Cooperative-ITS Security Policy Framework: Executive Summary

Document HTG6-1

Version: 2015-09

EU-US ITS Task Force
Standards Harmonization Working Group
Harmonization Task Group 6

European Commission
tca Transport Certification Australia
INTERNATIONAL ITS COOPERATION

Harmonization Task Group 6 Membership	
Gianmarco Baldini	European Commission's Joint Research Centre
William Ball	Merriweather Advisors
Claire Barrett	US Department of Transportation
Norbert Bißmayer	Fraunhofer, SIT
Dominie Garcia	Booz Allen Hamilton
Dawn LaFrance-Linden	US Department of Transportation
Tom Lusco	Iteris
Vincent Mahieu	European Commission's Joint Research Centre
Catherine McGhee	Virginia Department of Transportation
Robert Rausch	Transcore
William Whyte	Security Innovation
Harmonization Task Group 6 Leadership	
Knut Evensen	Q-Free, European Commission
Peter Girgis	Transport Certification Australia
Wolfgang Höfs	European Commission DG Communication Networks, Content and Technology
Suzanne Sloan	US Department of Transportation
Steve Sill	US Department of Transportation

Executive Summary

Advancements in communications technologies are rapidly transforming the world's strategies for increasing safety, gaining operational and cost efficiencies, and reducing environmental impacts from transportation. Using new forms of short-range communications, vehicles and devices are now capable of broadcasting or receiving data that allow them to sense the movements and status of other surrounding devices. These exchanges create a three-hundred-and-sixty-degree awareness that, when further fused with other open data, can enable drivers, and other users of the transportation system, to receive alerts and warnings regarding the formation of threats and hazards. Based on this cooperative exchange, these communications have the capability to result in prevention of crashes, leading to reductions in fatalities, injuries, and property damage.

Access to these new data sets can also transform network operations and minimize the capital investment costs of infrastructure owners and operators. Broadcast data sets from users within a highly mobile environment can complement or potentially supersede the need for significant roadside equipment on major roads. These data can also form a more complete representation of conditions on the arterial network, including road weather impacts, effects of traffic signal timing, support for incident and emergency responders, or changes in traveler decisions, among other conditions.

For these new cooperative intelligent transportation system (C-ITS) technologies to be widely accepted by markets and used by the public, new types and levels of security will need to be introduced into transportation. Envisioning this need, policy makers, vehicle manufacturers, infrastructure owners and operators, application developers, and other transportation stakeholders gathered with security experts to:

- Understand the technical capabilities of today's communications security solutions;
- Describe the technical requirements and constraints of a C-ITS security solution;
- Identify gaps as a means of tailoring solutions to meet the unique C-ITS requirements; and
- Develop concepts and testable prototypes that are now forming the basis of technical designs for initial C-ITS security systems.

In late 2013, acting under an international agreement to collaborate, the European Commission (EC), the United States Department of Transportation (USDOT), and Transport Certification Australia (TCA) committed resources and experts to address the policy needs of C-ITS security solutions. These decision makers formed the Harmonization Task Group 6 (HTG6), and this Executive Summary and series of reports are the outcome of this team's work. The focus of the work has been to develop collaboratively a policy framework that identifies key areas for C–ITS security policy harmonization across jurisdictional boundaries.

The outcomes are significant—the results identify the importance of requiring harmonized security policies. Key results note that:

- Implementation of harmonized policies engenders and sustains public trust in the C-ITS system and applications, particularly within a highly mobile environment that expects C-ITS services to remain available as networks evolve over time and as services cross borders.
- To support cross-border/cross-jurisdictional operations of C-ITS applications, individual security systems (known as C-ITS Credential Management Systems or CCMS) require a defined range of harmonized processes as well as specific, secure data flows to support digital auditing and system transparency.
- Planning for inter-CCMS or intra-CCMS communications will require decisions when developing near-term operational systems but those decisions may have longer-term impacts on crypto-agility, system flexibility, and evolution of systems that must be considered from the start.
- Critical near-term steps for policy and decision makers to perform include:
    - **Minimize the number of CCMS:** Policy makers must determine the number of CCMS that will be operational within a local, regional, or national jurisdiction. Increasing the number of CCMS, in particular the root authorities, significantly increases complexity and cost.
    - **Assess risk and set appropriate parameters for risk and privacy:** No system will ever be without risk. Policy and decision makers must set acceptable levels of internal and external risk, as well as levels of privacy protection. Further, systems managers must assess these levels continuously throughout the lifecycle both of the security solution as well as end-entity (user) devices and applications. Risk and privacy levels come with trade-offs that will need to be assessed by policy makers.
    - **Choose appropriate trust models**: After system managers assess and categorize risk, they can identify policy and technical controls to mitigate risk. Collectively, these controls support the implementation of trust models that range from no trust among security entities to full trust that allows users ("trusted actors" that are accepted into the C-ITS security environment) to receive security services even after leaving their "native" system in which they are enrolled. Decisions are also required to establish criteria that define who are trusted actors and policies and procedures for certification, enrollment, removal in the event of misbehavior, and reinstatement.
    - **Establish Governance**: These decisions include the identification and convening of key stakeholders who will require representation in ongoing decision-making. Once convened, this group will establish processes for decision-making, define criteria for new entrants into the governance process, assign roles and responsibilities, establish authority to provide governance and enforcement, and determine enforcement procedures.
    - **Implement harmonized processes:** The HTG6 team identified the priority areas for harmonization. Policy makers will need to examine them to determine which ones are

appropriate both to support their choice in trust models and throughout the CCMS lifecycle. With these policy decisions, technical system developers can use HTG6 reports to identify the interfaces and data flows that will need to be implemented to support harmonization and trust.

Importantly, to be harmonized does not require identical security solutions. Instead, systems can use common technical or even slightly incompatible approaches as long as there is coordination on a policy level regarding exactly what criteria are used to determine that a device is trustworthy enough to be issued credentials. Since the modern car market is global, it is likely that, at some point, devices authorized by one CCMS will have to interact with devices authorized by other CCMS. Further, mechanisms for devices of one CCMS to trust communications from devices native to another CCMS will be needed for neighboring jurisdictional systems. The degree to which CCMS implement similar functionality and share information depends on the degree to which CCMS 'trust' one another. At the very least, because CCMS will need to be upgraded, the future CCMS will need to be able to handle both existing and future devices. In addition, future devices will need to interact both with the original CCMS and with the newly implemented CCMS.

Fundamentally, this concept of inter-CCMS trust implies organizational trust between the entities managing the CCMS and technically such trust is reflected in digital interactions and shared policies between the CCMS. The C-ITS environment may end up with any number of CCMSs, which, for CCMS that do trust one another, expands the number of inter-CCMS interfaces if a polynomial fashion. It is crucial for future interoperability and extensibility that implementers understand the repercussions of inter-CCMS trust to inform their implementation decisions.

Format of HTG6 Results

HTG6 results are presented in a series of reports. The primary reports include:

- **Executive Summary (HTG6-1; this document).** This document is a high-level summary of the key results.
- **Summary of Results (HTG6-2).** This report summarizes the results across the body of HTG6 work for policy and decision makers.
- **Architecture Analysis (HTG6-3)**. This report identifies the primary elements of a Public Key Infrastructure (PKI) security system and compares these fundamental needs against four security architectures:
    - The EC's Joint Research Centre PKI for secure and confidential commercial vehicle digital tachograph regulation (an operational system)
    - TCA's Gatekeeper PKI for secure and confidential commercial vehicle regulation (an operational system)
    - EC's PRESERVE PKI architecture design for secure, authenticatable communications
    - US's Security Credential Management System (SCMS) architecture design for secure,

private, and authenticatable communications.

The comparative analysis yielded an understanding of the fundamental elements of a C-ITS Credential Management System (CCMS) that (a) are highly recommended for harmonization; (b) are recognized as beneficial if harmonized; or (c) do not require harmonization. The conclusions in this report highlight the areas for harmonization, describe them, and assign priority levels to harmonization decisions.

- **Functional Decomposition Analysis (HTG6-4).** This report further analyzes the recommended areas that are identified as "highly beneficial" for harmonization in HTG6-2. To come to these results, the team decomposed a CCMS architecture and identified the interfaces and data flows where actions are needed to achieve harmonization. In many instances, the harmonization action requires a technical solution to establish inter-CCMS or intra-CCMS trust. In some instances, our team recognized that harmonization of language is also needed. If devices can communicate their level of security in manner that is clear and consistently defined, the actual devices or other technical harmonization actions are not needed.
- **Organizational Analysis (HTG6-5).** This report identifies how policies need to be harmonized to support trust models—both among the various entities that comprise a jurisdictional CCMS (intra-CCMS) as well as between jurisdictional CCMS (inter-CCMS). This report also describes the requirements for communication of those policies as a basis for harmonizing inter-CCMS and intra-CCMS trust, particularly across jurisdictional boundaries.
- **Risk Management Framework (HTG-6)**. This report describes a process for implementers to identify and categorize their risks. This process leverages existing risk categorization processes from the National Institutes of Standards and Technology (NIST) and Common Criteria. The results support decision makers in identifying appropriate technical and policy controls to include in a CCMS architecture to mitigate or address risk. This report further identifies, at a high-level, some of the gaps that are not addressed by NIST/CC but that are needed for a cooperative security environment. Further analysis is needed to fully identify gaps.
- **Background Documents**. HTG6 also produced background documents to accompany these key deliverables. These documents include:
    - **PKI Primer (HTG6-7)**
    - **Primer on the Intelligent Transport Systems (ITS) Station concept and the Connected Vehicle Reference Implementation Architecture (CVRIA) (HTG6-8)**
    - **Glossary (HTG6-9)**

Next Steps

HTG6 results describe a C-ITS security policy framework that:

a) Delineates where key policy decisions are needed;

b) Describes roles and responsibilities;

c) Identifies where policy harmonization would be highly beneficial and provides guidance, in the form of trust models and implementation options, for achieving harmonization and trust between C-ITS participants;

d) Identifies consequences for not pursuing harmonization – whether it be the lack of trust or other impacts to the C-ITS environment;

e) Establishes that the parameters for policy are multi-dimensional—they span geography, time, application borders, and technology lifecycle stages; and

f) Presents a process for identifying and categorizing risks that lead to the proven processes for choosing policy and technical controls.

The collective analysis of CCMS and policy requirements led to conclusions about additional actions needed to address gaps. Key gaps of concern to policy makers are listed below. Additional technical gaps that may require further research are included in the appropriate reports. In summary:

- With regard to interfaces and standards:
    - The lack of interface specification between entities participating in C-ITS is among the biggest issues confronting CCMS designs and the long term C-ITS deployment.
    - To ensure consistency and scalability, the C-ITS community will need to develop standards to codify the interfaces between CCMS.
- With regard to certification and its relationship to security access:
    - The C-ITS community will need to establish requirements defining how end entities must be engineered, manufactured, and handled in order to obtain credentials, and establish shared requirements for proper disposal.
    - Device and application certification processes will need further definition to determine how they are linked with credential management, and as such must be considered concurrently with the architecting of security management systems and procedures.
    - A future harmonization activity is likely needed to clarify the relationship between certification and credentials distribution. If harmonization is lacking, each implementer will have to perform this analysis, making inter-CCMS trust unlikely.
- With regard to evolution:
    - The Crypto-agility concept will need further definition to identify processes needed beyond system maintenance.

- Further research will be needed to define options and use cases; and analysis is needed to identify how “day-one” decisions will impact future decisions and potentially constrain or support future system flexibility or evolutionary choices.

- Last, with regard to establishment of implementable policies:
  - The CCMS management community will need to collectively define CCMS policy frameworks. Issues such as resource management, CCMS policy management, actual CCMS policies, and CCMS scoping need to be further addressed.
  - Inter-CCMS trust scenarios will need further study, as they have significant implications for the architecture and management of a CCMS.
  - Further, the C-ITS policy makers may wish to leverage the HTG6 initiative and consider the value and of an international association or “federation” of CCMS that can develop near-term policies collaboratively, share best practices and other useful information, and develop “accreditation” criteria for new CCMS entrants, among other actions.