design and deployment cost.	3

9.13 Cost efficiency for Running costs (OPEX)

This requirement is related to the cost efficiency of the running costs (OPEX) for maintenance/upgrade of the PKI and the related security framework including the security elements in the C-ITS stations.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	The running costs of this trust model are limited to the maintenance of the CAs, especially the root CA, but administrative costs must also be taken in consideration.	4
Option 2a	The running costs of this trust model are higher than Option 1 because of the presence of different CAs/PKIs. In addition, there are organizational costs related to the support for the federation.	2
Option 2b	The running costs are higher than Option 1 and Option 2 because of the need to maintain the bridge CA.	3
Option 2c	The running costs are quite limited because the trust model is based on the CTL installed in the C-ITS stations	4
Option 3a	The analysis of this trust model is similar to option 2a, with the additional consideration that it must support different policies, which can increases considerable the running costs.	2
Option 3b	The analysis of this trust model is similar to option 2b, with the additional consideration that it must support different policies, which can increases considerable the running costs.	2
Option 3c	The analysis of this trust model is similar to option 2c, with the additional consideration that it must support different policies, which can increases considerable the running costs.	3

9.14 Performance efficiency

This requirement is used to evaluate a trust model option on the basis of the time performance in the field for the V2V and V2I certificate generation and checking/validation. For example, the time requested to exchange and process certificates among C-ITS stations in the operative environment (e.g., cars driving in the road).

Note, that we consider only the performance efficiency for C-ITS stations for regulator communication and operational conditions, not covering how quickly you can recover in special circumstances.

In general, in case the certificate is not known, the communication involves an extra request to the peer broadcasting C-ITS-S to provide that certificate, and additional traffic and real-time evaluation.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This trust model has the higher efficiency because the certificate chain is based on the single root CA.	4
Option 2a	This trust model is less efficient of option 1 because of the presence of various cross-certificate CAs, which can increase the complexity and length of the certificate chains.	3
Option 2b	This trust model is less efficient of option 1 because of the presence of various cross-certificate CAs, which can increase the complexity and length of the certificate chains, even in the presence of the bridge CA.	3
Option 2c	This trust model has the higher efficiency because the certificate chain is based on the single root CA installed in the ITS-S.	4
Option 3a	The performance efficiency for this trust model is limited because of the presence of various cross-certificate CAs and different policies	2
Option 3b	The performance efficiency for this trust model is limited because of the presence of various cross-certificate CAs and different policies	2
Option 3c	The performance efficiency for this trust model is limited because of the different policies	2

9.15 Storage minimization

This requirement is used to evaluate a trust model option on the basis of the memory storage needed in the C-ITS equipment, for example in the C-ITS station. For example, certificates with longer trust chains may require more space in the memory of the C-ITS station in comparison to other trust model options.

Note that the certificates all type of certificates. At least for the planned CAMP/C2C-CC PKIs the main storage requirements will probably be the number of pseudonyms concurrently stored in the ECU and not only the overhead for CA certificates.

Trust Model	**Analysis**	**Score** (1-5, 5 Maximum value)
Option 1	This trust model minimizes the storage of the certificates in the ITS station in comparison to other trust models because the certificates are based on the root CA.	4
Option 2a	Memory storage in the ITS station is higher than option 1 because the certifications must support the different CAs.	3
Option	Memory storage in the ITS station is higher than option 1 because the	3

2b	certifications must support the different CAs.	
Option 2c	In comparison to the other trust model options, this trust model has the higher need for the storage of certificates in the ITS station because the certificates must support the different trust anchors in the C-ITS system.	3
Option 3a	The memory storage needs in the ITS station are higher than option 2a because the C-ITS system must support different set of policies.	2
Option 3b	The memory storage needs in the ITS station are higher than option 2c because the C-ITS system must support different set of policies.	2
Option 3c	The memory storage needs in the ITS station are higher than option 2d because the C-ITS system must support different set of policies.	1

9.16 Summary of the analysis

In this section, we summarize with the following tables the evaluation of the different options for the trust model for the non weighted and the weighted case.

We present four different weighing models based on different points of views:

1. The point of view of the member states.
2. The point of view of the vehicles manufacturers (OEM)
3. The point of view of the telematics manufacturers (Tier 1)
4. The joint view of one Member State with Industry

The non weighted table is provided below:

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
	Single Root CA	Federation cross certified root CA in one domain	Bridge CA in the same domain	Certificate Trust List/independent CA in same domain	Federation of root CAs in multiple domains	Bridge CA multi domains	Certificate trust list/independent CAs in multi domains
Maintainability	4	3	3	3	2	2	2
Scalability	4	2	4	4	2	4	3
Crypto-flexibility	2	2	2	2	3	3	4
Trust model flexibility	2	3	3	3	4	4	4
Robustness	2	4	3	4	4	3	4
Organisational complexity	4	2	4	4	1	3	1
Technical complexity	4	2	2	4	1	1	1
Support for life-cycle	5	4	4	3	2	2	2
Certification life-cycle	5	3	3	4	2	2	2
Liablities & contractual aspects	5	4	4	4	3	1	1
Support for Revocation	5	3	3	3	1	1	2
Misbehaviour detection and countermeasures	5	4	4	3	3	3	3
Robustness against lack of harmonised standards	5	4	4	5	2	2	1
CAPEX	4	3	2	4	2	1	3
OPEX	4	2	3	4	2	2	3
Performance efficiency	4	3	3	4	2	2	2
Storage minimisation	4	3	3	3	2	2	1

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**68**	**51**	**54**	**61**	**38**	**38**	**39**

Figure 10 Non weighted summary table of the scores for each option

The weighted table for telematics manufacturers is provided below:

	Weight	Option 1 Single Root CA	Option 2a Federation cross certified root CA in one domain	Option 2b Bridge CA in the same domain	Option 2c Certificate Trust List/independent CA in same domain	Option 3a Federation of root CAs in multiple domains	Option 3b Bridge CA multi domains	Option 3c Certificate trust list/independent CAs in multi domains
Maintainability	0.1	0.4	0.3	0.3	0.3	0.2	0.2	0.2
Scalability	1	4	2	4	4	2	4	3
Crypto-flexibility	0.1	0.2	0.2	0.2	0.2	0.3	0.3	0.4
Trust model flexibility	0.1	0.2	0.3	0.3	0.3	0.4	0.4	0.4
Robustness	1	2	4	3	4	4	3	4
Organisational complexity	0.1	0.4	0.2	0.4	0.4	0.1	0.3	0.1
Technical complexity	1	4	2	2	4	1	1	1
Support for life-cycle	0.1	0.5	0.4	0.4	0.3	0.2	0.2	0.2
Certification life-cycle	0.1	0.5	0.3	0.3	0.4	0.2	0.2	0.2
Liabilities & contractual aspects	0.1	0.5	0.4	0.4	0.4	0.3	0.1	0.1
Support for Revocation	0.1	0.5	0.3	0.3	0.3	0.1	0.1	0.2
Misbehaviour detection	0.1	0.5	0.4	0.4	0.3	0.3	0.3	0.3
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	0.2	0.2	0.1
CAPEX	1	4	3	2	4	2	1	3
OPEX	1	4	2	3	4	2	2	3
Performance efficiency	0.1	0.4	0.3	0.3	0.4	0.2	0.2	0.2
Storage minimisation	0.1	0.4	0.3	0.3	0.3	0.2	0.2	0.1

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**23**	**16.8**	**18**	**24.1**	**13.7**	**13.7**	**16.5**

Figure 11 Weighted table for telematics manufacturers

The weighted table for vehicles manufacturers (OEM) is provided below:

	Weight	Option 1 Single Root CA	Option 2a Federation cross certified root CA in one domain	Option 2b Bridge CA in the same domain	Option 2c Certificate Trust List/independent CA in same domain	Option 3a Federation of root CAs in multiple domains	Option 3b Bridge CA multi domains	Option 3c Certificate trust list/independent CAs in multi domains
Maintainability	0.5	2	1.5	1.5	1.5	1	1	1
Scalability	1	4	2	4	4	2	4	3
Crypto-flexibility	0.1	0.2	0.2	0.2	0.2	0.3	0.3	0.4
Trust model flexibility	0.3	0.6	0.9	0.9	0.9	1.2	1.2	1.2
Robustness	0.8	1.6	3.2	2.4	3.2	3.2	2.4	3.2
Organisational complexity	0.5	2	1	2	2	0.5	1.5	0.5
Technical complexity	0.5	2	1	1	2	0.5	0.5	0.5
Support for life-cycle	0.4	2	1.6	1.6	1.2	0.8	0.8	0.8
Certification life-cycle	0.6	3	1.8	1.8	2.4	1.2	1.2	1.2
Liabilities & contractual aspects	0.1	0.5	0.4	0.4	0.4	0.3	0.1	0.1
Support for Revocation	0.1	0.5	0.3	0.3	0.3	0.1	0.1	0.2
Misbehaviour detection and countermeasures	0.1	0.5	0.4	0.4	0.3	0.3	0.3	0.3
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	0.2	0.2	0.1
CAPEX	0.5	2	1.5	1	2	1	0.5	1.5
OPEX	1	4	2	3	4	2	2	3
Performance efficiency	0.7	2.8	2.1	2.1	2.8	1.4	1.4	1.4
Storage minimisation	0.3	1.2	0.9	0.9	0.9	0.6	0.6	0.3

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**29.4**	**21.2**	**23.9**	**28.6**	**16.6**	**18.1**	**18.7**

Figure 12 Weighted table for vehicle manufacturers

The weighted table for member states are provided below. Three weighted tables from two different member states are provided.

	Weight	Option 1 Single Root CA	Option 2a Federation cross certified root CA in one domain	Option 2b Bridge CA in the same domain	Option 2c Certificate Trust List/independent CA in same domain	Option 3a Federation of root CAs in multiple domains	Option 3b Bridge CA multi domains	Option 3c Certificate trust list/independent CAs in multi domains
Maintainability	0.5	2	1.5	1.5	1.5	1	1	1
Scalability	0.8	3.2	1.6	3.2	3.2	1.6	3.2	2.4
Crypto-flexibility	1	2	2	2	2	3	3	4
Trust model flexibility	1	2	3	3	3	4	4	4
Robustness	1	2	4	3	4	4	3	4
Organisational complexity	0.4	1.6	0.8	1.6	1.6	0.4	1.2	0.4
Technical complexity	0.4	1.6	0.8	0.8	1.6	0.4	0.4	0.4
Support for life-cycle	0.1	0.5	0.4	0.4	0.3	0.2	0.2	0.2
Certification life-cycle	0.4	2	1.2	1.2	1.6	0.8	0.8	0.8
Liabilities & contractual aspects	0.1	0.5	0.4	0.4	0.4	0.3	0.1	0.1
Support for Revocation	0.4	2	1.2	1.2	1.2	0.4	0.4	0.8
Misbehavior detection and countermeasures	0	0	0	0	0	0	0	0
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	0.2	0.2	0.1
CAPEX	1	4	3	2	4	2	1	3
OPEX	1	4	2	3	4	2	2	3
Performance efficiency	0.4	1.6	1.2	1.2	1.6	0.8	0.8	0.8
Storage minimisation	0.2	0.8	0.6	0.6	0.6	0.4	0.4	0.2

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**30.3**	**24.1**	**25.5**	**31.1**	**21.5**	**21.7**	**25.2**

Figure 13 Weighted table for Member State 1

	Weight	Option 1 Single Root CA	Option 2a Federation cross certified root CA in one domain	Option 2b Bridge CA in the same domain	Option 2c Certificate Trust List/independent CA in same domain	Option 3a Federation of root CAs in multiple domains	Option 3b Bridge CA multi domains	Option 3c Certificate trust list/independent CAs in multi domains
Maintainability	0.1	0.4	0.3	0.3	0.3	0.2	0.2	0.2
Scalability	1	4	2	4	4	2	4	3
Crypto-flexibility	1	2	2	2	2	3	3	4
Trust model flexibility	0.4	0.8	1.2	1.2	1.2	1.6	1.6	1.6
Robustness	0.8	1.6	3.2	2.4	3.2	3.2	2.4	3.2
Organisational complexity	0.8	3.2	1.6	3.2	3.2	0.8	2.4	0.8
Technical complexity	0.8	3.2	1.6	1.6	3.2	0.8	0.8	0.8
Support for life-cycle	0.4	2	1.6	1.6	1.2	0.8	0.8	0.8
Certification life-cycle	0.4	2	1.2	1.2	1.6	0.8	0.8	0.8
Liablities & contractual aspects	0.6	3	2.4	2.4	2.4	1.8	0.6	0.6
Support for Revocation	0.1	0.5	0.3	0.3	0.3	0.1	0.1	0.2
Misbehaviour detection and countermeasures	0.1	0.5	0.4	0.4	0.3	0.3	0.3	0.3
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	0.2	0.2	0.1
CAPEX	0.1	0.4	0.3	0.2	0.4	0.2	0.1	0.3
OPEX	0.8	3.2	1.6	2.4	3.2	1.6	1.6	2.4
Performance efficiency	0.4	1.6	1.2	1.2	1.6	0.8	0.8	0.8
Storage minimisation	0.4	1.6	1.2	1.2	1.2	0.8	0.8	0.4

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**30.5**	**22.5**	**26**	**29.8**	**19**	**20.5**	**20.3**

Figure 14 Weighted table for Member State 2

	Weight	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
		Single Root CA	Federation cross certified root CA in one domain	Bridge CA in the same domain	Certificate Trust List/independent CA in same domain	Federation of root CAs in multiple domains	Bridge CA multi domains	Certificate trust list/independent CAs in multi domains
Maintainability	0.1	0.4	0.3	0.3	0.3	0.2	0.2	0.2
Scalability	1	4	2	4	4	2	4	3
Crypto-flexibility	1	0.2	0.2	0.2	0.2	0.3	0.3	0.4
Trust model flexibility	0.4	0.2	0.3	0.3	0.3	0.4	0.4	0.4
Robustness	0.8	2	4	3	4	4	3	4
Organisational complexity	0.8	0.4	0.2	0.4	0.4	0.1	0.3	0.1
Technical complexity	0.8	4	2	2	4	1	1	1
Support for life-cycle	0.4	0.5	0.4	0.4	0.3	0.2	0.2	0.2
Certification life-cycle	0.4	0.5	0.3	0.3	0.4	0.2	0.2	0.2
Liablities & contractual aspects	0.6	0.5	0.4	0.4	0.4	0.3	0.1	0.1
Support for Revocation	0.1	0.5	0.3	0.3	0.3	0.1	0.1	0.2
Misbehaviour detection and countermeasures	0.1	0.5	0.4	0.4	0.3	0.3	0.3	0.3
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	0.2	0.2	0.1
CAPEX	0.1	4	3	2	4	2	1	3
OPEX	0.8	4	2	3	4	2	2	3
Performance efficiency	0.4	0.4	0.3	0.3	0.4	0.2	0.2	0.2
Storage minimisation	0.4	0.4	0.3	0.3	0.3	0.2	0.2	0.1

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**23.0**	**16.8**	**18.0**	**24.1**	**13.7**	**13.7**	**16.5**

Figure 15 Weighted table for Member State 3

	Weight	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
		Single Root CA	Federation cross certified root CA in one domain	Bridge CA in the same domain	Certificate Trust List/independent CA in same domain	Federation of root CAs in multiple domains	Bridge CA multi domains	Certificate trust list/independent CAs in multi domains
Maintainability	0.1	0.4	0.3	0.3	0.3	-	-	-
Scalability	1	4	2	4	4	-	-	-
Crypto-flexibility	1	2	2	2	2	-	-	-
Trust model flexibility	0.4	2	3	3	3	-	-	-
Robustness	0.8	2	4	3	4	-	-	-
Organisational complexity	0.8	1.6	0.8	1.6	1.6	-	-	-
Technical complexity	0.8	1.6	0.8	0.8	1.6	-	-	-
Support for life-cycle	0.4	2	1.6	1.6	1.2	-	-	-
Certification life-cycle	0.4	2	1.2	1.2	1.6	-	-	-
Liablities & contractual aspects	0.6	0.5	0.4	0.4	0.4	-	-	-
Support for Revocation	0.1	0.5	0.3	0.3	0.3	-	-	-
Misbehaviour detection and countermeasures	0.1	0.5	0.4	0.4	0.3	-	-	-
Robustness against lack of harmonised standards	0.1	0.5	0.4	0.4	0.5	-	-	-
CAPEX	0.1	0.4	0.3	0.2	0.4	-	-	-
OPEX	0.8	3.2	1.6	2.4	3.2	-	-	-
Performance efficiency	0.4	1.6	1.2	1.2	1.6	-	-	-
Storage minimisation	0.4	0.8	0.6	0.6	0.6	-	-	-

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
Score	**25.6**	**20.9**	**23.4**	**26.6**	**-**	**-**	**-**

Figure 16 Joint view of Member State 3 with Industry

	Option 1	Option 2a	Option 2b	Option 2c	Option 3a	Option 3b	Option 3c
	Single Root CA	Federation cross certified root CA in one domain	Bridge CA in the same domain	Certificate Trust List/independent CA in same domain	Federation of root CAs in multiple domains	Bridge CA multi domains	Certificate trust list/independent CAs in multi domains
Non-weighted WG5 consensus	68	51	54	**61**	38	38	**39**
Weighted Telematics Manufacturers	23	16.8	18	**24.1**	13.7	13.7	**16.5**
Weighted OEMs	29.4	21.2	23.9	**28.6**	16.6	18.1	**18.7**
Weighted Member State 1	30.3	24.1	25.5	**31.1**	21.5	21.7	**25.2**
Weighted Member State 2	30.5	22.5	26	**29.8**	19	**20.5**	20.3
Weighted Member State 3	23.0	16.8	18.0	**24.1**	13.7	13.7	**16.5**
Joint view of Member State 3 with Industry	25.6	20.9	23.4	**26.6**	-	-	-

Legend: underlined = lowest score among a,b,c of Options 2 and 3
bold = highest score among a,b,c of Options 2 and 3

Figure 17 Summary of scoring results

10 Conclusions of the analysis

Policy context

Article 91 of the Lisbon Treaty sets the framework for the EU common transport policy, which explicitly defines transport safety across the EU as a Union responsibility.

Road safety spans across borders and motorists using ITS to improve their road safety have the right to expect the same service levels: 1.) wherever these services are provided across the EU; 2.) whatever vehicle they are driving.

This counts in particular for C-ITS, which functions only, if vehicles of various manufacturers, as well as road infrastructure managed by various road administrations or operators, are able to reliably communicate and interoperate with one another in the C-ITS Network.

Directive 2010/40/EU further underpins Article 90 stipulating that ITS, where deployed, shall run seamless across borders, whilst protecting personal data and improving traffic safety. Traffic Safety relies on reliable and secure information, which in turn demands for a dedicated system that provides tools to establish trust between communication end-points. In other words, there is the need to define a trust model for C-ITS at European level. As described in this technical report, C-ITS standardization activities driven by the industry (see also release 1 of Standardisation Mandate 453 of the European Commission) and Connected Vehicles in USA have proposed public key cryptography to implement the trust model. This requires the setting up of a public key infrastructure (PKI) and related certificate and security policies by all involved stakeholders.

Different trust models exist as known from literature and operational systems. The different PKI trust model options discussed in this technical report of WG5 of the C-ITS Platform all serve to provide mechanisms to ensure data protection and security through authenticating the communication between vehicles, no matter the brand, and road network equipment's, no matter the country or operator, who is running it.

Translating EU policies into a trust model for C-ITS – key priorities

These trust models will need to operate within the wider context of the EU, meaning that a key task of the working group was to find the right balance between technical complexity, operational feasibility and cost efficiency. In addition, aspects related to political drivers and mutual trust were also taken in consideration. It has been an additional task of WG5 for the trust model definition to take into consideration the current early phase of C-ITS Introduction in Europe with a few stakeholders and industry players and the future extensions of additional service categories, member state coverage and inclusion of new service providers. The stakeholders in the Working Group from the EU Member States, the automotive sector, telematics manufacturers and independent experts broadly agree on three top priorities that a trust model for C-ITS has to follow to function:

- *Scalability – implementing subsidiarity and offering flexibility*

The deployment of C-ITS is expected to be driven by a wide set of stakeholders, which include the European Union, EU Member States and their road infrastructures, vehicle manufacturers (to introduce C-ITS telematics equipment into their vehicles), application developers, service providers, manufacturers of C-ITS roadside equipment and other stakeholders. It has to be considered that the potential number of C-ITS equipped vehicles can be in the order of millions and support different kinds of C-ITS applications. The system has to be able to integrate new actors into its framework and assure them the same high levels of

authentic and secure communication across all participating vehicle brands and infrastructures. Aspects of harmonization at global level should also be taken in account, considering the manufacturers operate in worldwide markets and different conformance testing or security designs could negatively impact them. Cross-border interoperability with bordering countries is another important aspect to be addressed. See also existing case studies like the Digital Tachograph applications where the AETR agreement has been put in place to address similar needs.

- *Robustness – offering authentic communication under all circumstances*

The communication services used in C-ITS (e.g., exchange of CAM or DENM) have to be reliable and the system has to be designed in a way to be resilient in the case of hacking or a malfunction of any kind. For example, the design of the system should support requirements for the integrity of the exchanged messages, the functional and physical integrity of the on-board components and the integrity of the information provided by the sensor. In addition, authentication is another important property, which should be supported. The authentication of the originator of messages or the service providers is needed to ensure that messages come from a trusted source. In the context investigated in this technical report, we believe that cybersecurity risks in road transportation (which have received increasing attention in recent times) can be addressed by a) the deployment of a comprehensive trust model and by b) defining compliance assessment processes and tests which include security and privacy aspects (e.g. , through the common criteria).

- *Costs related to design, implementation, deployment and operation of the trust model*

Cost efficiency is one of the metrics used in the analysis. The design, development, deployment and operational phases of the trust model have associated costs (both CAPEX and OPEX), which include not only the placement of C-ITS stations in the market but also their end-of-life, repair and upgrade. While these costs are necessary because lack of safety can have serious consequences in road transportation, cost efficiency is an important parameter to evaluate the different technical solutions.

These three factors, which all stakeholders gave the highest priority in addition to 14 other aspects, deemed of varying importance by the stakeholders have been taken into consideration to rank the different options for a possible C-ITS trust model for the EU.

Weighing the options

Of the options given the “Single Root CA” (Option 1), as well a “Certificate Trust List/Independent CA in the same domain (Option 2c)”, both obtained the two highest scores from members of WG5 for the initial setup and starting phase of C-ITS in Europe. The option 1 “Single Root CA” would require all stakeholders, i.e. EU Member States as well as vehicle manufacturers to operate their PKI under the single Root CA and agree on the rules and procedures for doing this together upfront. Although several experts have expressed concerns, that this agreement can be achieved in short time frames, this is not reflected in the overall ratings. In order to take this into account a reduced and strict time limit for reaching an agreement between main stakeholders can be a way to cope with this aspect in the setup phase of C-ITS. On the other side, this option requires a strong mutual trust among the various participating entities (e.g., member states) at organizational (or even security policy) level, which may be difficult to achieve in short time periods, especially in the large context of C-ITS where millions of vehicles are in the road.

Bearing this in mind, the option 2c “Certificate Trust List/Independent CA in the same domain” appears to best combine high levels of protection with the flexibility to integrate new actors within the day one common

single trust domain. A single certificate policy (and the related CPS and security policy) and an according policy authority assures seamless and EU wide provision of a harmonized trust framework. In addition, the definition of an uniform certificate policy can also provide tools for protecting personal data by changing pseudonyms for vehicle movement data regularly (e.g., as defined in the Car2Car architecture based on pseudonym certification authority). This is consistent with the Certificate Policy structure, where a Privacy plan must be defined. At the same time the certification authorities are free to implement key security controls, policy structure and administration amongst other aspects through the respective CPS.

From the other options rated by WG5 experts and their organisations the option 2a seems to be consistently the least attractive one for all stakeholders with a high difference of rating points to all other proposed solutions. This is the case for an early starting phase of C-ITS and the analysed options in one domain (the options defined with a 2 in the numbering scheme) as well as in the more mature phase of C-ITS network operation, (with implicitly multiple domains needed and a 3 in the numbering scheme), were also the option 3a has been rated consistently with the lowest points by far. For this reasons the option a is not analysed any further in this report.

For the overall ratings of the options b and c this difference in scores is not so high in favour of c, even if it is fully consistent for all stakeholders in the initial setup phase for C-ITS. The main aspect to be taken into account here is the number of initial participants and the speed with which new stakeholders want to implement C-ITS and therefore join the common security solution and trust model area.

This difference in ratings between the options b and c still exists in the mature phase of C-ITS network operations according to WG5 members, but has become less important which is reflected in the similarly high overall ratings, were for most single member states option c seems to be the preferred option. However, there are also scoring results that ranked option b the highest – this shows that a further specific analysis on the benefits and trade-offs of pursing either a certificate trust list based (c-option) or a bridge solution (b-option) in the multi domain case might still be needed.

Overall option 2c appears to be the best and most reasonable way to allow flexibility within the EU C-ITS domain for first phase (or day 1) of road safety and traffic management applications. The additional possibility of trust extensions (for interoperability) with other domains within the EU member states (e.g a specific domain for all road side ITS stations in the EU or their member states) or in other parts of the world or future applications needs consideration as well. Here the option 3c “Certificate Trust List/Independent CAs in multi-domains” appears to show the best way forward for most members of WG5, although the option 3b follows not far in the ratings especially from industry but also in the non-weighted initial scheme.

Regarding the adoption of option 3b or 3c to support multiple C-ITS applications (for Day 1 and also beyond for future developments) in different domains, it has to be noted that one Member State has already now clearly stated, during the analysis, that a common certificate policy and a single domain has been agreed for the C-ITS applications related to both implementations periods. A similar approach could be adopted by other Member States, with the advantage of simplifying the trust model at least for the applications dimension.

Aspects that have been taken into account in the evaluation between these options are the overall numbers of participants in each future separate domain of C-ITS and their composition at the starting point or their extensions with additional members on one side and the available options for all other domain members in the case of a security breach in one domain. Why not all consequences of this aspect have been analysed in detail, it is understood by WG5 experts that in the second case the option 3b would offer additional

possibilities to recover trust for C-ITS units faster than the option 3c for one domain and as a consequence also for the complete network.

These options have been selected for the so called *Day One* applications and for the European area. A combination of different options may be needed for the interaction of the European C-ITS trust model with other trust models for C-ITS in the rest of the world, because other geo-political areas (even bordering to Europe) may set up trust models with different security and certificate policies. In this case, the different domains (Europe and outside Europe) must interoperate with one of the trust model options discussed in this report (e.g., bridge).

An additional aspect that has been discussed in WG5 and is probably not completely taken into account in current ratings is cryptoagility, which on its own is a strong indicator for a future group 3 solution in the C-ITS area. As experts agree that most C-ITS units will have a life time of up to 20 years, depending on the area were they are used, and in parallel confirm the long term trend that there is a certain risk that the cryptographic algorithms initially adopted in the design phase may not be secure in the overall lifetime. As a consequence, it is of vital interest for all C-ITS stakeholders that different levels of security exist in parallel and that in such cases units can be migrated from one domain to another in an agreed and controlled process.

From this analysis of the elaborated options the following recommendations for setting up a security solution for C-ITS in Europe are presented in the next chapter.

11 Recommendations

The goal of this technical report was to conduct an analysis of the options for the trust model of C-ITS in Europe taking in consideration different metrics, the lifecycle of C-ITS stations and similar case studies in transport in Europe and in the world.

From the analysis, WG5 of the C-ITS Platform defines the following recommendations for a way forward on the concrete deployment of a security infrastructure based on PKI for C-ITS in Europe:

(1) The agreed objective is to **deploy one common C-ITS trust model all over Europe** that shall support full secure interoperability at the European level. Since the experts of WG5 recognise that this cannot sufficiently be provided by either a single EU Member State, nor by individual stakeholders (e.g. automobile manufacturers) a joint effort to develop EU-wide policy with clearly identified roles and methods is required as outlined in section 8.2. As described in this report, the EU-wide C-ITS trust model is the implementation of the trust model based on a Public Key Infrastructure (PKI) system with the associated policies, organizational structures and processes including the links to the C-ITS compliance assessment process for certain types of applications.

a) This trust model **shall be implemented in a single trust domain version (**e.g., one single cryptographic algorithm and certificate format) **for the start-up day one phase** of C-ITS.
b) **Beyond the Day 1 phase, C-ITS may be extended with multiple interoperable trust domains** if deemed necessary to take the variety of stakeholders (including the global dimension) and the responsibilities for private and public entities involved into account.

In order to deploy a common C-ITS trust model specific elements and steps are needed. According to the WG5 experts the following recommendations are therefore further defined:

(2) **Need for Legal Certainty:** The appropriate legislative framework (e.g. new EU delegated acts or the identification of the amendments to the existing EU regulatory framework) needs to be set in place **quickly**.

(3) In order to achieve legal certainty a careful **analysis and discussion with the relevant stakeholders** is needed. The list of relevant stakeholders identified by the WG5 experts includes (but it is not necessarily limited) to:
- Member States
  - Responsible National Security Agencies
  - Responsible National authorities, ministries or bodies
- Vehicle manufacturers
- Infrastructure operators
- Telematics manufacturers for vehicle, roadside infrastructure and nomadic devices.

(4) The **responsible policy bodies for the definition of the security policy, certificate policy and related implementation measures (e.g. certificate practice statement) have to be identified** – this should be done in parallel with setting up the appropriate legislative framework. An independent governance structure will be needed to coordinate the definition and subsequent implementation of the commonly agreed elements (e.g. certificate policy) for *Day One* C-ITS applications deployment.

This includes the definition of the entities responsible for the setting up and implementation of the components of the trust model.

(5) The **financing scheme** needs to be discussed to identify which parties will support or contribute to the financing scheme.

(6) Compliance with the identified legislative framework in (2) **will need to be reflected in the compliance assessment process** for vehicle and roadside C-ITS equipment.

(7) A **time plan for the design and deployment of the EU wide C-ITS trust model** with the most significant milestones (e.g. identification of the CAs or definition of the certificate policies) should be drafted. The experience from the EU C-ITS corridor deployment initiatives, standardisation activities and pilot projects should be taken in consideration in the drafting of the time plan. The timeplan should include at least the following milestones:

- Definition of the Certificate Policy, Certification Practice Statement and Security Policy
- Identification and design of the PKI
- Definition of the distribution channels for the certificates
- Definition of the compliance assessment process
- Definition of the financing scheme

Annex 1

A.1. Certificate Policy and Certification Practice Statement

This annex describes a template for a C-ITS Certificate policy (CP) on the basis of IETF RFC 7382. A corresponding Certification Practice Statement (CPS) should be defined by the implementing organisation. In particular, the CP appositely leaves some degree of freedom in defining the CPS, and define requirements to the content of the CPS (which are meta-requirements to the organisation).

The structure of the main elements of the CP and CPS are the same. In fact (from [51]): A CP sets forth the requirements and standards imposed by the PKI with respect to the various topics. In other words, the purpose of the CP is to establish what participants must do. A CPS, by contrast, states how a CA and other participants in a given domain implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the participants perform their functions and implement controls.

An additional difference between a CP and CPS relates to the scope of coverage of the two kinds of documents. Since a CP is a statement of requirements, it best serves as the vehicle for communicating minimum operating guidelines that must be met by interoperating PKIs. Thus, a CP generally applies to multiple CAs, multiple organizations, or multiple domains. By contrast, a CPS applies only to a single CA or single organization and is not generally a vehicle to facilitate interoperation.

A.2. Certificate Policy template for C-ITS

The following structure and elements are defined:

1. Introductions

In this chapter, the types of entities and applications of this certificate policy are defined.

1.1. Overview

A general introduction to the certificate policy document: this CP defines legal and technical requirements for the management of public key certificates for V2X applications by issuing entities and their usage by end-entities. This CP is binding for certification authorities and end-entities that own a certificate. It is a guidance document to recipients of signed messages and certificates about which level of trust can be established from verification of the certificates. This CP is not a contractual agreement between parties.

1.2. Document Name and Identification

Names and identifiers for this document are defined here. The name can for example be European C-ITS Certificate Policy and the identifiers would be ASN.1 object identifiers.

1.3. PKI Participants

Description of the organisations that are part of the Cooperative-ITS Security Credentials Management System: this CP is applicable to all organisations that supports security management according to ETSI TS 102 940. It supports the co-existence of multiple PKIs in parallel with the following participants:

2. Root Certification Authorities: the organisation that issues certificates to Intermediate and /or Issuing Certification Authorities. It is the top of the hierarchy of the PKI, and is independent from other Root Certification Authorities/PKIs in the Cooperative-ITS Security Credentials Management System.
3. Intermediate Certification Authorities: the organisation that issues certificates to Issuing Certification Authorities (optional)
4. Issuing Certification Authorities: the organisations that issue public key certificates to end-entities, i.e.
    - Enrolment Authorities issue Enrolment Certificates aka Enrolment Credentials
    - Authorization Authorities issue Authorization Certificates aka Authorization Tickets
5. Registration Authorities: If necessary, registration authorities support certificate authorities by validating identity claims of subscribers. A registration authority cannot issue a public key certificate by itself.
6. Subscribers: End entities (i.e. ITS-Stations) needing to authenticate themselves in the C-ITS system. End-entities have associated permissions that can be coded in the certificates.

1.4. Certificate Usage

Description of the usage of the certificates produced by the PKI:

7. Root Certificates are used to verify CA certificates when verifying a certificate chain.
8. Authorization Certificates are used to verify V2X signed messages.
9. Enrolment Certificates are used to verify certificate request messages by the Authorization Authorities.

Description of not intended usage, such as cases where law, regulations or rights are breached or damage to persons or objects can be created.

1.5. Policy Administration

Who is responsible for the administration and maintenance of this certificate policy itself (organisation, contact person, description of the approval procedure).

2. Publication and repository responsibilities

2.1. Repositories

Requirements regarding the structure of the repository for storing the certificates and what information is provided by Root Certification Authorities and Enrolment Authorities, e.g. an online certificate repository, a CRL, an OCSP service.

Requirements to Authorization Authorities are not defined (but can be defined in their CPS)

2.2. Publication of Certification Information

Requirements regarding the publication of public key certificates and CRLs by CAs.

For example: *Each CA MUST publish the certificates (intended for public consumption) that it issues via the repository system.*

2.3. Time or Frequency of Publication

Requirements regarding the publication schedule of certificates and CRLs.

For example: *The CPS for each CA MUST specify the period of time within which a certificate will be published after the CA issues the certificate.*

2.4. Access Controls on Repositories

Requirements on access control to repositories.

For example: *Each CA or repository operator MUST implement access controls to prevent unauthorized persons from adding, modifying, or deleting repository entries.*

3. Identification and Authentication

3.1. Naming

Requirement on management of CA names in certificate. Requirements for absence of naming in Authorization Certificates.

3.2. Initial identity validation

Authentication for initial registration, renewal, reissue and revocation of certificates. It also includes the identification and authentication of C-ITS entity (organizations or individual applicants/vehicles).

3.3. Identification and authentication for re-key requests

Not applicable

3.4. Identification and authentication for revocation request

Requirements to Identification and Authentication of an entity that requests revocation

An example for a naming requirement: *The distinguished name for every CA and end-entity consists of a single CommonName (CN) attribute with a value generated by the issuer of the certificate.*

4. Certificate Life Cycle Operational requirements

This includes all the operations related to certificate life-cycle as described below in detail.

4.1. Certificate Application: registration of issuing CA, application for end-entity certificates
4.2. Certificate Application Processing: description of the process for certificate application by issuing CA and end-entities.
4.3. Certificate Issuance: description of the process of issuing of certificate and notification of CA and end-entity
4.4. Certificate Acceptance: requirements for acceptance of Root CA certificate
4.5. Key Pair and Certificate Usage: covered in 1.4
4.6. Certificate Renewal: this is not applicable
4.7. Certificate Re-key: this is not applicable, a new certificate application is used, see 4.1
4.8. Certificate Modification: this is not applicable
4.9. Certificate Revocation and Suspension: the process and responsibilities for revocation of CA certificates and of end-entity certificates (if used).
4.10. Certificate Status Services: requirements to CAs for CRL publication and OCSP.

An example for an enrolment process requirement: *The enrolment process and procedures MUST be described by the CPS for each CA.*

5. Facility, Management, and Operational Controls

This includes all the operations and controls for the setting up and maintenance of the infrastructure implementing the PKI, which are not addressed in the following section 6.

- **5.1. Physical Controls; requirement to CA location, its features and its access**
- **5.2. Procedural Controls: requirements to roles, duties and identification of personnel**
- **5.3. Personnel Controls: requirements to qualification, training, experience and background of personnel**
- **5.4. Audit Logging Procedures: requirements to the types of events recorded and the management of audit logs**
- **5.5. Records Archival**
- **5.6. Key Changeover**
- **5.7. Compromise and Disaster Recovery. This is an important area to investigate and defined in C-ITS, because the compromise of cryptographic material can generate a massive recall.**
- **5.8. CA or RA Termination**

An example for a physical control: *Each CA MUST maintain physical security controls for its operation that are commensurate with those employed by the root CA. The physical controls employed for CA operation MUST be specified in its CPS.*

6. Technical Security Controls

This includes all controls for proper functioning of the technical systems.

6.1. Key Pair Generation and Installation

Requirements for key generation ceremony and hardware support for CAs with reference to known and accepted standards such as FIPS 140-2

Requirements for key generation ceremony and hardware support for end-entities, with reference to a published and accepted protection profile

Requirements for certificate requests with reference to ETSI ITS standards or IT standards.

Requirements on key sizes with reference to standards such as ETSI ITS standards.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Requirements to key protection for CAs with reference to known and accepted standards such as FIPS 140-2

Requirements to key protection for End-entities with reference to a published and accepted protection profile

Requirements to private key activation data protection.

Requirements to key back-up for CAs

Requirements to private key destruction

6.3. Archival

Definition of lifetimes of Certificates

6.4. Activation Data

Requirements to generation and protection of activation data for CA keys.

6.5. Computer Security Controls

Requirements to CA's computer systems in accordance with best practice standards

6.6. Life Cycle Technical Controls

Requirements to CA's software development, lice cycle security and security management.

6.7. Network Security Controls

Requirements to the CA's networks

6.8. Time-Stamping:

Requirements to timestamping of security objects.

An example for a key transfer requirement: *When a public key is transferred to the issuing CA to be certified, it MUST be delivered through a mechanism ensuring that the public key has not been altered during transit and that the subscriber possesses the private key corresponding to the transferred public key.*

7. Certificate and CRL Profile

Structure of the Certificate, including the definition of cryptographic algorithms with reference to ETSI ITS standards for the end-entity certificates. Structure of CRL and OCSP.

8. Compliance Audit and Other Assessments

Requirements on audits to be performed at the PKI organisations. Requirements on the auditor. Requirements on actions to be taken in case of deficiencies.

An example for a compliance requirement: *The CPS for each CA MUST describe what audits and other assessments are used.*

9. Other Business and Legal Matters

9.1. Fees

Definition of which entity is entitled to charge fees and for what (this is not a contractual agreement).

9.2. Financial Responsibility

Requirement to insurance coverage, which the organisations shall maintain to reasonably cover errors

9.3. Confidentiality of Business Information

Requirements on confidentiality of data assets managed by the PKI organisations

9.4. Privacy Plan

This is the plan on what are the requirements for the treatment of personal information and privacy.