Connecting Mobility

White paper on cybersecurity & privacy in connected and cooperative mobility

Krachten bundelen voor de mobiliteit van de toekomst

Colofon

For contacting connecting mobility please use the following details:

info@connectingmobility.nl
088 7982631
www.connectingmobility.nl

Connecting Mobility acts as a catalyst. It creates the necessary conditions and preconditions, with great attention to security, safety and human factors and associated legal issues and set direction in collaboration with governments, knowledge institutes and market, including by making smarter use of pre-competitive cooperation and attention for standardization. Connecting Mobility monitors developments.

Connecting Mobility provide overview, boost innovation in the field of ITS and smart mobility. The action program knows developments nationally and internationally, linking developments and ensure that the parties can find each other. In successful projects, the program allows for the national rollout.

Content

1 Introduction

1.1 Overview

The next generation of vehicles will be communicating with each other, with road-side systems, and will be continuously connected to various networks. Many services will be offered to the drivers via, both in car and via handheld devices like smart phones that will be seamlessly integrated into the vehicles' systems. In this whitepaper, we summarize the challenges and privacy & security work taking place in this area.

On November 27, 2014, in Utrecht (the Netherlands) a workshop on privacy & security in connected and cooperative mobility took place with a group of subject matter experts. During this workshop information from earlier international studies and other relevant documents were discussed and a selection of relevant topics on privacy & security was identified.
The topics identified in the workshop are:

- Secure development of system components
- A certification approach and scheme to create security levels depending on the nature of the components and functions
- PKI: the solution for secure communication
- The need for interoperability
- Personal data: Ownership, usage, the rights of the owner and user.

We highlight the complexity of the problems, communication technologies being used, and the security challenges we face together with some possible solutions. We will not only focus on the challenges, but also focus on suggestions for in-depth research and solutions to work on. After an introduction on the current situation and a view on the future situation, we give a short introduction to the subject, cooperative and connected mobility, and the necessity to focus on privacy and security. We follow up by addressing the aforementioned topics to provide a perspective of the recognised challenges, possible solutions, and define future research.

1.2 Scope

The scope of this white-paper is the security and reliability of connected and cooperative mobility, the interoperability between road infrastructure managers, the different brands, suppliers and systems, and the protection of personal information which is collected and used.

1.3 Definitions

This document uses the following definitions of the concepts listed hereunder. The Oxford English Dictionary and the NHTSA Readiness-of-V2V-Technology-for-Application are used as source to define these concepts.

Privacy:
The Oxford dictionary defines privacy as “*a state in which one is not observed or disturbed by other people*”

Security:
The Oxford dictionary defines security as “*the state of being free from danger or threat*”

V2V:
Vehicle-to-vehicle (V2V) communications, a system designed to transmit basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes.

V2I:
Vehicle to Infrastructure communication. The same wireless technology that supports V2V safety applications (5.9 GHz DSRC) will also enable a broader set of safety and mobility applications when combined with compatible roadway infrastructure; therefore V2V serves as the gateway for the broader intelligent transportation system program.

2 Connected and cooperative communication

2.1 Current situation

In the current situation, vehicles are driven from one location to another, without communication between other vehicles in its path. It is normal that a driver gets into his vehicle, starts the engine and then has full control over his vehicle. In the coming decade vehicles are getting more intelligent and vehicles shall communicate to other vehicles and to the roadside systems. Today’s car is able to assist the driver in maintaining the correct speed by means of Advanced Driver Assistance Systems (ADAS) such as adaptive cruise control with pre-crash assistance. Other relative new safety systems are brake assist and lane assist. All interesting safety systems to be built in a car, however the cart is still a single entity which is not connected to a vehicle infrastructure network environment.

Until now, software security is never included in vehicles. This was never really a problem. Anti-lock braking system (ABS) for example has a software component which should not be immutable unless the change was again tested by the authority which issued the approval. ABS is a deep component in the vehicle and is not connected to any other system. This does not really come to a business case for abuse.

2.2 Future situation

The current situation is changing rapidly: various components are controlled by software components that have (wireless) interconnections with other vehicles and infrastructure. The probability and impact of cybersecurity breaches are increasing exponentially. Vehicles will communicate directly to other vehicles and to road infrastructures and other systems. To improve traffic safety and traffic flow, vehicles and road side systems share pieces of information about the position, speed, and location. Improvements are made to communication and context awareness. This will prevent accidents and obviate other safety related risks. In addition, the information can be used to guide traffic, aiming to reduce traffic jams and C02 emissions. These are but few of the foreseen possibilities of connected and cooperative mobility.

With the introduction of new functions we also expect new business case for abuse, criminality or even terrorism. Because the software also affects the safety features and environmental performance, it should become an integral part of the existing approval processes.

2.3 Connected and cooperative context

Vehicle to Vehicle communication is a part of a more broaden concept of Intelligent Transport Systems (ITS). The communication between vehicles, and between vehicles and the outside world, will in almost all cases be wireless via different channels. Exceptions may be found in repair shops and

when vehicles are parked. This white paper will not write about specific brands or manufacturers unless it is important for the discussion. Actual implementations may vary between brands and models. One of the challenges is to harmonize the way ITS systems will communicate.
Vehicle-to-vehicle (V2V) communications and Vehicle to Infrastructure communication using the same wireless technology that supports V2V safety applications use different types of communication within connected and cooperative systems:

- V2I: Vehicle-to-Infrastructure communication. Many services will be implemented and most are related to safety, for example to alert drivers about traffic lights, speed limits and to inform about road works ahead.
- V2V: Vehicle-to-Vehicle communication. This is the area most researchers and application developers focus on. Typical services are anti-collision systems such as early break warnings from other vehicles, information about emergency vehicles approaching, synchronized lane change support, traffic jam ahead warnings, and services facilitating the driving experience such as car platooning.

The core of the V2V communication is the exchange of the message '*here I am'* on Wi-Fi. The car can gather the necessary data from existing systems such as a navigation system (GPS, Satnav) or mobile phone. Also, sensor data can be sent out of the vehicle, such as the current rate and the extent to which one brakes at a time. Furthermore, details about the vehicle itself, such as the width, length and height may be transmitted. This information provides context-awareness of a car. The vision is that with V2V, all vehicles (including cars, trucks, buses, coaches and motorcycles) can communicate with each other, and other systems such as roadside units, through the exchange of important information. This information can be used for passive and active systems to provide the necessary information. In technical terms, it is achieved with so called cooperative Intelligent Transport Systems (C-ITS –also known as V2X communication for vehicle-to-vehicle and vehicle-to-infrastructure communication).

2.4 Why is there a need for connected and cooperative mobility?

There is a need for cooperative ITS. Noticing traffic jams in a safe and intelligent way, before you see them. Detecting risks before they become a threat. The goal is to arrive at your destination safe and sound.
This vision of safe and intelligent mobility can be realised by wirelessly connecting vehicles and infrastructure. Cooperative systems enable direct communication between vehicles, roadside infrastructure and traffic control centres.
The benefits of V2X communication are numerous. It enables anticipatory and safe driving, as drivers are informed about the current traffic situation and danger zones in time. In addition traffic centres receive precise and comprehensive information on the traffic situation from vehicles. This way, it is possible to control the traffic flow more efficient and responsive, result-

ing in an improved flow of traffic. The effect: more safety, less accidents, an improved use of the road network. Less traffic and therefore less CO2 emissions.

2.5 Connected and interacting systems, a complex next generation infrastructure

The security challenges of a system in which millions of vehicles are driving on the roads in Europe and global, is impressive. A pilot in a restricted environment, when there are hundreds of connected and cooperative systems is very complex to manage. However, this is not comparable to the dimensions that we face when we want to create a secure, connected and cooperative environment, available in all member states of the European Union. An international system will have to be designed, which can be utilized by vehicles of all manufacturers, without significant adjustments.

Properties of such a complex system are the necessary cooperation between the different stakeholders. The different interests of the stakeholders and the shift in ownership.

As projects and acquisitions become increasingly complex, companies and governments are challenged to find effective ways to manage risks in such an environment. Harmonisation is the basis of the success or failure in such an environment. Automated systems such as V2X communication rely on a web of parts which interact on an ad-hoc basis. V2X communication become more network-centric and complex. The businesses will be forced to find ways to manage complexity. Governments will be challenged to provide effective governance to ensure flexibility and resiliency while maintaining an accepted level of security.

2.6 The international context

The basis for the pan-European deployment of cooperative ITS is already in place. The cooperative ITS technology has been developed within research and development projects and evaluated in field operational tests (FOTs). The majority of the enabling technology is already standardised.

This standardisation however is focussed on communication security standards. Privacy and other security challenges are generally still out of scope.

The Amsterdam Group is a strategic international umbrella organisation in which CEDR, ASECAP, POLIS and Car2Car Communication Consortium (C2C-CC) are represented. The name is chosen because the initial series of meetings were organized at Schiphol Amsterdam Airport. Participation in the AG is voluntary and aimed at facilitating joint deployment of ITS in Europe.

Within the AG, the so called front runner countries, the Netherlands, Germany and Austria together with the C2C-CC have taken the initiative to develop the ‘Cooperative ITS Corridor’.

Alignment between AG and other European Union (EU) Corridor projects like Scope@F (France) and the Czech Republic ITS program is envisioned. The main purpose of alignment is to realize interoperability and EU-wide use of C-ITS.

2.7 Why are privacy and security important issues in a connected world?

The December 2, 2013, letter of US Senator Edward J. Markey to car manufacturers based on a US study funded by the Defense Advanced Research project, explains why security should be an important part of development of V2V communication and implementation. In this letter Senator Markey stated that today's cars and light trucks contain more than fifty separate electronic control units (ECUs), connected through a controller area network (CAN) or other network (such as Local Interconnect Networks or Flexray). Vehicle functionality, safety and privacy all depend on the functions of these small computers, as well as their availability. Integrating mobile devices with vehicle-based technologies have also fundamentally altered the manner in which drivers and the vehicles themselves can communicate influencing the vehicles' operation.

Vehicle functionality, safety and privacy all depend on the functions of these small computers, as well as their ability to communicate with one another. They have the ability to record and analyse vehicle data for performance improvement.

The senator's two main concerns are:

- The researchers were able to directly connect to vehicles computer system, send commands to different ECUs through the CAN and thereby control the engine, breaks, steering and other critical vehicle components.
- The increasing use of navigation (GPS, Navsat) or other technologies that could be used to record the location or driving history of those using them. A number of services have emerged that permit the collection of a wide range of user data, providing valuable information not just to improve vehicle performance, but potentially for commercial and law enforcement purposes.

These two concerns describe the reason why it is important to promote security as an integral part of system design (e.g., security by design) and the need to address privacy while developing connected and cooperative systems, both of these topics also form the main focus for this white paper.

3 Standardisation

For technical standardisation, a number of bodies such as ETSI, CEN, ISO, SAE and IEEE play an important role. This work is elaborated upon by the C2C consortium, aiming at an open European standard for C-ITS for V2X use.

A recent report "Overview of standards for first deployment of C-ITS" gives a coherent overview expressing especially the Infrastructure to vehicle related additional profiling, specifications and standardisations development. On various topics such as security, the EU, US and Japan are working on international harmonisation. At the Transportation Research Board's (TRB) 94th Annual Meeting in 2015, a whitepaper will be presented with the first findings and recommendations.

Vehicle-to-Vehicle Communications could save over 1000 lives annually in the US. The US Department of Transportation has calculated the benefits of V2V for two applications.

- Left Turn Assist (LTA). A driver is alerted when an oncoming vehicle constitutes a risk.
- Movement Assist (MA a driver is warned of a collision risk while driving onto an intersection.

On a total of 592,000 accidents per year in the US, in 1083 cases LTA and MA could have prevented collision and thereby saved lives.

Above is an US example, where other applications are planned than in Europe. In Europe the focus is on the connected and cooperative applications that require V2X communications.

The V2X solutions are the basis for managing and directing traffic flows in order to reduce traffic jams and environmental pollution.

For admission of new vehicles, requirements from the EU/UN are leading. Overall vehicle requirements are established within the UN World Forum for Harmonization of Vehicle Regulations (WP.29) and to a lesser extent in Working Party on Road Traffic Safety (WP.1). Security requirements need to be addressed within these groups, should there be a need for security requirements to be a part of the formal admission of vehicles. Within Europe, contributions to these groups is organised via the European Union. As an example the Rijksdienst voor het Wegverkeer (RDW) represents the Netherlands in both the EU and the UN formal meetings.

3.1 Research agenda

The development of communication security standards for V2X communication is well on its way in close collaboration between the IEC, CEN and IEEE. Security is just one element of these standardisation efforts. Research is needed to establish which blind spots are not covered by the standardisation efforts. This is especially true for privacy that needs a more information focussed security approach than a focus on communication security.

4 Security by design

As the US DARPA study shows, a secure connection between on board units is necessary. However it is not only the connection. It all starts at the very beginning, security by design in the development phase of the components. Security by design means that the security is integral part of software and systems design. Possible malicious practices are taken as a starting point, and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input.

Generally, designs that work well do not rely on secrecy. It is not mandatory, but proper security usually means that everyone is allowed to know and understand the design because it is secure. This has the potential advantage that many people are looking at the code, and this improves the odds that any flaws will be found sooner. Of course, attackers can also obtain the code, which makes it easier for them to find vulnerabilities as well.

Furthermore, it is very important to follow best practices, such as working with the least amount of privileges possible (principle of least privilege). For example a V2X component that runs as the administrative user (root or admin) can have the privilege to remove or change configurations. Thus, a flaw in that program could put the entire system at risk. On the other hand, a V2X component that runs inside an isolated environment and only has the privileges for required network and file system functions, cannot compromise the system it runs on unless the security around it is in itself also flawed.

4.1 Research agenda

Pointing to the US DARPA study, the need for a secure design is clear. How to secure, what to secure and the method used to secure is subject to be investigated in the near future. V2V components need to be tamper proof. The components should be totally separated from other vulnerable on-board-units such as the infotainment system, where external devices and channels are becoming part of the system.

In broader terms, before a large roll out of V2X components should be considered, a thorough risk analysis on this subject should be performed. Based on risk analysis, a worldwide accepted security baseline should be defined. It should define the minimum security levels of both the in car components, the infrastructure components, the road side units and the back-office systems. The risk assessment should be related to the main objectives of cooperative and connected systems.

Examples of areas in which to conduct security and privacy related research are:

- Risks
  - Jamming and spoofing
  - Malicious car owners/users
  - Hostile attacks from hackers/crackers

- Focus areas:
    - Functionality versus security
    - Classification of data

And examples of research areas of potential measures:

- Secure development process
- Secure production process
- Separation of “fun devices” (infotainment) from the critical vehicle infrastructure

5 The need of system (component) certification

Every new type of vehicle that is built must have a type approval (certified) before it is allowed on the road. This is a worldwide accepted standard approach. The technical requirements a manufacturer has to comply to are clear and are part of the development process of a vehicle. Privacy and security requirements for V2X communication, however, are not defined yet.

This chapter describes what specific needs have been identified to support the creation of a pan-European scheme for certification, and why such a scheme helps to create a chain of trust. The general need for certification has been addressed in numerous studies.

5.1 Stakeholder needs

The European Union, as well as previous studies have done by international organisations such as NHTSA, the EU Seventh framework programme, the Dutch Ministry of Infrastructure etc.; provide statements regarding the recognition of a need for pan European privacy and security requirements.

Below is a summary of the various reasons:

- To solve trust issues between EU stakeholders.
- Create a common reference model for security requirements in the EU.
- Establish the basis for a minimum set of auditable controls across Europe.
- An agreed method to determine the level of security for different functions.
- A harmonised international approach for component, system, and operational security to increase trust.
- EU guidance for a harmonized approach that facilitates national legislation.
- Promote public and private interaction within the EU world for security.
- Improve the maturity level of security.
- Shared responsibility in risk mitigation amongst EU stakeholders.
- Lower costs of certification of connected and cooperative systems in the EU
- A certification scheme that addresses the life cycle of European (in fact world-wide).

In the connected and cooperative environment, privacy is an important reason to implement security measures. To achieve a security certification approach, the need to harmonise on a European level is mandatory.

5.2 A common set of security requirements

A prerequisite for certification is the adoption of a common set of security requirements for individual components. A risk based approach is necessary to achieve a secure environment. By performing a thorough risk analysis, followed by the development of a set of controls, to ensure that a minimum

security level is achieved. This requires that manufacturers are willing to adopt the security requirements and that there is a clear benefit to use certification as a means.
Certification is always based on certain levels of security to achieve. A security requirement in this context means that the manufacturer must have a certain freedom to decide how he will implement security measures in a component or product.
Common Criteria could be a mechanism to show compliance to governmental privacy and security requirements. The manufacturer may choose a certain minimum degree of certainty, which complies to the governmental requirements for security and privacy. The manufacturer must meet these requirements to achieve successful certification which is necessary for approval.

A prerequisite to achieve a successful certification scheme is an international agreed set of privacy and security requirements that is in compliance with legislation.

5.3 A standardised certification method

There is a need for one or very limited number of security certification standards. Manufacturers and asset owners are regularly globally acting companies. Car manufacturers are not bound to one country, since car manufacturers sell their products worldwide and will be interested in one certification standard valid for all countries.

Since cybercrime does not stop at borders or continents, the risks drivers we are facing are the same in Europe, the Americas, and the other continents. The best result can be achieved when the foreseen European standard is a worldwide accepted standard, such as ISO/IEC standards are now.

If we take this as a starting point, than in fact Common Criteria is the only international standardised certification method. Certification schemes known in Germany are complementary to Common Criteria (CC).

Using CC Certification methodology is just one of the possible solutions though. A study should give an in-depth view of the possibilities, the benefits and the drawbacks of using such a method to certify V2x components. One of the possibilities could be that only certified communication components are accepted for approval by EU/VN.

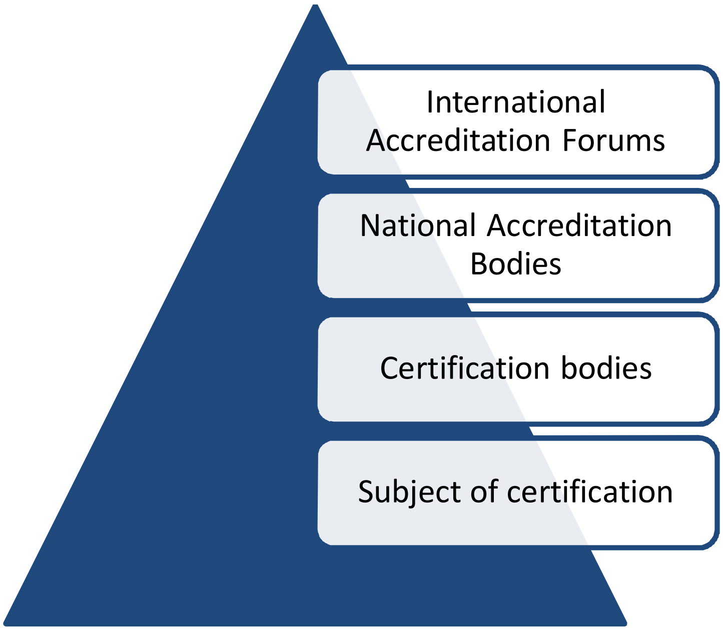
International Accreditation Forums
National Accreditation Bodies
Certification bodies
Subject of certification

Figure 1: Hierarchical approach of certification

5.4 Common Criteria

Common Criteria (CC) is an ISO/IEC 15408 framework completely focused on security in which computer system users can specify their security functional and assurance requirements through the use of Protection Profiles (PPs). Vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.

In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. The benefit of using Common Criteria is the fact it is a formal ISO/IEC 15048 standard which is widely accepted.

Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and for components in the critical infrastructure. The Participants of Common Criteria share the following objectives:

- to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles
- to ensure that evaluations of IT products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles

- to improve the availability of evaluated, security-enhanced IT products and protection profiles
- to eliminate the burden of duplicating evaluations of IT products and protection profiles
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles

The Netherlands, Germany, Italy, Norway and Sweden accepted Common Criteria as recognised standard for certification.

This all seems that CC is the de facto standard. However, it also has disadvantages. CC certification is a long and very expensive process. At every significant change in the software, hardware or design, the certification process must be repeated. You may wonder whether in a rapidly changing world as automotive, CC is an acceptable certification methodology. However, it could be possible to decide to apply CC for the primary and unchanging components.

The use of CC in combination with FIPS would be another opportunity to create a secure platform for the automotive industry

5.5 Certification schemes

The above requires a certification scheme that is industry led, widely adopted and recognised with focus on operational security requirements, such as availability, integrity and confidentiality while taking into consideration the specific constraints that are applicable for V2X systems.

A certification scheme will provide the customer or end client with clear identification of the resilience goal and an assurance that this resilience goal is realised by a valid strategy. Certification is deployed and maintained through a process of independent inspection, renewal of certification and annual surveillance checks.

The process for certification of a product is generally summed up in four steps:

- Application. including testing of the product
- Evaluation (does the test data indicate that the product meets qualification criteria)
- Decision (does a second review of the product application concur with the Evaluation)
- Surveillance (does the product in the marketplace continue to meet qualification criteria)

The use of certification schemes need to give confidence and proof that specified requirements are fulfilled.

There are several types of certification. Each type of certification has differentiating properties that deserve to be described separately. They can be subdivided in:

1. Component certification
2. System certification
3. Policies & Procedures certification
4. General certification

5.6 Conformity assessment

In general, conformity assessment is the process used to show that a product, service or system meets specified requirements. These requirements are likely to be contained in an ISO standard. But, ISO itself does not perform conformity assessments. Specific for automotive, all essential requirements are described in international guidelines and regulations. Showing that a product, service or system meets certain requirements has a number of benefits:

- It provides governments and consumers with added confidence.
- It creates a level playing field for manufacturers
- It helps regulators ensure that health, safety or environmental conditions are met.
- Governmental defined requirements lead to cost reduction for manufacturers as well as consumers.

The main forms of conformity assessment are certification, inspection and testing. Although testing is the most widely used, certification is the best known.

Conformity assessment enables buyers, sellers, consumers, and regulators to have confidence that products sourced in global market meet specific requirements. It is the demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

Conformity assessment procedures provide insurance that the products, services, systems, persons, or bodies have certain required characteristics. These characteristics are consistent from product to product, service to service, system to system, etc.

Conformity assessment can include:

- Supplier's declaration of conformity
- Sampling and testing
- Inspection and document evaluation
- Certification
- Management system assessment and registration
- the accreditation of the competence of those activities
- Recognition of an accreditation program's capability.

A specific conformity assessment scheme or program may include one or more conformity assessment activities. While each of these activities is a distinct operation, they are closely interrelated.

Conformity assessment activities can be performed by many types of organizations or individuals. Conformity assessment can be conducted by:

- A first party, which is generally the supplier or manufacturer
- A second party, which is generally the purchaser or user of the product
- A third party, which is an independent entity that is generally distinct from the first or second party and has no interest in transactions between the two parties, and
- The government, which has a unique role in conformity assessment activities related to regulatory requirements. For example in the Netherlands the RDW is the governmental certification body. The RDW however can use underlying test reports of third parties to decide for acceptance or rejection.

Terminology for conformity assessment in common is found in standard ISO/IEC 17000. Specific automotive certification schemes are defined for the European Union.

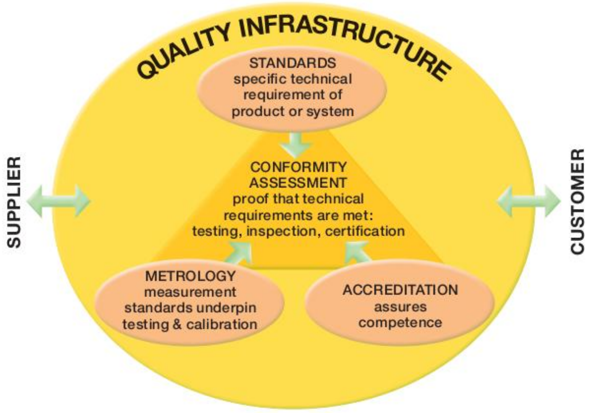
QUALITY INFRASTRUCTURE
STANDARDS
specific technical requirement of product or system
CONFORMITY ASSESSMENT
proof that technical requirements are met: testing, inspection, certification
METROLOGY
measurement standards underpin testing & calibration
ACCREDITATION
assures competence
SUPPLIER
CUSTOMER

Figure 2: Conformity assessment quality infrastructure

5.7 Research agenda

Before a large roll out of components a study is needed to support a decision whether or not certification and testing of components should be made mandatory. And for what components such a certification approach is relevant looking at the risks related to the various system components. The success stands and falls with a global standard and their industry acceptance. The ease with which components can evolve in a safe way will determine whether the industry is willing to invest. Should components be certified at the very strict assurance levels of Common Criteria? Or would it be possible to use a faster and cheaper conformance test against a globally adopted standard?

6 PKI

During the Utrecht workshop of V2V security, Public Key Infrastructure (PKI) was an important topic since it is the proposed solution to secure V2V communications. Amongst the experts, there is no consensus that the PKI is an overall solution for the variety of security requirements coming from the various use cases.

Public Key Infrastructure (PKI) refers to a global system of authentication, trust management, and privacy protection schemes where Certification Authorities (CA) act as electronic credentials issuers. The PKI model envisions ubiquitous and seamless recognition of electronic credentials in the form of security certificates.
The term Public Key Cryptography (PKC) refers to a class of cryptographic algorithms and related protocols and automated data processing mechanisms, which uses mathematical computations to avoid the use of a shared secret key between the parties while maintaining equivalent protection against adversaries as the Secret Key Cryptography (SKC) algorithms.

The deployment of PKC techniques should not be confused with the existence of a fully deployed PKI. PKI technologies have been criticized as being difficult to integrate with the applications that could make use of their services, requiring significant PKI-specific security expertise on the parts of application writers and maintainers.
Today's X.509 certificates have evolved into complex structures, with processing semantics that are far from trivial. This is primarily a matter of the information they carry, although it also involves its representation and encoding.
Formalization and simplification of these semantics may represent a valuable area for investigation.
Some of the complexity in certification results from a desire for a certificate to include a comprehensive set of ancillary information so that it can be used for off-line processing.
PKI models are evolving to include online components, which can offer alternative information sources to complement the certificates themselves.
Revocation mechanisms have long been recognized as a complex element in PKI, and path construction also introduces complexity. Despite the design attention that has been paid to revocation, it appears today that only a relatively small proportion of accepted certificates are actually checked for revocation status on an ongoing and timely basis.

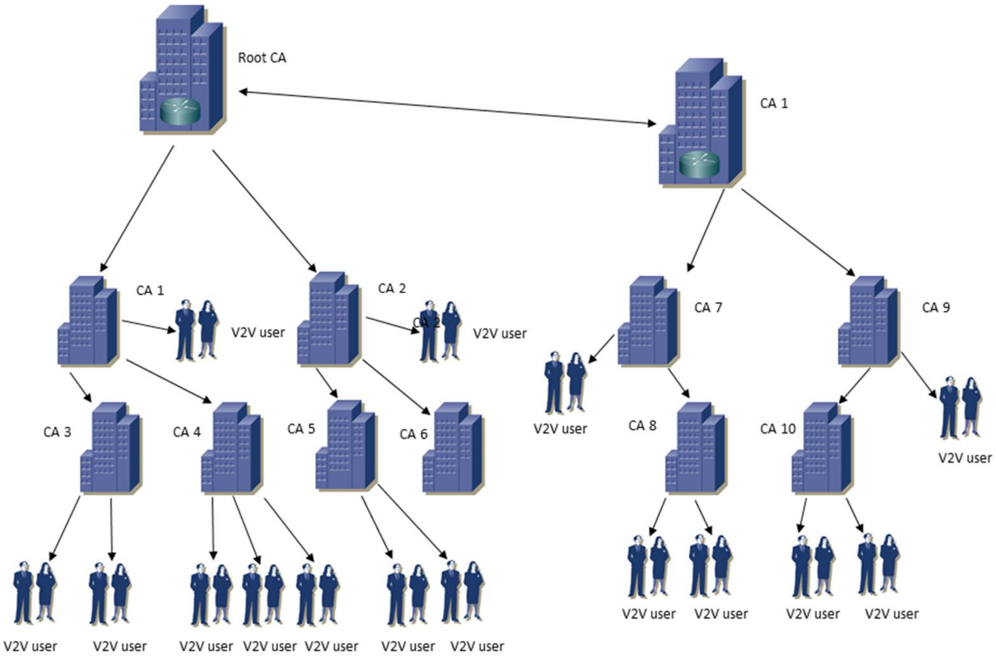

Figure 3: PKI hierarchy

One of the main concerns about a PKI is the enormous complexity of a PKI which should be implemented in millions of components such as the on board units in vehicles and road side units.

It is necessary to define three levels regarding the support of the driving task; strategic, tactical and operational levels.

- At the strategic level focuses on assisting motorists in planning the trip and navigating through a network. This typically takes off over greater distances (kilometres) and larger time scales (many minutes and even longer).
- The tactical level is the domain where the traffic management applications homes serving safety and flow in a network, typically of interest at the nodes (intersections where traffic is now controlled by traffic control systems).
- Operational support driving task takes self-same very small time and length scales (<100ms respectively. 10 stables meters) and ensures that the driver will always be safe. This can also be done directly on the engine management system.

Now to the problem: if the absolute safety is still guaranteed at the operational level, it is justifiable to use at the tactical level messages from not strictly authorized sources.

Most vehicles and vehicle owners have a personal interest (safety) not to manipulate their own systems. The majority of the vehicles will therefore provide reliable information.
PKI related questions are:

- why PKI provides a value in the process?
  - V2V authentication
  - V2I authentication
  - Confidentiality
- Which data has to be secured and at what level?
- Who issues certificates, this administration and manageable?
- How to organize your PKI?
- If you are going to use PKI, who is the root? How is that trust established?
- Who is the root CA? A government? A (non-)profit organisation?
- Are there multiple roots?
- Is there already an organisation available which can support a PKI or PKI alternative which is acceptable for all key players in this area?
- Who / why requests certificates?
- What problem do you solve using a PKI
- What can be done by the owner of a vehicle when his vehicles certificate is revoked?
- What is should be done by others when a certificate is revoked?
- What role does the government have in such a case?
- What is the effect on your PKI, authentication and authorization mechanism if you link your own device (smartphone) to the car systems?
- Is a PKI necessary for all communication security issues?
- PKI alternatives

6.1 Research agenda

Designing, implementing and organizing a full PKI solution for cooperative systems on a global or continental scale is such a complex challenge that it is has to be separated in several research questions. The main questions are whether there are other solutions that are less complex and easier to implement.

The international context described in chapter 2.3 is crucial to implement an overall secure and accepted solution. The international approach by both industry and authorities is necessary in order to achieve this goal. A study which answers the PKI related questions above, and gives clear directions on a secure implementation in V2X communication should be performed before a large roll out of V2X is possible.

7 Privacy

The Alliance of automobile manufacturers and the association of global automakers published a document called '*Consumer Privacy Protection Principles'* in November 2014. This document contains the privacy principles for vehicle technologies and services. Privacy is important to consumers, and it is important to the automobile industry. That is why the Alliance and Global Automakers have issued these Privacy Principles ("Principles"). The Principles provide an approach to customer privacy that members can choose to adopt when offering innovative vehicle technologies and services. Each member has made an independent decision about whether to adopt the Principles, and other companies may choose to adopt them as well.

Regardless of how participating members design their privacy programs and implement the Principles, they affirm the following fundamentals, as detailed in the relevant sections that follow:

- **Transparency:** Participating Members commit to providing owners and registered users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.
- **Choice:** participating members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.
- **Respect for Context**: Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.
- **Data Minimization, De-Identification & Retention**: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.
- **Data Security:** Participating Members commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.

These principles are covering some of the main concerns of the members of the Utrecht workshop. The Utrecht workshop defined the necessity to get a clear vision on data ownership. For this it is necessary to define roles and responsibilities, answering questions such as, who is entitled to use the data transmitted by the vehicle? Does the government have the right to tax a vehicle owner per mileage on the basis of automated data broadcasts? Could the government impose a fine for violations such as speeding, illegal parking based on information processed in the system?

In the European context it is necessary to integrate the "just enough principle" besides the opt-in and opt-out principles. The just enough principle forces the users of personal data to erase or anonymise all data which is in the data-packet and which is not direct necessary to use for the purpose the data is collected for. The collection of data is bound to the need to col-

lect such data, but also to the purpose for which the data is collected. Proportionality and subsidiarity are also part of the responsibility for the collection of personal data.
Other concerns are the use of data for commercial purposes. After a few times visiting the same brand fuel station, the user would be advertising the latest offering in the shop can be displayed on its display.
Has the owner/driver of a car the right to opt-in/opt-out for registration of personal data produced by his vehicle? This will possibly depend on the data produced and transmitted by the OBUs and road side units and the way this is handled by the other systems in the context of connected and cooperative mobility.
By implementing personal data protection as part of security by design, security will improve privacy.

7.1 Research agenda

Issues to investigate in the near future are:

- The definition of data
- To define data ownership
- To define the just-enough principle
- The users of the data, their rights, what data to use and how to use the data
- The need for a balance between the rights of the customer and transparency of the use of the data by governments and the car manufacturers
- To define the different levels of security of personal data produced by the OBUs, road side units and other infrastructural components
- To guarantee the personal data protection of EU citizens.
- Organise the protection of privacy related information in emerging Connected and cooperative mobility in the EU context

8 Behaviour

This white-paper is strongly focused on the protection of system components against misbehaviour by car manufacturers, governments and criminal organisations. The vehicle owner and the user of a vehicle however, can also be factor of risk.

Incorrect behaviour, but also consciously or unconsciously malicious acts may cause risks to other road users. Conscious behaviour can for instance result in the manipulation of the on board units and road side units. One reason may be that the user in some way benefits from knowingly broadcasting false signals and thus deceiving the systems that receive these falsified messages and triggering undesired and or unexpected system behaviour. Another reason may be that a malicious user benefits from receiving information that is otherwise not accessible. In part this behaviour could be avoided by an opt-out option for regular users, so he need not worry about the misuse of their personal data. On the other hand tamper proofing critical components might also contribute to reducing the risks related to abuse.

8.1 Research agenda

Perform a risk analysis to define the threats, risks and vulnerabilities related to abuse of critical components in the end-to-end communications within the system. The end-to-end system contains the OBUs, the road side systems, the infrastructure components and the back-end systems. Based on this risk analysis define a security baseline to comply in the design of the connected and cooperative systems.

9 Conclusion

The conclusion of the Utrecht workshop of November 27 2014 is that V2X is an important boost for road safety. The technique for achieving this goal is evolving rapidly, and will be available in the foreseeable future. In order to realize a large-scale deployment of connected and cooperative mobility, steps will have to be taken to clear the obstacles described in this paper. In the previous chapters the relevant issues that have been identified and discussed within the workshop are described and direction for further research is given.

Some of the research topics are related to obstacles that are mainly of a technical nature such as technical interoperability and identifying security best practices to be implemented. If not already addressed, these technical issues should be considered to put forward to the relevant international standardisation bodies. Other topics on the research agenda are related to obstacles that are related to policy, organisation and process oriented decisions that influence technical implementation decisions to be made. These topics should be addressed within the workgroups at the EU and VN that need to provide the required guidance coming from policy decisions still to be taken.

In the summary of the research agenda presented below for each of these topics an indication is given if the focus should be on addressing it at a technical level or at a policy level. It should be noted that it is expected that developing the required policies is still in an initial phase. Getting these topics on the agenda is the first step towards the required policy decisions to further stimulate the required technical developments.

The table below summarizes the research agenda:

Topic	**Research agenda**
Standardisation (Chapter 3)	The development of communication security standards for V2X communication is well on its way in close collaboration between the IEC, CEN and IEEE. Security is just one component of the system. Research is needed to establish which blind spots are not covered by the standardisation efforts. This is especially true for privacy that needs a more information focussed security approach than a focus on communication security. (Focus on technical aspects)
Security by design (Chapter 4)	Before a large roll out of V2X components would be considerate, a thorough risk analysis on this subject should be performed. The risk assessment should be related to the main objectives of cooperative and connected systems. (Focus on technical aspects) Based on risk analysis a wide accepted security

	baseline should be defined, which defines the minimum of security levels of both the in car components, the infrastructure components, the road side units and the back-office systems should be comply to. (Focus on policy, organisation and processes)
Certification and testing (Chapter 5)	An important study before a large roll out of components is a decision to take about certification and testing of components used for the communication between the various system components. The success stands and falls with a global standard and the reliability of the communication between these components. The ease with which components can evolve in a safe way will determine whether the industry is willing to invest. Should components be certified at the very strict assurance levels of Common Criteria? Or would it be possible to use a faster and cheaper conformance test against a globally adopted standard? (Focus on policy, organisation and processes)
PKI (Chapter 6)	Designing, implementing and organizing a full PKI solution for cooperative systems on a global or continental scale is such a complex challenge that it is has to be separated in several research questions. The main questions are whether there are other solutions that are less complex and easier to implement. (Focus on Technical aspects) The international context described in chapter 2.3 is crucial to implement an overall secure and accepted solution. The international approach by both industry and authorities is necessary in order to achieve this goal. A study which answers the PKI related questions above, and gives clear directions on a secure implementation in V2X communication should be performed before a large roll out of V2X is possible. (Focus on policy, organisation and processes)
Privacy (Chapter 7)	Issues to investigate in the near future are: • To define the different levels of security of personal data produced by the OBUs, road side units and other infrastructural components • The definition of data (Focus on technical aspects) • To define the data owner • To define the just-enough principle • The users of the data, their rights what to use and how to use the data • The need for a balance between the

	rights of the customer and transparency of the use of the data by governments and the car manufacturers • To guarantee the personal data protection of EU citizens. • Organise the protection of privacy related information in emerging Connected and cooperative mobility in the EU context (Focus on policy, organisation and processes)
Behavior (Chapter 8)	Define in a risk analysis the threats, risks and vulnerabilities related to abuse of critical components in the end-to-end communications within the system. The end-to-end system contains the OBUs, the road side systems. The infrastructure components and the back-end systems. (Focus on technical aspects) Based on this risk analysis define a security baseline to comply to in the design of the connected and cooperative systems. (Focus on policy, organisation and processes)

Annex

Contributors to this white paper
Connecting Mobility would like to recognise the contribution of the team members that contributed to this report in collaboration with and on behalf of Connecting Mobility:

Hans Baars	DNV.GL
Tjerk Bijlsma	TNO
Timo van Roermund	NXP
Sander de Kievit	TNO
Peter Goossens	Vialis
Marcel Otto	Connecting Mobility
Jordan Schonagen (co-facilitator)	TNO
Johan Lukkien	TU Eindhoven
Jaap-Henk Hoepman	Radboud University Nijmegen
Hellen Havinga	RWS
Hans Driever	Connecting Mobility
Gilles Ampt	HP
Fred Verweij	RWS
Chris Hottentot	ANWB
Ben Rutten	TU Eindhoven
Andre Smulders (facilitator)	TNO

Annex 1: Abbreviations

AG	Amsterdam Group
C2C-CC	Car2Car Communication Consortium
CA	Certification authority
CAN	controller area network
CC	Common Criteria
CEN	European committee for standardisation
C-ITS	Communication Intelligent Transport Systems
DARPA	Defence Advanced Research Projects Agency
ECU's	electronic control units
ETSI	European Telecommunications Standards Institute
EU	European Union
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IMA	Movement Assist
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transport Systems
LTA	Left Turn Assist
NIST	National Institute of Standards and Technology
OBU	On Board Unit
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration authority
SAE	global association of technical experts in the aerospace, automotive and commercial-vehicle industries
TRB	Transportation Research Board
USA	United States of America
V2V	Vehicle-to-Vehicle
V2I	Vehicle to Infrastructure
VC	Vehicular communication
W3C	World Wide Web Consortium
XML	Extensible Markup Language

Annex 2: Documents used in the workshop

[1] CEN/CENELEC/ETSI, *White Paper No. 01, Recommendations for a Strategy on European Cyber Security Standardisation*, 2014.

[2] Information-Technology Promotion Agency, Japan, *Approaches for vehicle information security*, 2013.

[3] C. Hesselman; J. Jansen; M. Wullink; K. Vink; M. Simon, *Een privacyraamwerk voor 'DNS big data'-toepassingen*, 2014.

[4] C. Rizzo; C. Brookson, *ETSI White Paper No. 1, Security for ICT - The work of ETSI*, 2014.

[5] S. Cadzow, *Presentation: ITS-Safety, security and Privacy*, 2012.

[6] C-ITS Platform WG5: Security & Certification, *Meeting Agenda*, 2014

[7] E.J. Markey US Senate, *Letter to Volvo Cars,* 2013

[8] National Highway Traffic Safety Administration, *Vehicle-to-vehicle communications: Readiness of V2V technology for application*, 2014*.*

[9] J. Petit; S. E. Shladover, *Potential Cyberattacks on Automated Vehicles*, 2014

[10] T. B. Lee, *Self-driving cars are a privacy nightmare. And it's totally worth it*, 2013*.*

[11] T. Bijlsma; S. de Kievit; J. van de Sluis, E. van Nunen; I. Passchier; E. Luiijf, *Security Challenges for Cooperative and Interconnected Mobility Systems*, 2013.

[12] J.H. Hoepman, *In Things We Trust? Towards trustability in the Internet of Things*, 2011.

[13] Ministerie van Verkeer en Waterstaat, *SSDD On-Board Equipment (OBE)-Level 1: System/Subsystem Design Document*, 2009

[14] Ministerie van Verkeer en Waterstaat, *SSS Trusted Element (TE) - Level 2: System/Subsystem Specification*, 2009

[15] 3rd Leipzig IOT Meeting, *Policy Challenges for the Internet of Things: Turning Opportunities into Realities*, 2013

[16] P. Goossens, *Presentation: Aanpak A58 security issues*, 2014

[17] S. Hania, *Presentation: Connected Car, Big data, Big Brother?: Using geolocation in a trustworthy and compliant way,* 2014

[18] S. Checkoway; D. McCoy; et.al, *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 2010

[19] ETSI, *ETSI TS 103 097, ITS Security: Security header and certificate formats*, 2013

[20] SysSec, *Deliverable D6.2: Intermediate Report on the Security of the Connected Car*, 2012

[21] Future of Privacy Forum, *The connected car and privacy navigating new data issues*, 2014

[22] Alliance of Automobile Manufacturers, inc; Association of Global Automakers, inc, *Consumer Privacy Protection Principles: privacy principles for vehicle technologies and services*, 2014

[23] P. Striekwold, *Opdrachtomschrijving software security voor ITS*, 2014

[24] Ministerie van Infrastructuur en Milieu, *Flyer: Cooperative ITS Corridor Joint Deploymen*

Connecting Mobility

For more information
www.connectingmobility.nl

Januari 2015