Cooperative-ITS Security Policy Framework: Summary of Results

Document HTG6-2

Version: 2015-09

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

European Commission

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

Contents

Figures

1 Introduction

Harmonization Task Group 6 (HTG6) began in early 2014 as a cooperative effort between the European Commission (EC), Transport Certification Australia (TCA), and the United States Department of Transportation (USDOT) to address multiregional Cooperative Intelligent Transportation Systems (C-ITS), also known as "Connected vehicle" or "CV" in the US. The focus of HTG6 was to develop a security policy framework for C-ITS collaboratively. The HTG6 work included:

- Identifying those policies and decisions that, if harmonized, offer significant public benefit;
- Analyzing the technical and policy/management elements of trust models associated with communications security systems, and identifying the impact of different privacy levels; and
- Developing consensus on policy options that effectively and beneficially result in coordinated management policies and security approaches to the extent possible for C-ITS.

The body of work produced by HTG6 members presents the maximum set of common policy approaches with justification for the benefits for commonality. The team further recognizes policies and approaches that can differ regionally without impact.

HTG6 is comprised of acknowledged hands-on policy and technical experts. The members of HTG6 are deeply involved in policy analysis, C-ITS implementation, and security-related fields, and include hands-on technical researchers, standards developers, communications engineers, certification experts, and original equipment manufacturers. The HTG6 team reached out to external experts for their input as a measure to ensure that the results would be viewed credibly by the broader standardization community.

1.1 Format of HTG6 Results

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

- **Executive Summary (HTG6-1).** This document is a high-level summary of the key results.
- **Summary of Results (HTG6-2; this document).** 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)**

2 Purpose of this Document

The goal of HTG6 is to facilitate successful implementation of any jurisdictional C-ITS security system seeking to harmonize with adjacent systems by presenting a C-ITS security policy framework. This document, **HTG6-2: Cooperative-ITS Security Policy Framework: Summary of Results,** summarizes the work documented in the series of reports provided by HTG6; identifies, for policy and decision makers, a set of recommendations; and offers an overall review of recommended actions.

2.1 Background

Transportation is on the edge of a significant transformation. Technological advancements have created the ability for short-range communications to provide sensing capabilities that offer drivers and transportation roadside equipment both a physical sense of the near-by environment (similar to radars and cameras) as well as a logical sense of the surrounding, built-environment (for example, short-range communications can alert drivers of impending crash scenarios even in the presence of buildings or other obstacles that might block the driver's view).

By adding short-range communications to the transportation environment, new forms of cooperative applications that utilize new vehicle-based safety/awareness data broadcasts and fuse that information with existing data sources in real-time, become possible. Cooperative applications include:

- Vehicle-to-vehicle communications (V2V) that enable crash-avoidance through broadcasts of a safety/awareness message that allow nearby vehicles to sense another vehicle's presence as well as calculate the formation of emerging threats and hazards to warn the driver;
- Vehicle-to-infrastructure or Infrastructure-to-vehicle (V2I/I2V) can similarly increase safety while also optimizing system efficiencies and reducing environmental impacts through broadcasts as well as peer-to-peer communications; and
- Vehicle-to-other types of devices (V2X) allows for the integration of pedestrians (V2P), motorcycles, bicyclists, and other transportation system users to be part of the cooperative environment.

These new forms of applications are cooperative because they require mutual exchange of data between trusted users within the environment. In order for C-ITS implementations to be successful, participants must be able to rely on alerts and warnings based on the exchange of data from trusted, if unknown, sources. In addition to authenticating thousands of data messages simultaneously in real-time, a C-ITS security system needs to provide protection against internal and external threats to the primary elements of a C-ITS: communications, devices, and network and organizational structure[1]. These are demanding requirements. The need for the C-ITS security solution to meet, among others,

[1] Another primary element of C-ITS is the Global Navigation Satellite System (GNSS) that provides location and timing information. The security of the GNSS is being treated as outside the scope of HTG6.

requirements for scalability, extensibility to multiple users, and financial stability, is a significant challenge.

A PKI approach is the security solution widely identified as uniquely suited to the C-ITS environment. It is a proven way of instantiating a credential management system and it can be tailored to meet the unique and demanding requirements of a C-ITS environment. Currently there are at least two projects underway to build a C-ITS Credential Management System based on PKI: one in the US and one in Europe. Australia is researching the ability to build upon or leverage an existing PKI for commercial vehicle regulatory applications.

These systems use slightly incompatible technical approaches and have not, to date, coordinated on exactly what criteria are used to determine that a device is trustworthy enough to be issued credentials. However, 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. In addition, as CCMS need to be upgraded, the future CCMS will need to be able to handle both existing and future devices and 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 CCMS, which, for CCMS that do trust one another, adds the number of inter-CCMS interfaces in a polynomial fashion. . It is crucial to support future interoperability and extensibility that implementers understand the repercussions of inter-CCMS trust to inform their implementation decisions.

2.2 Issue and Opportunity

With this background, three parties—the EC, the USDOT and TCA—committed time and resources to a collaborative effort to develop a C-ITS security policy framework. The timing was appropriate because:

- An EU-US Memorandum of Agreement (MOU) had been established in 2009 and provided the organizational mechanism to support harmonization efforts. In January of 2014 when HTG6 was launched:
    - HTG1 and HTG3 had resulted in success: similar (but not identical) standards had emerged for the broadcast safety message (known as the Cooperative Awareness Message, or CAM in the EU and the Basic Safety Message, or BSM, in the US) and for the communications security certificate.

  - HTG4/5 was underway to develop, collaboratively, key infrastructure standards.

- Two security system designs were emerging to address different functions and risk elements within a C-ITS environment. On the European side, opt-in V2I applications formed the basis of C-ITS security requirements, whereas in the US, potentially mandatory V2V applications were driving requirements. Although both systems were still in the concept stage and evolving, enough specificity was understood to allow for analysis.
- Deployments were being planned for 2015 in Europe (along a corridor from Rotterdam, The Netherlands to Vienna, Austria), in Australia (south of Sydney), and in the US (competitive grants will be awarded in the Fall of 2015 for multiple sites).
- Further, two transportation-based PKI systems that operate in the EU and in Australia were used to inform the HTG6 analysis and provide key lessons learned regarding risk analysis, device and system lifecycle analysis, effective management and operational policies, end-of-life policies, and evolutionary needs of a system.

The HTG6 team further recognized and confirmed through analysis:

- Critical future impacts if a holistic approach to security policy is not established at inception of systems:
  - There may be a lack of interoperability that leads to C-ITS services being non-functional as users cross borders;
  - Public trust may erode and new technologies may not be adopted; or
  - Changes will result in difficult and costly actions to revise these complex systems after they are deployed and operational.
- Opportunities that include:
  - Joint planning with cross-border and neighboring jurisdictional systems that will result in lower costs and simplified planning and design
  - Ability to leverage existing resources and build from them.

For the HTG6 team, the problems that plague the Internet provided an example of not taking a comprehensive approach to security—trust is frequently broken and it is proving difficult and costly to attempt to build security into the operational system. The PKI system for EC's JRC tachograph that secures commercial vehicle regulatory applications offers an additional example of how a system upgrade, or evolution, can become difficult and costly if planners do not consider how near-term decisions and choices may impact future system capabilities.

2.3 Structure of the Analysis

The HTG6 Work Item Description (WID) was developed in Fall of 2013 and included the interests of stakeholders regarding analysis to determine where harmonization was most beneficial or most needed. In late 2013, policy, technology, and security experts from the different geographic regions were identified and their time was committed. Upon gathering in 2014, the team described a path for analysis that evolved over time with insights and lessons learned.

Over the course of the year, the analysis path has included:

- A comparative analysis of PKI architectures—those in existence today and those being planned for the C-ITS environment.
- A synthesis of risk analyses from Government and industry sources and a categorization of C-ITS risks to identify a process for local policy and decision makers to determine their level of acceptance of risks and apply appropriate policy and technical controls.
- A functional decomposition of a generic CCMS to identify the key interfaces and their information flows or controls that establish trust between CCMS or among CCMS entities.
- A cross-jurisdictional organizational analysis that identifies the management policies and inter-organizational policies needed (in alignment with the technical controls) to support inter- and intra-CCMS trust.
- A comparison of the language and terminology differences and their effect upon harmonization. Specific to this analysis was an examination of the ITS Station concept and the Connected Vehicle Reference Implementation Architecture (CVRIA).

Two key fundamental concepts that guided the HTG6 team included:

- C-ITS environments have unique constraints that policies must support:
    - The system must scale to meet the needs of millions of users;
    - To support privacy at the highest levels, the system must not need to know the identity of participating parties and must comply with data protection requirements of relevant legal frameworks;
    - The system must be fast (and thus the communications exchange not burdened by security overhead) to support crash-avoidance applications, in particular;
    - The system must provide security to protect critical assets as well as access to critical assets by trusted users;
    - The system must work with a highly mobile environment; and
    - The system must support trust among known cross-jurisdictional and operational partners.

- A C-ITS security solution is implemented for a set of specific roles:
    - To protect critical ITS assets (such as devices and applications); and
    - To protect access to critical ITS assets for trusted users (for instance, access to the spectrum or the global positioning system).

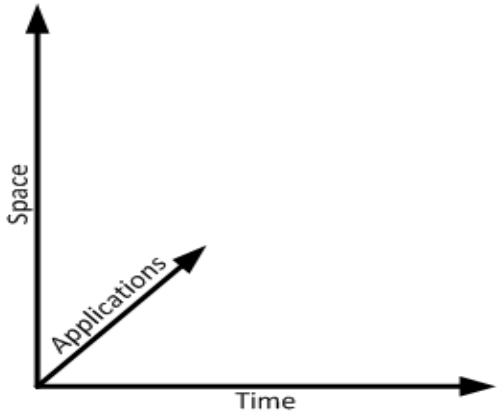


Figure 1: Scope of CCMS Operations

Importantly, PKI is used in many other industries (such as banking, telecommunications, passports, e-commerce, and others). Standards and processes exist that were used by the HTG6 team to inform and guide the analyses. The team relied upon standards, profiles, and processes described by Common Criteria (CC) and the National Institute of Standards and Technology (NIST). These standards are in use by information technology systems around the world. They provide a consistent language and set of common and accepted approaches to identifying, categorizing, and addressing risk.

Overall, the HTG6 analyses have resulted in:

- Recommendations to system developers and integrators that identify technical and policy actions to implement a successful, holistic C-ITS security system.
- Future actions for policy makers, standards developers, and analysts to further clarify relationships, develop standards and policies, and explore and define the remaining gaps.

2.4 Summary Observations and Conclusions

The following summary observations and conclusions can act as a checklist for policy and decision makers and planners. Each observation requires careful consideration for how a C-ITS security solution will be implemented within a jurisdiction. Considerations include:

2.4.1 CCMS Scope

✓ A CCMS operates in a three-dimensional environment (see Figure 1 on the following page). A CCMS's area of responsibility is defined by:

- Geo-political boundaries: interoperability will be needed across borders and some borders will involve less trusted transport areas.
- Time: Security breaks over time, typically within a 5-10 year timeframe. In addition new security installations may be needed because of changes in regulatory frameworks. For every security installation, two operational systems may be needed in parallel to

support evolution.

- Applications: Several applications will need cryptographic solutions that will not be part of initial C-ITS implementations. There are borders to applications, particularly applications that require different levels of trust or have different stakeholders managing them in different environments.
- The long term viability of a given CCMS is dependent on its ability to evolve, in particular with regard to changes in cryptographic processes. The *crypto-agility* of its supporting end entities must support such changes. ***Hardware-based crypto-processors should be discouraged, or designed so as to be easily replaced or upgraded***. Otherwise, end entities could be made permanently insecure in the event of a cryptographic failure.

➔ ***Recommendation: Define expectations associated with boundaries, timeframes, and the level of support for applications that will be required from initial implementation through the lifecycle of a security solution.***

➔ ***Recommendation: Identify how current day design choices may impact the ability to evolve a security solution in the future.***

➔ ***Recommendation: Plan for crypto-agility and system evolution.***

2.4.2 Minimization of the CCMS/Roots

✓ Policy and decision makers, operators, and system designers must plan for a multi-CCMS world with multiple roots. The HTG6 team highly encourages minimizing their number:

- If there is more than one CCMS governance/manager/root, more effort and expense will be required to establish trust from CCMS-to-CCMS.
- Most inter-CCMS interfaces are 1-to-many, so as the number of CCMS increase, the number of implemented interfaces increases in polynomial fashion.
- However, given disaster recovery requirements and expected system upgrades, a CCMS must be defined to exist in an environment where it must communicate with at least one other CCMS, such as the original and a CCMS implemented either as part of disaster recovery, or as part of a system upgrade.
- Notably, CCMS that have different institutional structures are possible, so long as each independently managed component fulfills its requirements, including interfaces to other components in that CCMS.

➔ ***Recommendation: In the planning stages, identify other critical stakeholders and C-ITS users, define common security objectives and needs, and determine the minimum number of CCMS***

required to support a jurisdictional, regional, or national C-ITS environment.

2.4.3 Establishment of Trust Models

✓ There are several distinct degrees to which CCMS may trust one another; establishment and maintenance of this inter-CCMS trust is contingent on the exchange of policy information. HTG6 work defines five trust models:

- ***No Trust***
  - The policy decision to have no trust results in no cross certification of CCMS roots. Each user that desires to use the C-ITS services across jurisdictional boundaries will be required to register in both CCMS (CCMS1 and CCMS2 that will have different canonical certificates). User's end entity devices must receive:
    - Root certificates of CCMS1 and CCMS2 in order to trust messages signed by Pseudonym certificates from the other CCMS
    - Enrollment certificate from CCMS1 and CCMS2
    - Pseudonym certificates from CCMS1 and CCMS2
  - CCMS1 do not trust certificates from CCMS2 and vice versa.
- ***Registration Level Trust***
  - The policy decision to have trust at the registration level also results in no cross certification of roots. Users can be registered only in one CCMS, either CCMS1 or CCMS2. **Importantly, the registration in one CCMS is trusted by the other CCMS.** Thus, a user's end entity device can:
    - Receive an enrollment certificate from both CCMS1 and CCMS2 based on the single canonical certificate registered at one CCMS. **End entity needs to have two enrollment certificates.**
    - Receive Pseudonym certificates from both CCMS1 and CCMS2 based on the enrollment cert of the specific CCMS.
  - CCMS1 only trusts canonical certificates from CCMS2 and vice versa.
- ***Enrollment Level Trust***
  - The policy decision to have trust at the enrollment level also results in no cross certification of roots. User devices can be registered only in one CCMS, either CCMS1 or CCMS2. End entity can have an enrollment certificate from either CCMS1 or CCMS2. **The enrollment in one CCMS is trusted by the other CCMS. End entity needs to have only one enrollment certificate from CCMS1 or CCMS2 but can have enrollment certificates from both CCMS.**
  - End entity gets pseudonym certificates from CCMS1 and CCMS2 based on the CCMS that has issued the enrollment certificate. In the process of requesting pseudonym

certificates the CCMS can verify the enrollment certificate when the enrollment component of the other CCMS is in the list of trusted entities.

- If CCMS1 or CCMS2 have region restrictions then the enrollment certificate cannot be used to authorize the request of pseudonym certificates for another region.

- CCMS1 only trusts enrolment certificates from CCMS2 and vice versa.
- End entity needs to have root certificates of CCMS1 and CCMS2 in order to trust messages and to trust messages signed by pseudonym certificates from the other CCMS

- ***Pseudonym Level Trust***
  - The policy decision to have trust at the pseudonym level requires cross certification of roots or adding root cert of other CCMS to trust store. The User's device must be registered in one CCMS, either CCMS1 or CCMS2; and have an enrollment certificate from one CCMS, either CCMS1 or CCMS2. End entity can receive pseudonym certificates from CCMS1 or CCMS2. In the process of requesting pseudonym certificates the **CCMS can verify the enrollment certificate of every CCMS due to the cross certification of roots or installation of root certificate of other CCMS in trust store**.
    - NOTE: Policy might limit the number of pseudonym certificates that are valid for the same time period and location. If end entity is allowed to request pseudonym certificates from different CCMS then there has to be information exchange to ensure this policy.

✓ Privacy is a fundamental policy requirement, but it is also an implementation choice. The level of privacy protection desired for users within the C-ITS environment is as significant a factor in the design and management/operational policies as the levels of confidentiality, integrity, and availability of the system.

➔ ***Recommendation: At inception, gather CCMS policy makers and managers to determine the trust and privacy levels that will then determine the requirements to share their policies, information, or assets with other CCMS (inter-CCMS trust), with their CCMS entities (intra-CCMS trust), and with other end entities (devices, applications).***

➔ ***Recommendation: Employ the HTG6-5 report to establish organizational decisions about trust and identify inter-organizational agreements and roles; and the HTG6-4 report to guide technical designers in implementing those trust decisions and policies from a technical, interface communication perspective.***

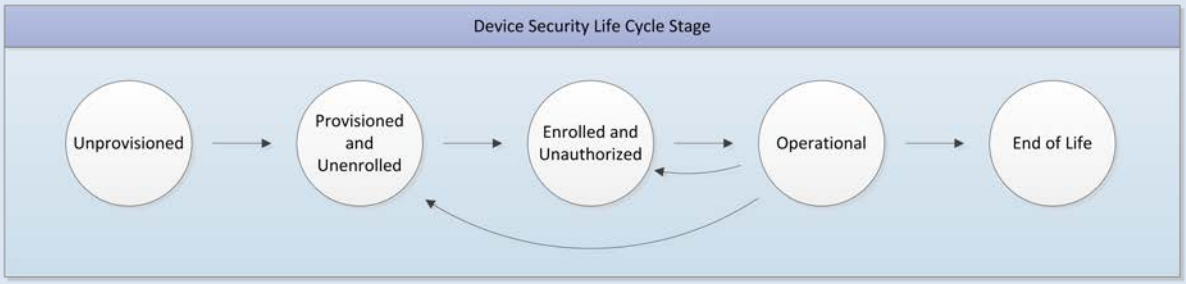
2.4.4 Lifecycle Alignment

- ✓ Lifecycle requirements—both for the CCMS as well as for the end-entity devices/nodes—must be considered and brought into alignment. CCMS lifecycle harmonization is a key factor in enabling ongoing trust and interoperability.
- ✓ Applications and devices have a changing set of relationships depending on the lifecycle stage. In order to frame the discussion of how the CCMS interacts with end entities, it is necessary to define the stages through which an end entity passes. A simplified version of the end entity security lifecycle is depicted in Figure 2 on the following page.
- ✓ CCMS' components interact with end entities at different phases of their lifecycles. There are aspects of the end-entity lifecycle that do not involve direct interaction between the end entity and the CCMS, but about which the CCMS must be informed, and may generate secondary interfaces between CCMS and other systems (for instance, re-certification or conformance testing).

2.4.5 Human Factors and Resources

It is important to remember that the deployment and maintenance of such systems require important investments in human resources, both for the technical aspects and the organizational structures. Requirements must be in place to train and monitor key actors with responsibilities in the CCMS: security auditors, system administrators, appointments, renewal, and handover of key actors.

Figure 2: Definition of Lifecycle Stages



Unprovisioned: The device does not have any cryptographic material or certificates necessary to interact with any parts of the CCMS other than the Provisioning components. Since the end entity is not part of the C-ITS at this stage, it cannot interact in trustworthy fashion with other end entities.

Provisioned and Unenrolled: The device has the cryptographic material and root certificates necessary to communicate with Enrollment components. At this stage the end entity is still not part of the C-ITS and cannot interact in trustworthy fashion with other end entities.

Enrolled and Unauthorized: The device has all the material it needs to communicate with Authorization components. It still cannot interact with other end entities in a trustworthy fashion.

Operational: The device has all the material it needs to communicate with the Misbehavior components, Revocation components, and other operational end entities.

End-of-Life: The device is unable to communicate with any component of the CCMS or other end entities.

➔ ***Recommendation: Agree to change management processes to provide continuation of trust within ongoing operations of the C-ITS security infrastructure. Agreed-upon processes that address the evolving security environment ensure that changes that are made to one CCMS will be compatible with or supported by another CCMS.***

➔ ***Recommendation: Employ the HTG6-4 report to review the use cases associated with the lifecycle of technology moving from one state to another state. The security use cases identify the functions that are needed throughout these transitions.***

2.4.6 Roles and Responsibilities

- ✓ The HTG6 team analysis resulted in the definition of a proposed set of roles and responsibilities associated with access policies for critical ITS resources and enforcement.
- ✓ The definitions were derived from the analysis of the key, critical assets of a C-ITS environment, and which assets required access from trusted actors within the system and how that access would be protected or when enforcement would need to be applied, if necessary.
- ✓ An important insight from this effort was to identify the role of the CCMS in acting as a "gatekeeper" that provides access to C-ITS environments. To become a trusted actor within the environment, a device or an application will require certification or demonstrate conformance. In this situation, certification requirements can be linked to initial decisions about the levels of security to be provided as well as the levels of trust that are to be enabled.

➔ ***Recommendation: Employ the list from HTG6-5 to determine the scope of responsibilities for regulators, device manufacturers, application developers, service providers, certifiers, and system designers (or specifiers).***

2.4.7 International CCMS Harmonization

- ✓ In a multi-CCMS world that supports a global transportation marketplace, trust will need to be defined beyond jurisdictional boundaries. The HTG6 team's analysis found a need for an international association, or federation, of CCMS managers to:
  - o Confirm the findings and recommendations within these reports
  - o Further develop policy language associated with the proposed policies
  - o Share best practices and lessons learned
  - o Take ownership of these documents as well as standards to ensure that they are updated and evolve as needed
  - o Define metrics for and accredit new CCMS entities
  - o Assist in mitigating cascading effects when additional security systems emerge, including the sharing of critical information about the risks of the new C-ITS environment and the implementation of controls, levels of trust, and policies.

2.5 High Priority Areas for Harmonization

The following areas were identified in the course of the HTG6 analysis to be the high priority areas for security policy harmonization.

➔ ***Recommendation: Harmonize security policies in the following core areas to ensure trust and interoperability:***

2.5.1.1 Cryptographic Material

- ✓ **Cryptographic material (credentials/certificates/keys) distribution and injection:** The key security objective here is to ensure confidentiality and integrity in the distribution of cryptographic material. Given the importance of confidentiality in cryptographic material distribution, this is something that will affect cross-border activities and hence should be harmonized. As an example, the technical guidelines for the distribution channel used to install the initial credentials for Enrolment in the telematics equipment should be harmonized.

  As long as the distributed cryptographic material is still valid, the absence of harmonized security policies in the area will have a limited negative impact on interoperability. However, the absence of harmonized policies can have a significant impact on organizational trust among different CCMS. If the protection of the cryptographic material is uneven among CCMS, the levels of security risk for different CCMS could differ, negatively affecting organizational trust, because one CCMS may consider the security measures of another CCMS to be inadequate for establishing a trust relationship. The lack of harmonization in this area also impacts costs for Original Equipment Manufacturers (OEMs) because they will need to implement multiple distribution channels.

- ✓ **Generation of cryptographic material (credentials/certificates/keys):** A problem in the generation of cryptographic material for different levels of the CCMS (from the CA to the telematics devices for temporary keys) could create significant security breaches and have far reaching impacts. For example, a malicious entity could implement denial of service attacks by overloading the certificate generation process. While some processes and choices of technologies can be local, common best practices and guidelines can be useful for manufacturers and service managers. Using different processes for the generation of cryptographic material at the lower layers of CCMS (e.g., in the vehicle or telematics systems) could also negatively impact interoperability. Another example: key generation might be similar to a product recall where the impact is quite material leading to availability issues. Additionally, confidentiality is potentially at risk with poor harmonization. Consideration should be given as to whether there should be harmonized applications/standards that key generation is done against to reduce these issues.

  This is a high priority issue and may require significant levels of harmonization. Lack of harmonization could have a negative impact on the interoperability for the case of cryptographic material generated at the lower layer (networks, car, or telematics devices) as in the case of temporary keys to protect privacy. Organizational trust can be significantly damaged if the key generation processes and technologies differ significantly between CCMS, because one CCMS may be more vulnerable to malicious attacks. If policies and processes related to the

generation of cryptographic material are not harmonized in the beginning, attempting to do so later risks that the cost will be high, if not prohibitive. Such costs could include redesigning and redeploying the components that generate cryptographic material.

- ✓ **Cryptographic material storage:** The cryptographic materials (credentials/certificates/keys) that are key components of PKI, may be distributed across back office systems and devices. As an example, cryptographic material in the form of private keys within certificates could be stored in a back office system where each certificate is then injected into a device. Access to cryptographic material storage negatively impacts the integrity of the privacy protection. Storing cryptographic material in multiple locations across different stages in the lifecycle of devices increases the risk of security breaches by the creation of multiple site requiring protection. To ensure cross-organization trust, the privacy needs of users must be met by ensuring that cryptographic material storage in each organization conform to agreed standards that meets the needs of all organizations. The use of different standards for cryptographic material storage can result in a lack of trust and privacy, ultimately leading to increased cost and decreased levels of interoperability. Practically, this means there should be agreement between CCMS Managers on the level of security.

  This is high priority, primarily due to the need for organizational trust that is based upon agreed levels of security. Inter-organizational trust can be significantly threatened if differing cryptographic material storage approaches result in appreciably different levels of security. Therefore, adoption of applicable standards is recommended. Since most aspects of cryptographic material storage are isolated, interoperability is not an issue. Cost impacts from a lack of harmonization will be minimal because the interoperability requirement is insignificant.

2.5.1.2 CCMS Components

A CCMS is complex and has many components that have security requirements. This section discusses: Certificate Authorities (CAs), Registration Authorities (RAs), and Ceremony Rooms. In all cases, oorganizational trust can be negatively affected by uneven policies or processes, because a CCMS may consider those of another CCMS to be inadequate for establishing a trust relationship.

- ✓ **Certificate Authority (CA)** A CA derives its authority from the trust anchor for the PKI, designated as the "Root CA," and issues security certificates to other credential management entities in the CCMS in accordance with system policies and procedures. These concerns could affect cross-domain (e.g. a state road authority trusting certificates issued by an aftermarket device manufacturer or car manufacturer) as well as cross-border (inter-jurisdictional) trust.
  - o **Data Center Management:** Vulnerabilities due to diverse CA Data Center Management processes could be significant and lead to a break down in trust. Lack of harmonization has a limited negative impact in interoperability until the PKI services are supported.

There may be a negative impact on costs in case of security breach or for the restructuring of the processes technologies in case harmonized policies are requested in a second phase.

- **Processes and Procedures:** This topic includes all the processes and procedures for CA setup and management apart from those considered in other sections (e.g., Data Center management, Audit, storage of Cryptographic material), which are addressed in other sections. The security objectives are diverse. The level of compromise that could occur through diverse CA processes and procedures is significant and could lead to a break down in trust across borders. This may also occur locally with regard to trust between entities within the same border. Organizational processes and procedures are a critical component to PKI security and the integrity of such an integrated and interdependent environment is paramount to this. The reference to standards may be suitable. Lack of harmonization will only impact interoperability once the PKI services are supported. There may be a negative impact on costs in case of security breach or for the restructuring of the processes technologies in case harmonized policies are requested in a second phase.

✓ **Registration Authority (RA)** The RA checks that requests for security certificates come from entities that are entitled to them and processes those requests. Within an anonymous environment, there is a higher reliance on the registration process to ensure correct issuing of certificates. Within an identified environment, maintenance and accuracy of registration information, not to mention the higher privacy obligations, will be important.

- **Data Center Management:** The level of compromise that could be achieved through diverse RA Data Center Management is significant and could lead to a break down in trust across jurisdictions. The risk of compromise on a large scale varies with the amount of information collected and its potential value. Although harmonization is important to guarantee an adequate level of trust, the recommended level of harmonization for interoperability of data centers is low because RA Data Centers are usually functionally and physically separated. Adherence to standards may be sufficient. Noting the possible value of information contained within the RA and the potential impact, both locally and cross-border, of a breach, harmonization could provide the comfort needed to drive the trust relationships between entities. Similar to the CA Data Center Management, lack of harmonization has a limited negative impact on interoperability until the PKI services are supported. There may be a negative impact on costs in case of a security breach or if redesign of the RA data centre management is required in a subsequent phase.
- **Processes and Procedures:** This topic includes all the processes and procedures for RA setup and management apart from those considered in other sections (such as, data centre management, audit, and storage of cryptographic material). The level of

compromise that could occur through diverse RA Data Center Management is significant and could lead to a break down in trust across jurisdictions. The risk of privacy breaches varies with the extent of information contained and its potential value. This could lead to compromise on a large scale. Organizational processes and procedures are critical to the security of the PKI. The integrity of such an integrated and interdependent system depends on this.

Lack of harmonization has a limited negative in interoperability until the PKI services are supported. There may be a negative impact on costs in case of a security breach or if redesign of the RA processes and procedures is required in a subsequent phase.

- ✓ **Ceremony Room Management/Entity Credential:** The Ceremony Room is used for signing and verification of root certificates. Signing is akin to executing a contract. A Ceremony Room provides an offline environment where this can be done in a highly secure and controlled manner. Root CAs often issue certificates in a physical manner (often on some type of secure media) and then the certificates are transported to a subordinate CA. Each CA receives its authorization to issue certificates from the CA directly above. While issuing CAs are typically online, the root CAs are often offline and this requires a physical rather than online exchange. This is performed in the Ceremony Room in cases where a high level of security is required. Standards for a Ceremony Room are well established and are used internationally. While there may not be a need for this to be a harmonized function, the need for organization trust here will drive some level of harmonization. There may be legal aspects that require consideration in relation to the Ceremony Room. For example, if the signing of a root CA is compromised through poor controls with regard to the use of the Ceremony Room where this process is carried out, and this is identified after the root CA issues certificates, there will be a requirement to revoke the root CA certificates and re-issue, a process that will impact all subordinate certificates in the tree, resulting in significant cost and logistical challenges that would be best avoided.

  The Ceremony Room is a critical point of interaction between two organizations that wish to establish trust. Importantly, as it impacts the “exchange of a contract” between CCMS Managers (and between two CCMS), there must be agreement between organizations on required standards. This is required up front to avoid significant logistical issues if there needs to be changes to the root certificates in the future due to their integrity. There are available standards relating to a Ceremony Room and additionally, the Statement of Auditing Standards 70 (SAS 70) may be applicable. The level of harmonization is high to ensure that the integrity required by the organizations is established and maintained. While this does not assume a Ceremony Room is mandatory, it is a well-known and widely used method of establishing offline CAs and if it is used, or an equivalent is implemented, this requires very high levels of harmonization. It should

also be noted that there may only be a limited number of Ceremony Rooms and these could be provided by third parties.

2.5.1.3 Organizational Trust

- ✓ **Audit:** Audit procedures and technologies have the objective of identifying non-compliances and non-conformances in the PKI architectures and services. A harmonized set of best practices and standards for the Audit function could be useful to ensure a high level of quality in the Audit process. While some aspects of the Audits are related to local implementation and deployment aspects (e.g., configuration of the databases), a common set of standards could be used as a reference.

  A common set of standards could be adopted to support a high level of quality in the Audit process. The lack of harmonization of the audit processes can negatively impact the organizational trust, because the processes designed or applied by one organization may not be sufficient to meet the expectations of another. Impact on interoperability and costs are low unless the redesign of the audit processes is required in a subsequent phase.

- ✓ **Vetting and Certification of Organizations:** Vetting and certification of organizations is important to guarantee specific levels of trust among different domains or geo-political areas. If different processes or policies are defined for vetting of organizations, it may increase the risk of generating different levels of trust for essential services related to Key/certificates generations.

  Lack of harmonized practices for vetting of organizations could lead to unbalanced levels of trust and quality which can impact the mutual trust across PKI architectures in different domains (e.g., commercial vehicles/consumer vehicles) or bordering geo-political areas (e.g., Europe, Russia, Africa). The impact on interoperability and cost is low.

- ✓ **Cross Certification (e.g., among different CAs):** If there are 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 deals with this need to form trust relationships between formerly unrelated PKI installations. Support for cross certification can be divided into the following categories:
  - o Protocols for implementing cross-certification (interoperability)
  - o Harmonization of policies and practices that make cross-certification trustable. For example, to which policies and practices PKI architecture must conform to be trusted.

  Cross-certification in C-ITS can arise both because there may be a CA/RA from different domains (commercial vehicles and consumer vehicles), from different set of applications (regulated applications and commercial applications) or from different regions (e.g., Canada, USA or

Europe and AETR). It is important to guarantee cross-certification among the different CA/RA to support interoperability and internetworking of C-ITS in the field. Lack of harmonization could lead to security breaches or lack of mutual trust.

Lack of harmonized practices for cross-certification may also lead to trust and security challenges. This can be an issue especially when new PKIs will be connected or interface with each other. Lack of harmonization can have a strong, negative impact both on interoperability and organizational trust, because specific PKI services/processes (e.g., revocation) may not work, or may offer low quality service if the cross-certification processes are not harmonized. For example, the notification about the revocation of a specific certificate among different PKIs could be complex or slow to execute if the related processes are quite different. This will impact interoperability in the field. Organizational trust will also be impacted because different PKI managers may not accept different or poorly defined processes. The negative impact on costs of a lack of harmonization is limited unless it requires a re-design in subsequent phases.

2.5.1.4 Additional Privacy and Security Protections

- ✓ **Data Authentication and Integrity:** ITS applications will be based on the exchange of data among the elements of the CCMS. The integrity of data, the authentication of the data sources and the mutual trust among the elements of CCMS are essential to support the ITS applications.

  A common policy should be defined to guarantee a basic level of security functions to support the exchange of data used to support ITS applications. For example, location information should come from a trusted source (e.g., GNSS receiver) and be distributed to other elements of the ITS system in a way that supports its integrity. Harmonization of the policies in this area could support both interoperability and organizational trust. Lack of harmonization may reduce mutual trust especially for ITS applications, which have to work cross-border. In addition, lack of harmonization could negatively impact interoperability if security functions like integrity and authentication are implemented in different ways.

- ✓ **Header/MAC information:** Wireless communication standards could make visible (e.g., send in clear) header/MAC information, which could be linked to the identity of the user or the vehicle. Privacy can be impacted if header information in the wireless communication standards is transmitted without encryption and if it is linked to the user or directly or through the identity of the vehicle.

  A common policy should be suggested to avoid the risk to link header information with the user of the vehicle. Lack of harmonization could have a serious impact on interoperability in the field because telematics systems would use different wireless communications standards and they would not be interoperable. Organization trust could also be impacted with an increased risk to

the privacy of the user. Cost could be negatively impact to implement specific Privacy Enabling Technologies (PET).

- ✓ **Electronic and Physical Security of Telematics Devices:** Even if the wireless communication (e.g., DSRC) could be made secure, the end-point of the connection, like the telematics equipment in the vehicle or the infrastructure, may not be secure, which can generate severe security breaches. Physical or electronic security of the telematics devices could be an important factor to support the overall security and integrity of the ITS systems as these devices often represent the end points of the communication. Definition of a harmonized policy (which could link to a set of standards) could support trust between different CCMS.

  A common policy should be defined to guarantee a minimum level of security of the telematics devices to support mutual trusts in a CCMS or among CCMS. Negative impact on costs or interoperability is limited.

- ✓ **Secure Time Stamping:** Secure Time Stamping is a function needed to ensure that the artefacts are time stamped correctly and accurately. For example, the lifetime of the certificates is based on a correct time-stamp. In a similar way to other domains (smart grids, telecom networks), the synchronization of the time sources is essential to support interoperability and internetwork among different infrastructures. Harmonization could be focused on the definition of common calibration and synchronization procedures and the identification of common time sources (e.g., GNSS based).

  Lack of harmonized practices for time-stamps could impact interoperability and internetworking among PKI architecture or the C-ITS (e.g., certificates). Interoperability could be impacted especially for keys/certificated, which are frequently generated (e.g., pseudonyms certificates). Organization trust and cost are not impacted significantly by harmonization because the risk of significant security breaches is low and the cost of time-stamping solutions is low.

- ✓ **Certification and Bootstrap**: Certification and bootstrap includes the processes and technologies used to support the certification, installation, activation and registration (or Enrolment) of devices for CCMS. For example, this may include the certification of On Board Units and their subsequent installation and activation on a vehicle. We recommend harmonization of certification and bootstrap policies. This will support the vehicle and telematics manufacturers, who otherwise would have to deal with different requirements in the various jurisdictions they serve. If bootstrap and certification policies are not harmonized, the challenge of meeting a wide range of requirements could limit the deployment of C-ITS and related functions (communications, positioning, security). Additional benefits are realized as well. The harmonization of these processes can also improve mutual trust between C-ITS (e.g., ITS

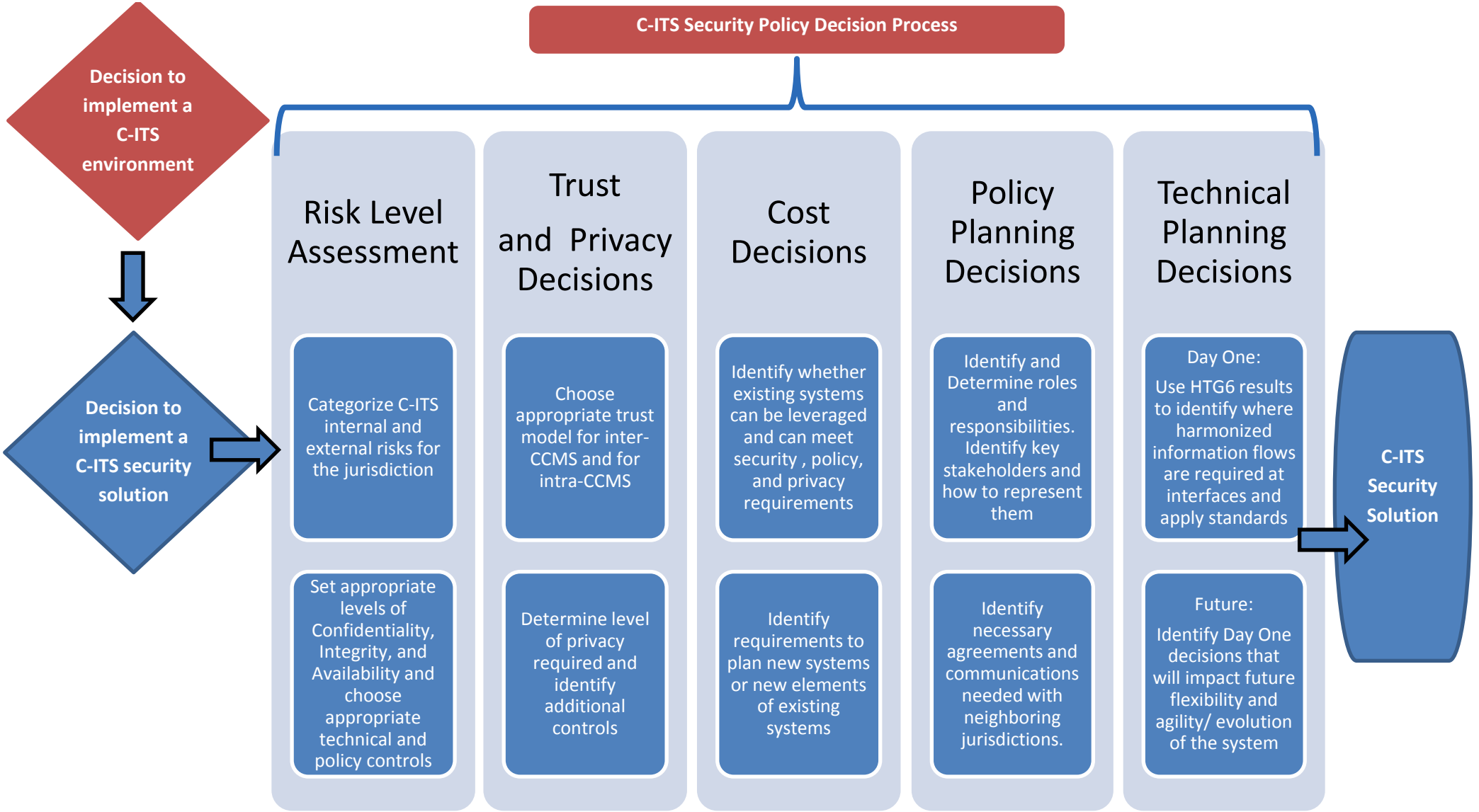
station), because they will be conformant to well defined best practices, which are designed to a high level of quality. Changes to the certification and bootstrap processes on a global scale will be easier to implement because they will be based on a harmonized basis of best practices.

Lack of harmonization will not significantly impact interoperability. Lack of harmonization can have a high impact on organizational trust, because uneven processes for bootstrap can make CCMS more vulnerable to others to security breaches with the consequence that CCMS may not trust each other. Lack of harmonization can also have a high impact on cost for manufacturers, which will have to implement different processes for installation and certification in different geopolitical areas. In addition, uneven processes can increase the risk of security breaches. Because bootstrap is one of the most critical phases in ITS, a security breach can have a major impact on the deployed systems/vehicles. For example, recall may be needed for an update of the cryptographic material (i.e., when Over the Air is not possible).

2.6 Decision Process

Building on the summary conclusions and observations, the HTG6 team identified a decision process that supports policy and decision makers in the early stages of planning for C-ITS security implementation. Figure 3 on the following page proposes a set of steps to guide planning and policy decisions.

Figure 3: C-ITS Security Policy Decision Process



2.7 Gaps and Recommended Future Actions

The collective analysis of CCMS and policy requirements led to conclusions about additional actions needed to address gaps:

- Existing CCMS designs incorporate much of the required functionality of a comprehensive CCMS. However, neither surveyed design has addressed many of the inter-CCMS communications aspects identified in this analysis. Neither has the standards community described the relevant interfaces. ***This lack of interface specification is among the biggest issues confronting CCMS designs and the long term C-ITS deployment.***

- Equally important, ***device and application certification processes, whatever they may be, are linked with credential management, and as such must be considered concurrently with the architecting of security management systems and procedures.*** There are other issues however, such as ***resource management, CCMS policy management, and CCMS scoping,*** which also need to be further addressed.

- Crypto-agility needs further definition. It is intimately tied to processes associated with system maintenance and evolution. ***Further research is needed to define options and use cases. Additionally, analysis is needed to identify how "day-one" decisions will impact future decisions and potentially constrain or support future system flexibility or evolutionary choices.***

- There are a large number of inter-CCMS interfaces. In order to ensure consistency and scalability, the ***C-ITS community should develop standards to codify the interfaces between CCMS.***

- Certification of applications and devices, including the ways that ITS resources are accessed, is linked with the granting of digital credentials. Credential distribution and certification are distinctly different functions that may benefit from different operational, institutional structures, but since they are linked the requisite relationships are important to the overall success of C-ITS. ***A future harmonization activity should clarify the relationship between certification and credentials distribution.*** Absent harmonization, each implementer will have to perform this analysis, making inter-CCMS trust unlikely.

- Devices and applications have a lifecycle, and in some phases of that lifecycle they have no relationship to the CCMS, i.e., prior to provisioning and subsequent to end-of-life. There are security-related policy concerns with how these end entities are handled in the times when they do not have a CCMS relationship. ***The C-ITS community should establish requirements defining how end entities must be engineered, manufactured, and handled in order to obtain credentials, and establish shared requirements for proper disposal.***

- CCMS Components are responsible for managing the policies governing their operation, and disseminating that policy information to users. This sounds self-evident, but what it means is

that the institutional framework governing the CCMS component is affected by and affects the technical design. Making changes to one has a causative effect on the other. This also implies something about how CCMS enter into trust relationships with one another. Depending on how much CCMSs trust one another, their policy frameworks must be compatible, and may need to be identical. The ripple effect here is that if one CCMS changes policy, it jeopardizes the trust relationship between CCMSs. ***The CCMS management community should collectively define CCMS policy frameworks. Further, the C-ITS policy makers should determine the value and structure 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.***

- Last, there are several likely-viable Inter-CCMS trust scenarios, and they have significantly different implications for the architecture and management of CCMS. ***Inter-CCMS trust scenarios need additional study.***