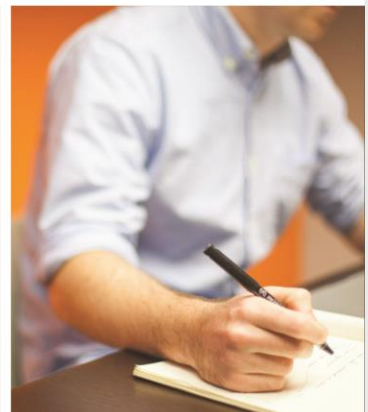
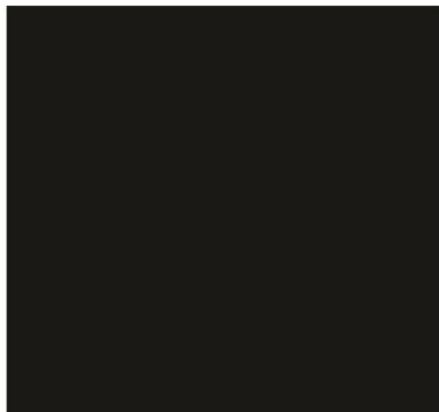
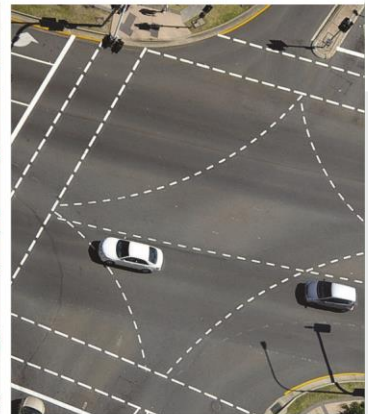
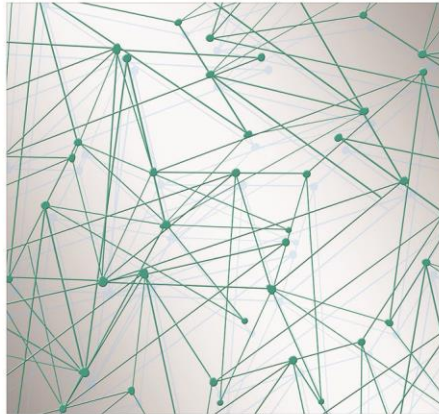


KEY DECISIONS TO PROGRESS AUSTRALIAN DEPLOYMENT OF A SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS)



© Transport Certification Australia Limited 2018.

This document has been published by
Transport Certification Australia Limited.

This document is copyright. Apart from any use as
permitted under the Copyright Act 1968, no part may
be reproduced by any person or process without the prior
written permission of Transport Certification Australia Limited.

Transport Certification Australia Ltd

T +61 3 8601 4600

F +61 3 8601 4611

E tca@tca.gov.au

W www.tca.gov.au

ABN 83 113 379 936



Document Details

Title	Key Decisions to Progress Australian Deployment of a SCMS
Document Number	TCA-B067
Version	1.3
Version Date	January 2018
Printing Instructions	Double sided, colour

Document History

Version	Date	Description
1.0	May 2017	Confidential release for stakeholder representatives
1.1	September 2017	Incorporation of feedback from stakeholder representatives
1.2	October 2017	Limited release (to TCA Members)
1.3	January 2018	Public release

Transport Certification Australia Limited believes this
publication to be correct at time of printing and does not
accept responsibility for any consequences arising from the
use of information herein. Readers should rely on their own
skills and judgment to apply information to particular issues.

TCA™, Transport Certification Australia™, TCA National Telematics
Framework™, TCA Certified™, TCA Type-Approved™, Intelligent Access
Program™, IAP®, IAP Service Provider™, IAP-SP™, In-Vehicle Unit™,
IVU™, Electronic Work Diary™, EWD™, On-Board Mass™ and OBM™
are trade marks of Transport Certification Australia Limited.

This document is public

EXECUTIVE SUMMARY

Intelligent Transport Systems (ITS) refer to a broad range of information and communications technologies used across the transport network.

Cooperative Intelligent Transport Systems (C-ITS) build on the capabilities of ITS, and enable real-time wireless communication between vehicles, roadside infrastructure, mobile devices and back-office systems. C-ITS have the capability to deliver a safer and more efficient transport network that is less congested and more environmentally friendly.

Examples of C-ITS applications include information and alerts about the speed and location of other vehicles, collision and hazard warnings, alerts for pedestrians, and real-time information about changed traffic conditions due to congestion, road closure and weather.

C-ITS – also commonly referred to as connected vehicles, and vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-elsewhere (V2X) connectivity – will see the progressive introduction of connected systems that will change the way transport networks function and how they are managed. Widespread C-ITS adoption will progressively link vehicles and infrastructure to build real-time situational awareness, increasing the safety and productivity of the transport network.

C-ITS are a critical part of the disruptive transformation occurring to our vehicles, roads, cities and technologies – including automated vehicles, smart cities and smart infrastructure, and the Internet of Things (IoT).

They are part of the same paradigm shift in the connectivity of people, systems and services – they will *co-exist*, *co-develop*, and *interconnect*.

Providing security for this new environment has emerged as one of the key deployment and ongoing challenges.

A commercially sustainable global market for C-ITS will not be possible without security, and neither will safety nor true connectivity.

The broad goals of security are two sides of the same coin. Security needs to:

- **Protect** against threats that can *deny*, *degrade*, *disrupt* or *destroy* technical, organisational, commercial, privacy and safety services, settings and assurances
- **Enable** public purpose and commercial outcomes to be realised.

A C-ITS deployment without adequate security may be one in which:

- **Safety is threatened** – by lapses in standards or misbehaving C-ITS devices (both malicious and unintentional)
- **Privacy is compromised** – by hackers and malicious behaviour, or inadequate policies and processes surrounding access to data
- **Efficiency is compromised** – by unclear roles and responsibilities, or inadequate governance

- **The market is not supported** – security will need to cater for new and old devices, using different communications methods (Wi-Fi, Bluetooth, etc.), from a global market of vehicle manufactures, mobile phone suppliers, etc.
- **The needs and expectations of users are not met** – users will need and expect their C-ITS devices to work seamlessly and safely across regions. Security facilitates required levels of interoperability and trust.
- **The needs and expectations of Road Managers are not met** – governments and other operators (such as toll road operators) will not have required or anticipated levels of control, or ability to provide services.

The security solution for the connected, C-ITS environment that has emerged out of international collaboration is called a Security Credential Management System (SCMS).

A SCMS is not one single thing. Rather, it is:

- An operational framework with defined interactions and actors
- A business model
- An operational environment
- A piece of infrastructure
- A collection of people, processes and policies
- An assemblage of highly advanced technological systems, technologies and management practices
- Within one or more organisational structure.

The SCMS is a central pillar to enable security across systems, and is fundamental to a C-ITS deployment.

A SCMS is not just a technical system. Nor is it an off-the-shelf product or a ready-made solution. A SCMS is both an institutional framework and a piece of infrastructure, encompassing human/management, electronic and physical elements – it is ‘cyber-physical.’

Like any piece of infrastructure, its development needs to be approached as a long-term investment: the product of careful policy, planning and consideration as to its capability and longevity, and the organisational elements necessary to operate and maintain it.

This document presents a detailed, yet high-level discussion of the core issues at hand to progress Australia’s deployment of the SCMS.

While touching on a breadth of key decisions, two themes are common, and cut across and unify these decisions:

- The benefits of national collaboration and agreement on key issues
- The importance of progressing decisions relating to management of the SCMS to provide technical and operational advice to implement these key decisions.

The designers of the United States SCMS – and inventors of many of its novel aspects – capture the necessity of careful policy planning, technical expertise, and – critically – ongoing management:

[The SCMS] is distinguished from a traditional PKI [Public Key Infrastructure – the framework for the SCMS] in several aspects, the two most important ones being its size (i.e., the number of vehicles that it supports) and the balance among security, privacy, and efficiency. At its full capacity, assuming 300 million vehicles, it will issue approximately 300 billion certificates per year. The largest current PKI, deployed by the US Department of Defence, is several orders of magnitude smaller and issues under 10 million certificates per year.¹

The Australian C-ITS deployment will not be nearly as big as that of the United States but the quotation captures the necessity of:

- Getting it right from the outset – from a policy making and technical perspective: retrofitting the system will be difficult and expensive
- Having a management entity to guide this process: the SCMS Manager translates government policy into technical and operational processes, systems and policies; and ensure and, where necessary, enforce compliance.

Purpose of This Document

The purpose of this document is to present the key decisions for progressing the development of a SCMS in Australia.

Although it isolates issues specific to the SCMS, where necessary, the document points to developments in C-ITS more broadly, given that one cannot exist without the other, and developments in one area will impact and be impacted by the other.

The SCMS is a highly specialised area, drawing on established and bespoke cybersecurity strategies and techniques, progressed in unison with the latest advancements in intelligent transport technology.

This document intends to contribute to an existing body of knowledge, and to facilitate national collaboration on security management for connected vehicles.

The document restricts the discussion to issues that require the attention of policy and decision makers, since technical decisions for the SCMS can largely be progressed once key decisions or intentions are made clear.

The SCMS will be a highly sensitive and responsive system comprising people, technical and operational processes and policies, and its overall composition and operation will be designed to translate the Australian policy environment into security outcomes. This means that the discussion can take place at a relatively high level, without sacrificing complexity. Technical insights and concepts are defined and described where necessary, so that readers can make informed decisions.

¹ Whyte, W., Weimerskirchy, A., Kumar, V., Hehn, T. 2013. *A security credential management system for V2V communications*. Conference paper. Available from William White, Security Innovation, Inc.

The goal is to capture the need for decision making across the following domains:

- **Policy:** what rules are needed to provide guidance for the SCMS, to protect users and businesses, and who makes them?
- **Technical:** what should a SCMS do, and how should it do it?
- **Operational:** how will the SCMS work in the real world, today, tomorrow and into the future?
- **Commercial:** what are the commercial decisions required for the SCMS, the impacts to government and industry, and who will benefit?

Context

Australia's C-ITS and SCMS deployment is dependent on aligning with and adopting international standards and best practices.

This document points out where international progress is sufficiently advanced, such that Australia is able to initiate decisions that will progress the SCMS – and by extension, C-ITS – without compromising Australia's immediate or future security and operational capabilities, public and private interests, or reputation.

Indeed, decision making in these areas can be expected to bolster these.

This document therefore draws on the international context in which SCMS security strategies, concepts and tools are being developed, and international developments in the broader area of C-ITS.

Through TCA, Australia has taken a co-leadership role in the creation of the SCMS concept by working collaboratively with the United States and Europe on international Harmonisation Task Groups (HTG).²

Building on this work, in September 2016, TCA published (and invited feedback on) a document titled *Discussion Paper: Towards a national vision for a secure, connected future through Cooperative Intelligent Transport Systems (C-ITS)*.³ Included in the *Discussion Paper* was a set of initial SCMS requirements.⁴

² HTGs bring together and draw on the expertise of vehicle and equipment manufacturers, technical standards development organisations, and government bodies. The overall aim is to benefit government agencies, technology and vehicle manufacturers, and transport system end-users by improving interoperability of C-ITS across local and international borders, reducing development and deployment costs, and increasing access, competition and innovation in the market.

³ Available at http://www.tca.gov.au/publications_and_reports. The paper was also published on Australian Policy Online, available at <http://apo.org.au/resource/towards-national-vision-secure-connected-future-through-cooperative-connected-transport>

⁴ These initial requirements were informed by the needs and outcomes identified internationally for a SCMS. These requirements are initial, insofar as they assume that necessary policy decisions will be made for C-ITS and for the SCMS, but do not assume the direction or implementation specifics of these policy decisions for the Australian deployment.

How This Document Works

After establishing the conceptual terrain, the Strategic Policy Context section of this document identifies forthcoming actions falling under the National Policy Framework for Land Transport Technology (Transport and Infrastructure Council, 2016) that will affect the Australian SCMS deployment.

Given the importance of developments in Europe and the United States, these are factored into and inform both the context and specifics of the discussion.

This document highlights where key decisions may be progressed in unison with the Framework, or as part of it.

The key decisions presented in this document span the entirety of the SCMS. While they may trigger its development, implementation and deployment, they will also have significant ongoing impacts on SCMS management and operations. That is: they will impact the ability of the SCMS to provide security support and services that deliver policy outcomes, and meet user expectations and needs.

The key decisions identified in this document are classified by their:

- *Primary domain*: whether the decision logically sits (policy, technical, operational, commercial)
- *Type*: which aspects and functions of the SCMS will be established or guided by the outcomes of the decision.

These are followed by:

- The key decisions themselves
- The urgency with which this report has identified they are in need of action.

Bounded by Australian and international contexts, the content of the document therefore proceeds from the general to the particular as shown in Figure 1:

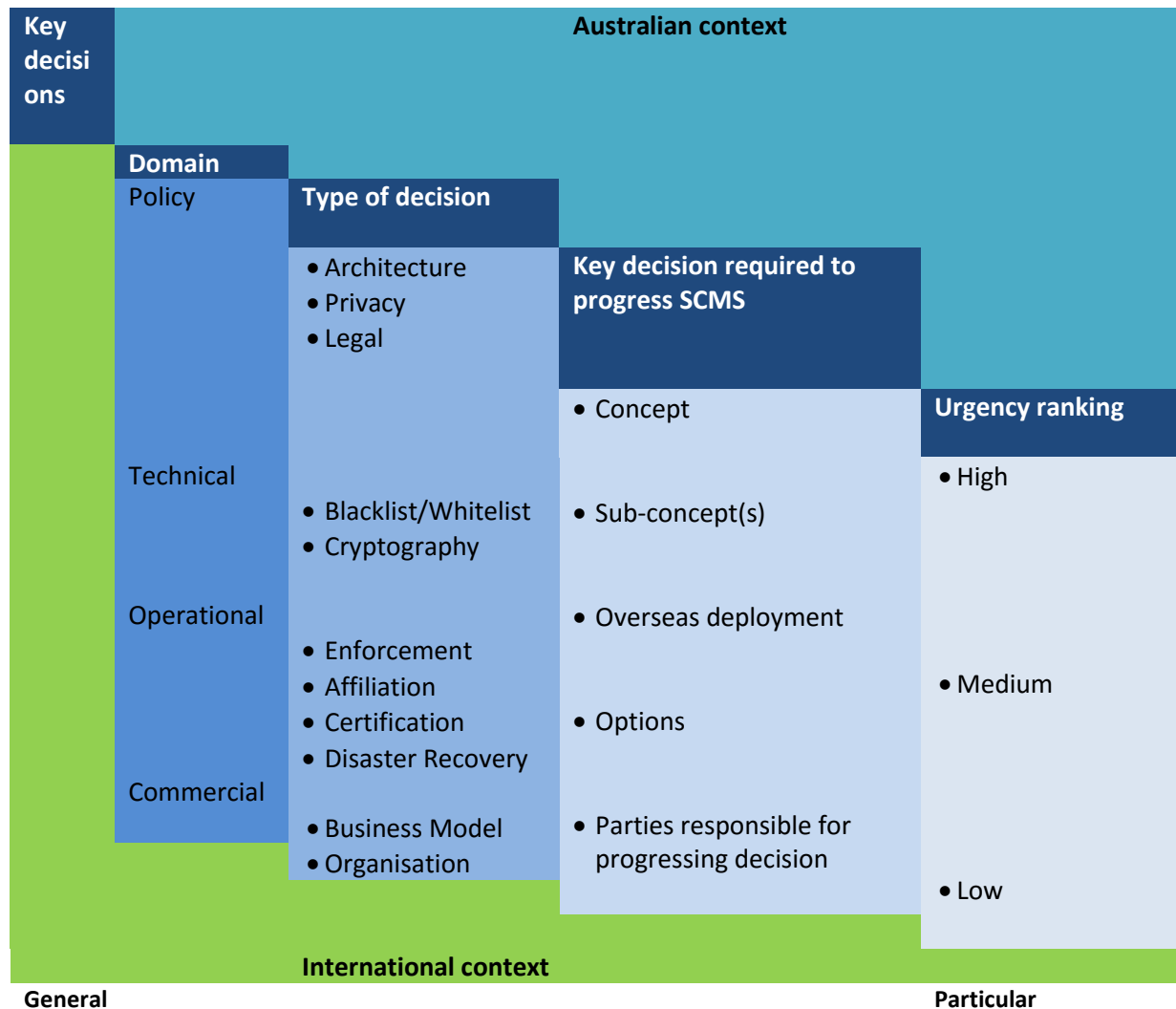


Figure 1 How This Document Works

Table 1 below maps out the structural logic of this document, and how it groups and classifies decisions into:

- Domains
- Types of decisions involved in the domain
- Aspects specific to the SCMS affected by the decision type
- What this document provides.

Table 1: Structural Logic of Document

Key decisions	Policy	Domain role		WHAT THIS DOCUMENT PROVIDES
		Establish rules needed to provide guidance for the SCMS, to protect users and businesses, and who makes them		
		Types of decisions	SCMS specific	
		<ul style="list-style-type: none">• The underpinning architecture and deployment of the SCMS• How information is gathered, distributed, used and destroyed in a way that it both optimal and compliant• How vehicles will enter the connected SCMS security environment• The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in ensuring this.	<ul style="list-style-type: none">• Architecture• Privacy• Legal	
	Technical	Domain role		
		Establish what the SCMS should do, and how it should do it		
		Types of decisions	SCMS specific	
		<ul style="list-style-type: none">• How to mitigate risk, and protect the security and safety of users• How information is protected and able to be exchanged, and how user ability to be trusted is confirmed.	<ul style="list-style-type: none">• Blacklist/Whitelist• Cryptography	
	Operational	Domain role		
		Establish how the SCMS will work in the real world, today, tomorrow and into the future		
		Types of decisions	SCMS specific	
		<ul style="list-style-type: none">• How to mitigate risk, and protect the security and safety of users• How political alignment and engagement can shape technical decisions to boost international cooperation• The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in supporting this• The ability to offer uninterrupted support during disaster or upgrade.	<ul style="list-style-type: none">• Enforcement• Affiliation• Certification• Disaster Recovery	
	Commercial	Domain role		
		Establish the commercial decisions required for the SCMS, the impacts to government and industry, and who will benefit		
		Types of decisions	SCMS specific	
		<ul style="list-style-type: none">• Decisions underpinning initial and ongoing economic and organisational composition and viability of the SCMS• Nominating the entity who will translate the policy environment into SCMS technical policy design and operations, ensure compliance, and engage national and international SCMS stakeholders.	<ul style="list-style-type: none">• Business Model• Organisation	

Concept

A high-level explanation of the primary concept in this domain, and why it is important to progressing the SCMS.

Sub-concepts

Many of these decisions and their concepts need to be broken down into more manageable concepts and decisions.

Overseas deployment

Because Australia depends on aligning with and adopting overseas developments, the similarities and differences between the United States and European deployments are identified and explained.

Options

A discussion of the options available to policy and decision makers, measured against overseas deployment plans, and any progress in Australia.

Parties responsible for advancing decision

Identifies logical stakeholders, the desirable or necessary level of discussion (national, jurisdictional, overseas) and parties involved in ongoing decisions and operations.

WHAT THIS DOCUMENT PROVIDES

Concept

A high-level explanation of the primary concept in this domain, and why it is important to progressing the SCMS.

Sub-concepts

Many of these decisions and their concepts need to be broken down into more manageable concepts and decisions.

Overseas deployment

Because Australia depends on aligning with and adopting overseas developments, the similarities and differences between the United States and European deployments are identified and explained.

Options

A discussion of the options available to policy and decision makers, measured against overseas deployment plans, and any progress in Australia.

Parties responsible for advancing decision

Identifies logical stakeholders, the desirable or necessary level of discussion (national, jurisdictional, overseas) and parties involved in ongoing decisions and operations.

Summary of Key Decisions to Progress Australian Deployment of a SCMS

Across the four domains, this report identifies 17 key decisions required to advance Australia's SCMS deployment. Grouped by domain, these are presented in Table 2, and accompanied by an 'urgency' ranking from High to Low. The nature of the key decision, and the rationale for its urgency is explained in greater detail in Table 3.

Table 2 Summary of Key Decisions to Progress Australian Deployment of a SCMS

	Decision type	No.	Key decision to progress SCMS	Urgency
Policy	Architecture	1	Determine whether AU has one or multiple SCMS	High
		2	Determine whether AU has a national SCMS (Root CA location)	High
	Privacy	3	Develop clear position on data usage and privacy policy	Medium
		4	Determine user information for enrolment in SCMS	Low
	Legal	5	Clarify and form consistent interpretation and application of existing privacy legislation	Low
		6	Compel vehicles to use SCMS	Medium
		7	Clarify implications of privacy and surveillance regulation and policy	Low
		8	Clarify implications of security regulation and policy	Low
		9	Clarify implications of consumer protection regulation	Low
Technical	Blacklist/Whitelist	10	Determine whether SCMS will use Blacklisting, Whitelisting, or both	Low
	Cryptography	11	Determine cryptographic curve for use in AU	Low
Operational	Enforcement	12	Determine outcomes for enforcement and threat mitigation	Medium
	Affiliation	13	Determine whether AU should affiliate/plan to affiliate with EU, US, or both	Medium
	Certification	14	Determine desired levels of compliance assurance	Medium
	Disaster Recovery	15	Determine disaster recovery and business continuity management	Low
Commercial	Business Model	16	Determine SCMS business model	High
	Organisation	17	Determine SCMS Manager	High

Where this document identifies evolving discussions overseas, this does not indicate that key decisions should be reserved, or that expressing clear policy outcomes and intentions would not be beneficial.

Most of these issues are *permanently ongoing*. A disruptive technology will not, by its nature, stay still.

Key decisions identified in Table 2 – and especially those whose urgency is rated ‘High’ – are expected to strategically position policy makers to better *anticipate, manage* and *provide certainty* for these evolving developments and disruptions, and to respond, recalibrate and negotiate with agility.

The urgency with which a key decision is required to progress the Australian SCMS deployment is a relative ranking: all of these decisions are urgent, but some are of a higher urgency compared to others. The rationale for this ranking is explained in the ‘Rationale’ column.

The urgency of the decision is measured against:

- The extent to which the decision will serve as a trigger or catalyst for the resolution of other decisions
- The extent to which responsibility and leadership relating to one decision can be delegated once a decision of a higher urgency has been progressed
- The ease or difficulty with which similar decisions in related areas have been progressed in the past
- The progress made in relation to the decision in Europe and/or the United States.

Within the urgency ranking, the decisions proceed in the numerical order in which they appeared in the previous table: they are *not* ranked beyond the High-Medium-Low value.

There are:

- 4 decisions whose urgency is ranked High
- 5 decisions whose urgency is ranked Medium
- 8 decisions whose urgency is ranked Low.

A summary of these tables and the overall document is presented in Appendix A.

Table 3 Key Decisions to Progress SCMS and Rationale

	No.	Domain	Type	Key decision to progress SCMS	Rationale
High	1	Policy	Architecture	Determine whether AU has one or multiple SCMS	<p><i>Concerns decisions underpinning architecture and deployment of the SCMS.</i></p> <p>US will have one SCMS; EU will have multiple: this is due to different levels of government involvement in C-ITS (mandatory in US) and geopolitical interests (EU).</p> <p>SCMS are complex and expensive, and require local and international coordination – the <i>minimum</i> number is desirable.</p>
	2	Policy	Architecture	Determine whether AU has a national SCMS (Root CA location)	<p><i>Concerns decisions underpinning architecture and deployment of the SCMS.</i></p> <p>Both US and EU will have ‘sovereign’ SCMS.</p> <p>Local/overseas location of Root CA will affect alignment and level of policy, technical and operational control.</p> <p>Overseas Root CA not being contemplated by any other deployment.</p>
	16	Commercial	Business Model	Determine SCMS business model	<p><i>Concerns decisions underpinning initial and ongoing economic and organisational composition and viability of the SCMS.</i></p> <p>US and EU know how SCMS will work not just politically, but organisationally and commercially.</p> <p>Level and method of SCMS funding will affect overall technical design and operational capability – these matters can only be progressed so far without certainty of business model.</p> <p>Policy outcomes need to be guided by what is economically feasible.</p>
	17	Commercial	Organisation	Determine SCMS Manager	<p><i>Concerns nominating the entity who will translate the policy environment into SCMS technical policy design and operations, ensure compliance, and engage national and international SCMS stakeholders.</i></p>

No.	Domain	Type	Key decision to progress SCMS	Rationale
				<p>Both the US and the EU have incumbent or effectively incumbent SCMS Managers (USDOT and EC Joint Research Centre); governments in US and EU will play leading roles in setting SCMS policy.</p> <p>For pre-deployment, SCMS Manager role is able to inform policy development by telling decision makers:</p> <ul style="list-style-type: none"> • What is available • What the costs would be • How policy intent can be realised • Where policy intent may conflict with other requirements and capabilities. <p>Incumbent SCMS Managers serve as a point of contact for progressing technical matters, and in EU and US are liaising with industry and international stakeholders.</p> <p>SCMS Manager can take the lead, or help to progress issues of Medium or Low urgency.</p>
Medium	3	Policy	Privacy	<p>Determine clear position on data usage and privacy policy</p> <p><i>Concerns how information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.</i></p> <p>Privacy is a policy decision and an implementation choice, and critical for users and industry.</p> <p>How data is used will guide SCMS day-to-day operations, required architecture, and enforcement implementation and capability.</p> <p>Both EU and US have vision of outcomes, which are driving SCMS progress.</p>
	6	Policy	Legal	<p>Compel vehicles to use SCMS</p> <p><i>Concerns how vehicles will enter the connected SCMS security environment.</i></p>

No.	Domain	Type	Key decision to progress SCMS	Rationale
				<p>All stakeholders are anticipating the use of a SCMS – <i>how</i> users will be required to participate is important to establish.</p> <p>US will be mandatory; in EU use will be more or less automatic and inventible.</p> <p>Deployment applications using SCMS clear or progressing in US and EU; other uses also evolving.</p>
12	Operational	Enforcement	Determine outcomes for enforcement and threat mitigation	<p><i>Concerns how to mitigate risk, and protect the security and safety of users.</i></p> <p>Both EU and US have mature visions for enforcement capabilities for deployment and beyond; developing capabilities are planned or being discussed. Both are being driven by desired policy outcomes.</p>
13	Operational	Affiliation	Determine whether AU should affiliate/plan to affiliate with EU, US, or both	<p><i>Concerns how political alignment and engagement can shape technical decisions to boost international cooperation.</i></p> <p>EU will have to affiliate, but it will be a significant initial and ongoing challenge; US in a position to affiliate as desired.</p> <p>Harmonisation work undertaken by TCA gives AU the option to affiliate with EU more easily; this could be progressed with US. Doing the formal and informal groundwork at pre-deployment desirable.</p> <p>Will also inform/be informed by architecture decisions.</p>
14	Operational	Certification	Determine desired levels of compliance assurance	<p><i>Concerns the vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in supporting this.</i></p> <p>Balance required. Desired levels of trust essential to protect and assure government, industry and users; market will not tailor itself for AU needs.</p> <p>Decisions will affect devices before and after participation in SCMS.</p> <p>Progress in US well under way; urgent in EU.</p>
Low	4	Policy	Privacy	<p>Determine user information for enrolment in SCMS</p> <p><i>Concerns how information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.</i></p>

No.	Domain	Type	Key decision to progress SCMS	Rationale
				<p>User/vehicle information and linkages will affect SCMS roles and enforcement capabilities.</p> <p>Technical and organisational measures to protect user/vehicle information are of equal importance.</p> <p>US and EU still arriving at decisions.</p>
5	Policy	Legal	Clarify and form consistent interpretation and application of existing privacy legislation	<p><i>Concerns how information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.</i></p> <p>No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.</p> <p>US situation clearer; EU situation urgent and evolving.</p> <p>However, applicable regulations were not made with C-ITS/SCMS in mind. Exceptions may present complications.</p> <p>National approach highly desirable; implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.</p>
7	Policy	Legal	Clarify implications privacy and surveillance regulation and policy	<p><i>Concerns how information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.</i></p> <p>No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.</p> <p>US situation clearer; EU situation urgent and evolving.</p> <p>However, applicable regulations were not made with C-ITS/SCMS in mind. Exceptions may present complications.</p> <p>National approach highly desirable; implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.</p>
8	Policy	Legal	Clarify implications of security regulation and policy	<p><i>Concerns how information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.</i></p>

No.	Domain	Type	Key decision to progress SCMS	Rationale
				<p>No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.</p> <p>US situation clearer; EU situation urgent and evolving.</p> <p>However, applicable regulations were not made with C-ITS/SCMS in mind. Exceptions may present complications.</p> <p>National approach highly desirable; implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.</p>
9	Policy	Legal	Clarify implications of consumer protection regulation	<p><i>Concerns the vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in ensuring this.</i></p> <p>No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.</p> <p>US situation clearer; EU situation urgent and evolving.</p> <p>However, applicable regulations were not made with C-ITS/SCMS in mind. Exceptions may present complications.</p> <p>National approach highly desirable; implications for SCMS can be assessed by appropriate entity (possible SCMS Manager) at pre-implementation.</p>
10	Technical	Blacklist/Whitelist	Determine whether SCMS will use Blacklisting, Whitelisting, or both	<p><i>Concerns how to mitigate risk, and protect the security and safety of users.</i></p> <p>Both common to US and EU deployments, although at different levels. Blacklisting is closely linked to Enforcement; Whitelisting to Certification.</p> <p>Opportunities to optimise cooperation and affiliation make national consistency and strategy desirable.</p>
11	Technical	Cryptography	Determine cryptographic curve for use in AU	<p><i>Concerns how information is protected and able to be exchanged, and how user ability to be trusted is confirmed.</i></p>

No.	Domain	Type	Key decision to progress SCMS	Rationale
				<p>Fundamental decision.</p> <p>US deployment unambiguous; EU will need to be monitored – highly technical decisions subject to political environment.</p> <p>Policy decision will trigger more complex work (lead by SCMS Manager) to ensure deployment and ongoing viability.</p> <p>A commitment to future security strategy prudent and desirable.</p>
15	Operational	Disaster Recovery	Determine disaster recovery and business continuity management	<p><i>Concerns ability to offer uninterrupted support during disaster or upgrade.</i></p> <p>Essential but local (desirably national) decision.</p> <p>Redundancy and disaster recovery measures can be progressed by SCMS Manager; broader business continuity management approach to be set at policy level.</p>

Contents

1	INTRODUCTION	1
1.1	Context.....	1
1.2	Purpose of This Document.....	1
1.3	Scope.....	2
2	LAYOUT OF THIS DOCUMENT.....	3
3	STRATEGIC CONTEXT	4
3.1	Background	4
3.1.1	The Automotive World is Changing	4
3.1.2	Security is Essential	5
3.1.3	Striking the Right Balance	6
3.2	The Security Solution: Security Credential Management System (SCMS)	6
3.3	The Need for Decisions.....	7
3.4	Assess the Situation, Identify the Risks, Build a Strategy	7
4	SCMS BASICS.....	10
4.1	Governance.....	10
4.2	Basic Operation.....	11
4.3	Frequently Asked Questions	13
5	STRATEGIC POLICY CONTEXT	16
5.1	National Policy Framework for Land Transport Technology (TIC 2016)	16
5.1.1	Framework Policy Principles	17
5.1.2	Framework Action Items.....	18
5.1.3	Critical Policy Decisions to Progress the SCMS within the National Policy Framework for Land Transport Technology	19
5.2	Policy Decisions for the SCMS Implicit In or Potentially Progressed by the National Policy Framework for Land Transport Technology.....	20
5.3	Cooperative Intelligent Transport Systems (C-ITS) Final Policy Paper (National Transport Commission 2013)	21
5.4	Regulatory Reforms for Automated Road Vehicles (National Transport Commission 2016)	22
6	POLICY	23
6.1	Architecture	23
6.1.1	Concept.....	23
6.1.2	Root Certificate Authority, SCMS Manager, Public Key Infrastructure (PKI)	24
6.1.3	PKI as Adapted for SCMS.....	26
6.1.4	United States.....	27
6.1.5	Europe	30
6.1.6	Options.....	34
6.1.7	Parties Responsible for Advancing Decision	39

6.2	Privacy	39
6.2.1	Concept.....	39
6.2.2	Users and Commercial Operators	40
6.2.3	Clear Position on Privacy Policy for Users, Industry, and for Inter-SCMS Trust and Interoperability	41
6.2.4	United States.....	41
6.2.5	Europe	42
6.2.6	Identifying Information for Enrolment (and thus Participation)	42
6.2.7	Policy and Legislation	44
6.2.8	Options.....	44
6.2.9	Parties Responsible for Advancing Decision	45
6.3	Legal	46
6.3.1	Concept.....	46
6.3.2	United States.....	46
6.3.3	Europe	47
6.3.4	Need for Clear and Consistent Interpretation and Application of Existing Legislation for Privacy	47
6.3.5	Need for C-ITS Enabled Vehicles to be Compelled to Use and Receive Credentials from the SCMS.....	48
6.3.6	Privacy and Surveillance Regulation and Policy	48
6.3.7	Security Regulation and Policy.....	51
6.3.8	Consumer Protection Regulation	52
6.3.9	Options.....	53
6.3.10	Parties Responsible for Advancing Decision	56
7	TECHNICAL	59
7.1	Blacklist / Whitelist	59
7.1.1	Concept.....	59
7.1.2	Blacklisting	60
7.1.3	Whitelisting.....	62
7.1.4	Options.....	64
7.1.5	Parties Responsible for Advancing Decision	66
7.2	Cryptography.....	66
7.2.1	Concept.....	66
7.2.2	Europe	67
7.2.3	United States.....	67
7.2.4	Cryptoagility	68
7.2.5	Options.....	69
7.2.6	Parties Responsible for Advancing Decision	70

8	OPERATIONAL	71
8.1	Enforcement	71
8.1.1	Concept	71
8.1.2	Revocation	72
8.1.3	United States	73
8.1.4	Europe	74
8.1.5	Options	74
8.1.6	Parties Responsible for Advancing Decision	76
8.2	Affiliation	77
8.2.1	Concept	77
8.2.2	Europe	78
8.2.3	United States	79
8.2.4	SCMS Policy Tools	79
8.2.5	Options	83
8.2.6	Parties Responsible for Advancing Decision	84
8.3	Certification	84
8.3.1	Concept	84
8.3.2	Lifecycle Management	85
8.3.3	United States	86
8.3.4	Europe	87
8.3.5	Options	87
8.3.6	Parties Responsible for Advancing Decision	88
8.4	Disaster Recovery	89
8.4.1	Concept	89
8.4.2	Options	91
8.4.3	Parties Responsible for Advancing Decision	92
9	COMMERCIAL	93
9.1	Business Model	93
9.1.1	Concept	93
9.1.2	United States	95
9.1.3	Europe	95
9.1.4	Options	95
9.1.5	Parties Responsible for Advancing Decision	96
9.2	Organisation	96
9.2.1	Concept	96
9.2.2	SCMS Manager	97
9.2.3	United States	98
9.2.4	Europe	99
9.2.5	Options	100

9.2.6 Parties Responsible for Advancing Decision	101
--	-----

APPENDIX A : SUMMARY OF DOCUMENT 102

FIGURES

Figure 1 How This Document Works	vii
Figure 2 Basic SCMS Operations	11
Figure 3 Simplified PKI Trust Hierarchy.....	25
Figure 4 Simplified PKI as Adapted for SCMS.....	26
Figure 5 Generic PKI for United States SCMS	28
Figure 6 United States SCMS.....	29
Figure 7 European SCMS Deployment Model	30
Figure 8 European SCMS Deployment Model Compared to United States	33
Figure 9 Australian SCMS Deployment, Single Root CA	35
Figure 10 Australian SCMS Deployment, Multiple Root CAs.....	36
Figure 11 Australian SCMS Deployment, Overseas Root CA.....	36
Figure 12 SCMS Policy Tools.....	80
Figure 13 European Certificate Policy	81
Figure 14 SCMS Lifecycle Management	86
Figure 15 Disaster Recovery/Update Support	90

TABLES

Table 1: Structural Logic of Document.....	viii
Table 2 Summary of Key Decisions to Progress Australian Deployment of a SCMS	ix
Table 3 Key Decisions to Progress SCMS and Rationale	xi
Table 4 Information Security Questions for Government Managers, and Transport Agency Risks.....	9
Table 5 SCMS FAQ	13
Table 6 Privacy and Surveillance Regulation and Policy	49
Table 7 Security Regulation and Policy	51
Table 8 Consumer Protection Regulation	52
Table 9 Blacklistng vs Whitelisting.....	64
Table 10 Summary of Document	102

1 INTRODUCTION

1.1 Context

A Security Credential Management System (SCMS) is not one single thing. Rather, it is:

- An operational framework with defined interactions and actors
- A business model
- An operational environment
- A piece of cyber-physical infrastructure
- A collection of people, processes and policies
- An *assemblage* of highly advanced technological systems, technologies and management practices
- Within one or more organisational structure.

A SCMS is deliberated and designed; developed, implemented and deployed; and managed and updated.

It is a long-term solution to a rapidly-approaching, disruptive phenomenon, emerging out of international cooperation and agreement in which Australia through Transport Certification Australia (TCA) has had co-leadership role.

A SCMS is a fundamental part of a connected and cooperative environment, enabled by Cooperative Intelligent Transport Systems (C-ITS): technologies that will connect vehicles with other vehicles and their environment, transform cities into Smart Cities, and our connected world into the Internet of Things.

This is a significant task: people will need to trust the systems that have been designed to make them safer.

These systems will need to trust each other, yet remain unknown to one another.

The SCMS ‘squares the circle:’ it allows systems in a large-scale, complex environment to trust strangers, and allows strangers to trust the systems.

It does so by providing security support and services.

A commercially sustainable global market for C-ITS will not be possible without security, and neither will safety nor true connectivity.

1.2 Purpose of This Document

The purpose of this document is to present the core policy decisions for progressing the development of a SCMS in Australia.

The SCMS is a highly specialised area, drawing on established and bespoke cybersecurity strategies and techniques, progressed in unison with the latest advancements in intelligent transport technology.

Most of the issues and decisions necessary for progressing the SCMS for the Australian C-ITS deployment are of a policy nature.

Although it attempts to isolate issues specific to the SCMS, where necessary, the document points to developments in C-ITS more broadly, given that one cannot exist without the other, and developments in one area will affect and be affected by the other.

The document restricts the discussion to issues that require the attention of policy and decision makers, since technical decisions for the SCMS can be progressed once key decisions or intentions are made clear.

The SCMS will be a highly sensitive and responsive system comprising people, technical and operational processes and policies, and its overall composition and operation will be designed to translate the Australian policy environment into security outcomes (detailed and discussed in 8.2.4 on SCMS policy tools).

1.3 Scope

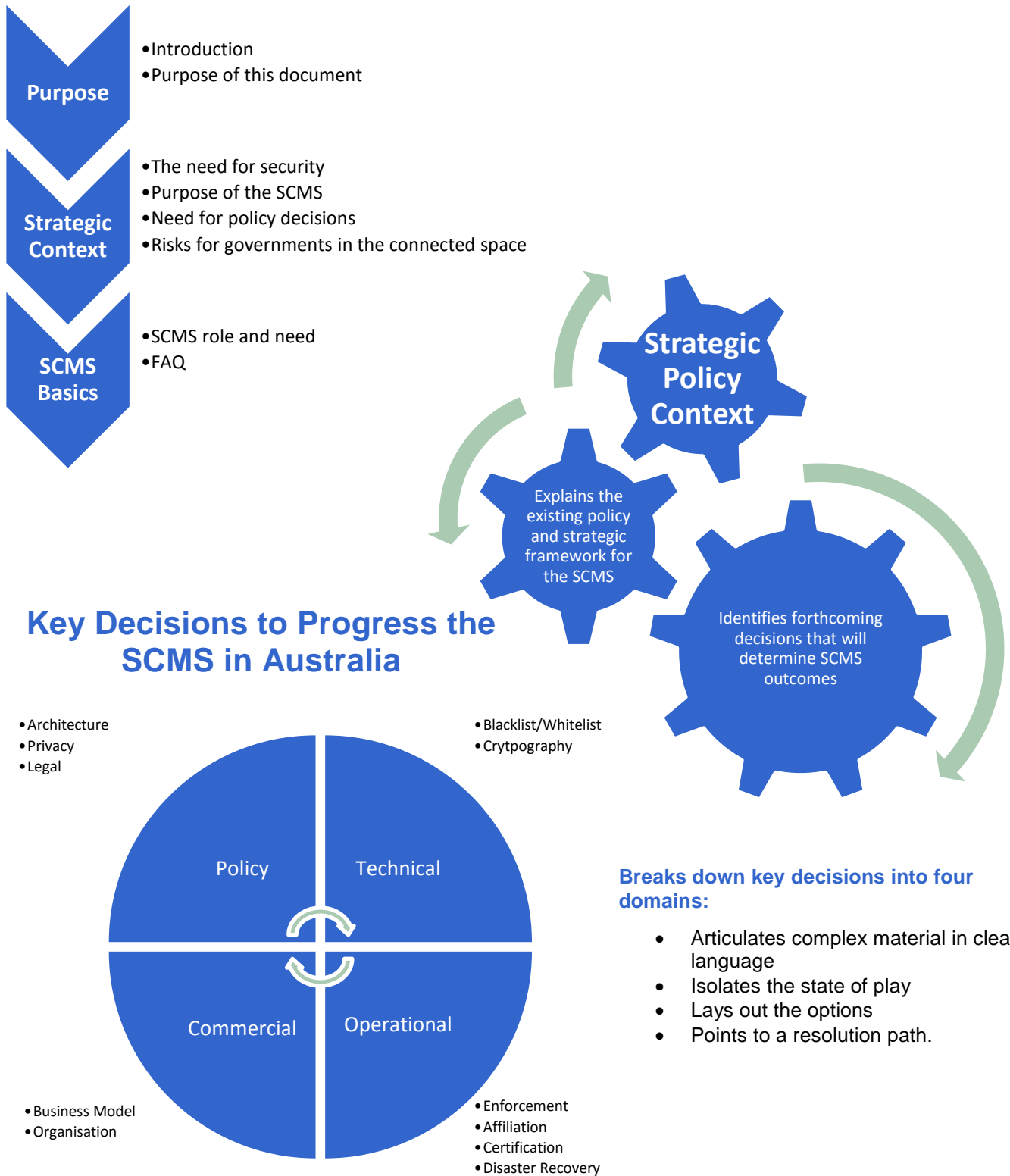
The context for this document means that the discussion can take place at a relatively high level, without sacrificing complexity. Technical insights and concepts are defined and described where necessary, so that readers can make informed decisions.

The goal is to capture the need for decision making across the following elements within this context:

- **Policy:** what rules are needed to provide guidance for the SCMS, to protect users and businesses, and who makes them?
- **Technical:** what should a SCMS do, and how should it do it?
- **Operational:** how will the SCMS work in the real world, today, tomorrow and into the future?
- **Commercial:** what are the commercial decisions required for the SCMS, the impacts to government and industry, and who will benefit?

The contents of this document are presented along these lines. However, there is a high level of overlap and interrelation between these four elements. This means that a decision affecting one element is highly likely to significantly impact one, or indeed, all, of the others.

2 LAYOUT OF THIS DOCUMENT



Appendix A: summarises this document

3 STRATEGIC CONTEXT

3.1 Background

Confidence in the security of online systems is essential to fully realising the potential of the digital economy (and is already critical in closed communication systems used to operate the national electricity market, telecommunications, public transport and other infrastructure).⁵

3.1.1 The Automotive World is Changing

Connected and cooperative vehicles and intelligent transport systems are a critical part of the disruptive transformation occurring to our vehicles, roads, cities and technologies – including automated vehicles, smart cities and smart infrastructure, and the Internet of Things (IoT).

They have been developed as a way to deliver a safer and more efficient transport network that is less congested and more environmentally friendly.

What all these transformations have in common is the growing – and unprecedented – convergence of the physical and digital spheres. If managed correctly, they have the ability to enhance our quality of life.

Together, these transformations constitute a paradigm shift. As with any new technology that facilitates economic and social change, safeguards protect the public interest and enable innovation in equal measure.

It is in Australia's highest interests to adopt Cooperative Intelligent Transport Systems (C-ITS) in a manner that delivers safe, secure, and commercially and operationally sustainable outcomes.

The technology for C-ITS already exists, or will soon be available. But this doesn't mean it will work the way we want it to work, and it doesn't mean it will deliver the best results for the majority of people.

In ushering in this new technology, all regions, including Australia, have had to grapple with the same fundamental questions:

- **Technical:** what does it do and how will it do it?
- **Policy:** what rules are needed to provide guidance, to protect users and businesses, and who makes them?
- **Operational:** how will the technology work in the real world, today, tomorrow and into the future?
- **Commercial:** what will it cost and who will benefit?

⁵ The Productivity Commission. 2016. *Digital Disruption: What do governments need to do? Productivity Research Paper*. Australian Government, p. 119. Available at <http://www.pc.gov.au/research/completed/digital-disruption/digital-disruption-research-paper.pdf>

3.1.2 Security is Essential

The connected and cooperative shift will blur the boundaries of what has been previously easy to identify as the transport sector.

This means that new entities may be exposed to threats and vulnerabilities from technologies and entities not found in the traditional automotive world.

Security is an assumption and an expectation for end users. Not meeting these could have very serious safety consequences, and could undermine public confidence.

It essentially comes down to trust: how to enable it, how to encourage it, and how to make sure it endures.

That level of trust is going to become a lot more important, and a lot harder to achieve for the connected and cooperative space. That trust wouldn't be very useful if it only extended to a few people, or to a few brands. It needs to be able to extend to whoever wants access, when they want it.

This is essentially asking systems – and their users – to trust systems that are unknown to them, and to trust that these systems can interoperate safely, securely, and reliably.

To achieve what industry, government and users envision – and expect – *trust and interoperability need to be the default, not a choice.*

If the systems in the cooperative and connected environment cannot trust each other, then people cannot trust the systems.

Security and safety can no longer be treated as separate concerns. It is becoming more and more important that safety and security considerations and provisions advance in unison. The solution to this challenge is, in effect, leveraged from the cryptographic (encryption) technologies and management processes used in information communications technologies (ICT).

Security that provides protection for communications, devices, and the overall environment is a common need in any C-ITS deployment. As we move into a world where vehicles become computers on wheels, we need to establish new ways for 'trust' to be established between vehicles and all road users – not just drivers.

The provision of security extends to multiple, overlapping challenges, such as the requirements for scalability, extensibility, multiple applications and users travelling across regions, a market of vehicles and devices sourced from around the globe, financial stability and operational sustainability.

3.1.3 Striking the Right Balance

Security has as much to do with reimagining, and getting the most out of, our transport network, as with preparing for changes that are rapidly approaching.

The broad goals of security are really two sides of the same coin. It needs to:

- **Protect** against threats that can deny, degrade, disrupt or destroy technical, organisational, commercial, privacy and safety services, settings and assurances
- **Enable** public purpose and commercial outcomes to be realised.

The security environment in Australia and overseas continues to develop, but one of the key things that is emerging is how security will be one of the key drivers for promoting change and innovation, and for driving uptake and availability.

Security will need both to deliver the level of confidence sought by governments and users, while also aiding developers and manufacturers.

Striking the right balance ensures that security is a conduit to the global market, where international acceptance and availability can be achieved with minimal changes.

Security is one of the fundamental ways different regions establish and communicate their trust in each other's systems and devices.

A commercially sustainable global market for C-ITS will not be possible without security, and neither will safety nor true connectivity.

3.2 The Security Solution: Security Credential Management System (SCMS)

The security solution for the connected C-ITS environment, and the focus of this document, has emerged out of international collaboration, and is called a Security Credential Management System (SCMS).

The SCMS is a central pillar to enable security across systems, and is fundamental to a C-ITS deployment.

A SCMS is both an institutional framework and a piece of infrastructure, encompassing human/management, electronic and physical elements – it is 'cyber-physical.' Like any piece of infrastructure, its development needs to be approached as a long-term investment: the product of careful policy, planning and consideration as to its capability and longevity, and the organisational elements necessary to operate and maintain it.

The SCMS allows both government policy and commercial applications to be implemented. It ensures that the C-ITS environment is secure by managing privacy, access, prioritisation and cybersecurity, and is a foundation on which the day-to-day use of, and benefits associated with, C-ITS can be realised.

3.3 The Need for Decisions

As C-ITS deployments overseas and in Australia near operation, there are a number of issues that will need to be resolved by policy and decision makers.

While these issues may need to be resolved by different entities and at different levels, the overarching sentiment captured in this document is that these are predominantly issues that would ideally be resolved – or at the very least discussed – on a national level.

It is accepted that Australia's C-ITS deployment is dependent on aligning with international standards, models and practices.

This is especially important for the SCMS given that, by providing security essentials, and as a fundamental part of a security strategy, the SCMS will effectively undergird the C-ITS environment.

Where necessary, this document points out where these standards, models and practices are still developing, and highlights Australia's need to maintain an active and, where suitable co-leadership, role – not just as an observer.

By the same token, this document points out where international progress is sufficiently advanced, such that Australia is able to initiate decisions that will progress the SCMS – and by extension, C-ITS – without compromising its immediate or future security and operational capabilities, public and private interests, or reputation.

Indeed, decision making in these areas can be expected to bolster these.

3.4 Assess the Situation, Identify the Risks, Build a Strategy

C-ITS is a specialised field – developing a SCMS even more so. But both draw on existing technologies, entities, resources and capabilities.

For Government Transport Agencies, this poses new opportunities, but also new challenges and risks.

Some of these challenges and risks can be mitigated by using existing resources.

The *Information Security Manual* (ISM) is the Government's flagship product designed to assist Australian Government agencies in adopting a risk-based approach to information and ICT systems, and supports the strategies and principles of the *Australia's Cyber Security Strategy*.⁶

The ISM is aimed at Government operations and organisations that make use of, among other things, cybersecurity, communications systems and cryptography – operations directly concerning C-ITS and the SCMS.

The ISM poses questions to Senior Management in order for them to assess their organisation's cybersecurity situation. The ISM can be used by Government Transport Agencies to assess their C-ITS and SCMS situation, identify risks, and build a strategy.

⁶ Department of the Prime Minister and Cabinet. 2015. *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity*. Australian Government <https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf>

The following table captures the questions posed, key messages, and risks identified in the ISM, and highlights their applicability – and the additional risks – for Government Transport Agencies.

There are important differences between the type of Government Agency the ISM has in mind, and the use to which it can be put for Transport Agencies.

The ISM helps Agencies provide security for their organisation and operation – its premises, off-site locations, and the technologies and systems used and the people that use them. In short, their user base is generally employees in fixed locations.

Transport Agencies need to consider these standard information security risks and operational environments for their organisations, yet also recognise from the outset that:

- Users of C-ITS will be *drivers, passengers* and *pedestrians*
- Systems (and their users) will be both *fixed* and *mobile*
- They need to provide security for the transport *network*.

Table 4 can be used when assessing the risks to government agency and transport network information security practices discussed in this document.

Table 4 Information Security Questions for Government Managers, and Transport Agency Risks

Question for Senior Management	Key message	Government Agency risks	Additional Transport Agency risks
What would a serious cyber security incident cost our organisation?	Good information security is like an insurance policy.	<p>Costs of clean-up, downtime, taking a whole system offline, lost productivity, reputation and confidence in the agency.</p> <p>Customer records, financial data and intellectual property are vulnerable to theft, yet determining what was stolen can be difficult.</p>	<p>The cost of a security incident is measured in physical and emotional trauma and loss of life, not just lost productivity, damaged reputations and dollars (cost of road trauma in AU is approx. \$27 billion each year).⁷</p> <p>Security is not just an insurance policy – true connectivity is not possible without it, nor is safety.</p> <p>User appetite for new technology is strong – but not if it doesn't work, or poses a safety or security threat.</p>
Who would benefit from having access to our information?	Information is valuable.	<p>Threats can be local or non-local.</p> <p>Compromised confidentiality, integrity and availability threaten essential and ongoing functioning.</p> <p>Individual records are valuable – but aggregated information can be just as valuable.</p>	<p>Integrity means information is not modified or manipulated. A modified message is as dangerous as a fake message, or one that fails to arrive at all.</p> <p>Availability means information needs to happen in real time for safety purposes. Deci-seconds will make a difference.</p> <p>Individual and aggregated information may be as valuable to unauthorised recipients as to an authorised party intent on doing the wrong thing – knowing who, what, when, where and how to trust.</p>
What makes us secure against threats?	Security is an ongoing process, not a product.	<p>Security needs to be as sophisticated as the threat, and they co-evolve.</p> <p>Lack of appropriate security governance, clearly defined policy, educated users.</p> <p>Security products alone are not a solution.</p>	<p>Finance, defence and intelligence agencies are familiar with the security task – Transport Agencies are not.</p> <p>Like roads and bridges, cyber-physical infrastructure needs to be maintained and managed – but the timeframes and response times are tighter.</p> <p>Defining and distributing roles and responsibilities amongst traditional and non-traditional stakeholders.</p>
Is the behaviour of my staff enabling strong security culture?	Education is key.	<p>Unwitting users and honest mistakes and can do serious damage.</p> <p>Ignorance can be as dangerous as malicious activity.</p>	<p>Transport Agencies have worked hard to foster safety culture, in their organisations and on the road. Now they must do the same with security.</p> <p>Everyone is a user of the transport network: knowingly or unknowingly, every user can deny, degrade, disrupt and destroy as much as they can do the right thing.</p>

⁷ Department of Infrastructure and Regional Development, Bureau of Infrastructure, Transport and Regional Economics. 2014. *Impact of road trauma and measures to improve outcomes*. Australian Government. Available at https://bitre.gov.au/publications/2014/files/report_140.pdf

4 SCMS BASICS

4.1 Governance

A SCMS will play a critical function in a C-ITS deployment. It will therefore be a 'governed' and 'managed' system. Both of these aspects are touched on in this document, but for introductory purposes:

- **Governed** means that the SCMS will involve multiple stakeholders, both public and private. Governance arrangements determine how these stakeholders interact (their roles and responsibilities) and the defined outcomes they will work together to deliver.
- **Managed** means that the SCMS does not operate by itself: many of its functions are *automated*, but they *don't happen automatically*: they do not happen without the active involvement of different stakeholders – and these stakeholders themselves need active management. A key part of a governance arrangement is to determine how the SCMS is managed, and by whom.

There are key decisions relating to governance and management identified in this document. However, the key points can be understood as follows:

- Policy is likely to be developed by a national policy body which is approved under Ministerial arrangements.
- A body is then needed to translate these policy outcomes into operational policies and processes. This body is the SCMS Manager, who also ensures that these operational policies and processes are adhered to by entities within the system.
- The system is hierarchical in nature: generally, those at the top are more 'trusted' and can authorise more actions than those below. Below the SCMS Manager, the most trusted operational entity is called the Root Certificate Authority: trust and authority can always be 'traced back' to the Root Certificate Authority.
- Vehicles (and devices in pieces of infrastructure, etc.) have to be enrolled or registered into the system by authorised bodies known as Enrolment Certificate Authorities.
- Registered vehicles then get anonymous permits or certificates to participate in various C-ITS applications. The Pseudonym Certificate Authorities do this.

The section immediately below illustrates how these different roles work together to deliver the basic operations of the SCMS.

4.2 Basic Operation

Figure 2 (below) represents a distilled presentation of how a SCMS operates.

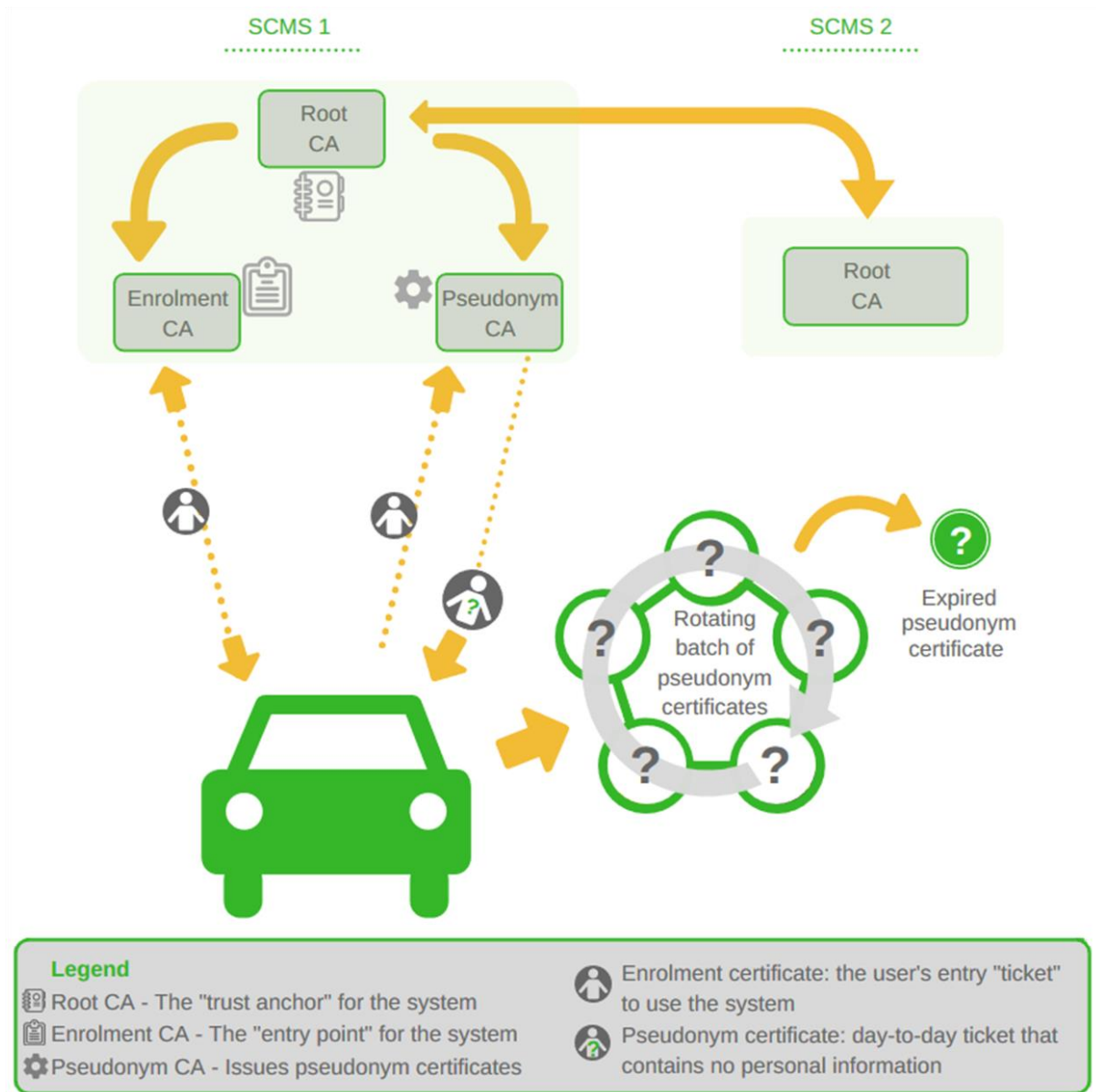


Figure 2 Basic SCMS Operations

In summary:

- The user (driver) needs to be anonymous, yet the messages they send to other users need to be received and relied upon; other users need to know that *messages* can be relied upon, but they should not know *who* is sending them.
- The user approaches the Enrolment Certificate Authority with a request to join the SCMS, and supplies the necessary information.
- The Enrolment Certificate Authority makes sure everything is in order, and issues the user with an enrolment certificate⁸ – a very important item that allows the user to participate in the SCMS.
- The enrolment certificate is signed by the Enrolment Certificate Authority, who has the authority to do so by virtue of being trusted by the Root Certificate Authority. The enrolment certificate carries the signatures of both the Enrolment Certificate Authority and the Root Certificate Authority.
- The user approaches the Pseudonym Certificate Authority with their enrolment certificate. Because they have an enrolment certificate signed by the Enrolment Certificate Authority and the Root Certificate Authority, the Pseudonym Certificate Authority can issue the user with pseudonym certificates. The Pseudonym Certificate Authority has the authority to do so by virtue of being trusted by the Root Certificate Authority.
- Pseudonym certificates are used for different applications – such as processing a vehicle's safety 'heartbeat' message into an application (used, for example, for crash avoidance).
- These pseudonym certificates identify *permissions*, not the *person* – they tell other users that this user's message can be trusted, but do not reveal any identifying information about the user. They can be trusted because they have the signatures of the other Certificate Authorities on them.
- The user has a batch of pseudonym certificates: they rotate and are used for different applications – using the same pseudonym certificate all the time would mean that people could trace the constant use of the pseudonym certificate to a user.
- Pseudonym certificates are only valid for a certain amount of time. This ensures that they *rotate and expire* – as reusing pseudonym certificates would invite linkages to be made to the user.
- When the user is out of valid pseudonym certificates they go back and get more from the Pseudonym Certificate Authority.
- The Pseudonym Certificate Authority checks with the Enrolment Certificate Authority to see if it is okay to issue new pseudonym certificates. If the user has been misbehaving (intentionally or unintentionally) and posing a threat to other users, they should not be issued certificates that would enable them to continue to pose a threat.
- What if the user wants to travel from jurisdiction/region A to jurisdiction/region B, but B is supported by a different SCMS? The Root CA of SCMS-A can forge a relationship with SCMS-B to facilitate this with minimum hassle – or possibly no hassle – and can ensure that the user receives the same level of security and protection under SCMS-B as they enjoyed under SCMS-A.

⁸ All 'signatures' and 'certificates' are digital; these processes are 'online' and automated.

4.3 Frequently Asked Questions

Table 5 below captures the need for a SCMS in a series of answers to common questions, in addition to defining some of the key terms and concepts introduced above and used throughout this document. These are answered in conversational language.

Table 5 SCMS FAQ

Why does security matter for cars?
<p>A computer network is sufficiently complex and its users removed from the presence of others to enable users to claim to be one thing, while really being another.</p> <p>It is also very possible to intercept messages on a computer network.</p> <p>Cars and the transport network are becoming more and more like computer networks – there are new opportunities to make it better, and new opportunities to make it worse.</p>
What does a SCMS create?
<p>A SCMS creates trust for a specific security domain. A security domain can be defined as:</p> <p style="padding-left: 40px;">a system or collection of systems operating under a security policy that defines the security to be applied to information of the system or systems. That security may be represented by a classification, caveat or releasability marking with or across classifications.⁹</p> <p>A SCMS security domain can be defined by at least one or a combination of the following:</p> <ul style="list-style-type: none"> • Geography: a country or a jurisdiction • Applications: the types of services that the certificates it issues, renews and revokes and supports • Industry: a car manufacturer may have a SCMS for their cars and their cars alone • Politics: the reach of a SCMS may be shaped by political tensions and affiliations • Time: a SCMS may cease to be operational, but the certificates it issues may be valid for longer than the life of the SCMS.
Could C-ITS work without a SCMS?
<p>Yes. But not for very long, and not for more than a handful of users.</p> <p>This is the equivalent of asking if you need a password for your email account, a swipe card for your office, or security for online banking; and the reason why you keep your password private, why you don't share your swipe card with a stranger, why you give your bank account details to no one, and why you trust your bank not to share your information with the world.</p> <p>Added to this: the SCMS and security in general will keep you safer on the road.</p> <p>All parties, from governments to vehicle manufacturers are aware of and are planning to use a SCMS.</p>
What is 'trust' in the context of C-ITS and the SCMS?
<p>Trust is multifaceted. Basically, it means being able to know you can rely on the users around you, without knowing who they are.</p> <p>The United States Department of Transportation writes that trust is:</p> <p style="padding-left: 40px;">defined by the requirement that thousands of data messages will be authenticated, in real-time, as coming from a trusted (but unknown) source. It is also a critical element in achieving interoperability – the ability of vehicles of different makes, models, and years to exchange trusted data without pre-existing agreements or significant alteration of</p>

⁹ Department of Defence, Strategic Policy and Intelligence. 2016. *Australian Government Information Security Manual. Principles*. Australian Government, p. 66. Available at http://www.asd.gov.au/publications/Information_Security_Manual_2016_Principles.pdf

existing vehicle designs. Further, the system must be secure against internal and external threats or attacks.¹⁰

Who needs to be trusted, and who needs security?

Everyone needs some level of basic security; others will need more:

- Users: vehicles at first, later cyclists and mobile devices
- Roadside infrastructure
- Government transport agencies
- Private companies with road management responsibilities
- Service Providers
- Manufacturers (of cars and other devices and developers of applications).

All the systems owned and used by, connecting to and relied upon by these entities need, at some level, to be:

- Trusted – unknown and untrusted parties are a threat
- Publicly accepted – people won't use it if it doesn't work
- Harmonised – one device needs to be able to talk to another
- Compliant – breaking the law, deliberately or by mistake, should not be easy or tolerated.

The SCMS helps C-ITS do this.

And these qualities need to apply to the SCMS as well.

Isn't this something that industry will sort out on their own?

For a number of reasons explained later in this report, this approach is very unlikely to be effective.

On this topic, the USDOT summarised industry stakeholders' responses to the United States Notice of Proposed Rulemaking on C-ITS thus:

industry commenters vehemently disagreed that a private self-governing industry coalition could be a viable mechanism for SCMS system governance. Commenters believed that a private SCMS could not provide the security, privacy, certainty, stability, long-term functionality, or management of costs and risk required for a nationwide SCMS to support V2V DSRC communications, and lacked the legal authority to address cross-border issues or require industry-wide participation and compliance with uniform requirements. For these reasons, virtually all industry commenters took the position that a strong leadership role for the Federal government in the SCMS would be required for successful deployment of V2V and V2X DSRC communications.

European commentators have also recognised an important government role in SCMS management.

What else does a SCMS do?

A SCMS also provides Misbehaviour Management: the ability to detect and, where appropriate, remove from the operational environment threats to security and/or safety threat.

What is Public Key Infrastructure and why is it important for a SCMS?

Public Key Infrastructure (PKI) consists of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of data.

PKI is used to confirm the validity of digital certificates – the electronic 'passports' of users, applications and devices – and that they are coming from a safe and secure source. PKI is already used in the issuing of new passports, and in telecommunications – environments where confidentiality, integrity, and authentication are essential.

¹⁰ United States Department of Transportation. 2015. *Status of the Dedicated Short-Range Communications Technology and Applications. Report to Congress*, p. 45-6. Available at <https://trid.trb.org/view.aspx?id=1400143>

PKI is used in many daily tasks conducted across the Internet today, such as Internet Banking, e-Commerce transactions, sending secure emails and lodging company tax returns with the Australian Taxation Office (ATO). It is also used in the provision of Australian healthcare services by the Department of Human Services, and in Australia's Intelligent Access Program (IAP).

A SCMS (like PKI) is a collection of roles and responsibilities, not a purely technical system or process.

What are digital certificates?

You use digital certificates all the time without knowing it – whenever you browse the Internet, or use a smartphone, or make an online payment.

Digital certificates are electronic passports that may or may not identify the holder.

Digital certificates need to be issued by a trusted party – you can't print your own passport or make your own driver licence. Anything like a digital certificate needs to be managed and maintained by the proper procedures.

If the procedure is bad, then the certificates are bad.

A digital certificate has other things inside it:

- They state what you're allowed to do – they state your permissions and *credentials*, but do not tell others who you are
- They contain keys – keys are used for cryptography, which allows you and others to 'unlock' the code used to scramble the contents of the messages you send and receive.

Is a SCMS all that is needed for security?

No. The SCMS is fundamental, but it is a fundamental part of an overall security strategy.

The SCMS is dependent on, affects and is affected by this security strategy that includes, among other things, robust compliance assessment.

What is needed to build a SCMS in Australia?

A SCMS could be built for Australia starting tomorrow.

But a SCMS built tomorrow using today's information would be useless.

The SCMS is complex. Of all the systems needed for a C-ITS environment, it is the most sophisticated.

A SCMS requires a number of decisions to be made. Some of these are dependent on decisions being made overseas; others require the attention of Australian policy and decision makers.

Once decisions are made overseas and in Australia, a SCMS can be progressed and built.

Why does a SCMS need a SCMS Manager?

There are many entities and functions in a SCMS.

These can be distributed or centralised, with some more logically centralised than others, with oversight provided by a single management entity – the SCMS Manager.

The SCMS Manager ensures that the SCMS functions in accordance with the policy environment: they 'translate' government policy into technical details to keep people safe and secure.

5 STRATEGIC POLICY CONTEXT

The policy and decision-making context for C-ITS in general and the SCMS in particular is responsible for the following activities:

- Establish government policies relevant to the security and privacy management aspects of C-ITS
- Establish the necessary regulatory and non-regulatory instruments to underpin and enable policy intent
- Policy decisions on SCMS governance, including roles and responsibilities.

Policy and strategic decisions are the primary drivers for progressing the development of SCMS operational policies, system management, system operation and, ultimately, the experience of end users.

For the SCMS, many of the activities that enable the delivery of security support and services will be realised by operational policies: security policy, certificate policy and certification practice statements, which are developed, circulated, maintained and enforced by an entity empowered as the SCMS Manager (see 8.2.4 and 9.2.2). The SCMS effectively creates a 'trust domain' – a system or system of systems that operate under a single security policy.

The SCMS will be a highly sensitive and responsive system. Its overall role is to translate the policy environment into operational policies (that is, security and certificate policy) and technical systems and processes.

Policy requirements that are developed by the SCMS Manager, at the system management level, and flowing through the system operation level, are primarily related to security and certificate policy.

While these policies will also shape and be shaped by other implementation decisions, the primary driver for their content is government policy.

Government policies are external to the SCMS as such, but are enabling decisions insofar as detailed SCMS requirements cannot be progressed in their absence.

An initial set of SCMS requirements can reflect the necessity of government policy decisions, but cannot make assumptions as to the content of those government policy decisions themselves.

A public version of initial SCMS requirements was published by TCA in the *Discussion Paper: Towards a national vision for a secure, connected future through Cooperative Intelligent Transport Systems*; ¹¹ a more detailed version of these requirements is currently progressing with Austroads.

5.1 National Policy Framework for Land Transport Technology (TIC 2016)

The National Policy Framework for Land Transport Technology (2016) has been developed by the Transport and Infrastructure Council and supersedes the policy and strategic guidance of the Policy Framework for Intelligent Transport Systems in Australia (2011).

¹¹ Available at http://tca.gov.au/publications_and_reports

The objective of the Framework is to foster an integrated policy approach by governments to the development and adoption of emerging transport technologies, in order to achieve improved transport safety, efficiency, sustainability and accessibility outcomes.

The SCMS is a critical component in enabling these outcomes, and its role in supporting a C-ITS deployment will play a significant role in addressing the operational and policy challenges identified in the Framework as 'Key Issues for Government in Deploying New Transport Technologies'. The SCMS itself aims to respond to the challenges identified:

- Safety, Security and Privacy
- Digital Infrastructure
- Data
- Standards and Interoperability
- Disruption and Change.

5.1.1 Framework Policy Principles

The Framework is underpinned by seven policy principles that have been agreed to by Australian governments:

1. Government decision-making on transport technologies will be based on capacity to improve transport safety, efficiency, sustainability and accessibility outcomes.
2. New technologies should be implemented in a way that is consumer centric (i.e. designed to meet the needs of those using the service). This includes consideration of
 - a. options to deliver transport information and services in a way that is consistent and familiar, and
 - b. the diverse needs of travellers, in particular travellers with a disability, vulnerable road users such as cyclists and pedestrians, and users of multiple modes of transport.
3. Where government investment is required to support the deployment of new technologies, that investment will be evidence based, consistent with long-term strategic planning and will deliver value for money.
4. Where feasible, government agencies will avoid favouring particular technologies or applications, in order to encourage competition and innovation. New applications should support interoperability, backwards compatibility and data sharing, and should account for possible future transitions to other technology platforms.
5. Planning for transport technologies will build on existing infrastructure networks (including public transport) and seek to leverage existing consumer devices (such as smart phones) where appropriate.
6. When considering regulatory action, governments will consider low cost approaches such as collaborative agreements or self-regulation before pursuing formal regulation.
7. If required, best practice regulatory approaches will be adopted to ensure regulation is cost efficient, transparent, proportionate to the risk, fit for purpose and done in consultation with affected stakeholders. This includes adopting relevant international or regional standards, unless there is a compelling reason for a unique Australian requirement.

The operation, management and role of the SCMS will be shaped to a large extent by the overall strategy proposed by the Framework and its policy principles. It is an assumption that the SCMS will be a reflection of the policy principles in the Framework, and be required to uphold the principles themselves.

5.1.2 Framework Action Items

In addition to the Framework's policy principles, outcomes for two of the 14 Action Items in the Framework are of particular relevance for this document.

The first Action Item of relevance reads:

Publish a connected vehicle (Cooperative ITS) statement of intent on standards and deployment models (Action Item # 5).

With the outcome of this Action Item informed by other work TCA is progressing with Austroads, the Framework highlights that the statement of intent will provide industry with guidance on:

- Non-regulatory deployment models possibly adopted by convention in Australia
- Regulatory standards which may form part of the formal regulatory framework in Australia.

TISOC/Commonwealth are the lead entities on this Action Item, which is to be delivered in early 2017.

The Action Item will have a substantial role in determining the regulatory framework for C-ITS, and is therefore of substantial relevance to the SCMS.

The outcomes of this Action Item will be critical for progressing the SCMS, insofar as the SCMS can be said to translate the overall policy and regulatory landscape for C-ITS into operational, management and technical systems and processes that provide security.

More narrowly, the SCMS will be greatly impacted by compliance assessment processes.

To simplify, the compliance assurance regimes adopted for C-ITS will have to work hand in hand with the SCMS, and the SCMS itself will have an active role in ensuring that certificates are issued to C-ITS devices on the basis that they are compliant with compliance assurance regimes.

Options for compliance assessment regimes are presently being progressed by TCA with Austroads.

The second Action Item of relevance reads:

Develop a nationally agreed deployment plan for the security management of connected and automated vehicles (Action Item # 6).

The Framework highlights that preventing cyber threats and malicious acts will be a key challenge in deploying connected and automated vehicles, and identifies the SCMS as the model that has emerged internationally to address cyber security issues.

This Action Item will explore options for meeting security management requirements, factoring in costs, risks, feasibility, timing, and overseas experience.

The overall output for this Action Item will be a nationally agreed plan for security management.

TISOC/Austroroads are the lead entities on this Action Item, which is to be delivered in mid-2018.¹²

Informing the discussion of a nationally agreed deployment plan for security management, the Framework identifies that consideration will be given to:

- Role of government
- Whether other telematics and intelligent transport services could also utilise the SCMS.

A key output from this Action Item, however, will be a decision as to whether a national SCMS is required in Australia. In more technical terms, this decision relates to whether the Root Certificate Authority (the trust anchor for the SCMS, from which all other certificate management entities and C-ITS devices inherit their trust) will be:

- A single Root Certificate Authority located in Australia
- One of multiple Root Certificate Authorities in a multi-SCMS Australian environment
- A Root Certificate Authority located overseas (see 6.1.2).

The location of the Root Certificate Authority will have substantial cascading effects for the design, and operation of the SCMS, and will be especially important in determining the security and certificate policies that will undergird the overall security environment (see 8.2.4).

Detailed system requirements and security and certificate policies will vary significantly based on this outcome, and there are a number of serious consequences (see 6.1 on Architecture).

5.1.3 Critical Policy Decisions to Progress the SCMS within the National Policy Framework for Land Transport Technology

Given that it is the overall role of the SCMS to translate the policy environment into operational policies (that is, security and certificate policy) and technical systems and processes, the Framework contains three critical policy decisions: one implied, and two pending.

The implied policy decision in the Framework relating to the SCMS is:

- The SCMS (in its development and operation) shall be a product of, and will uphold, the seven policy principles agreed to by Australian governments.

The two pending policy decisions in the Framework relating to the SCMS are:

- A statement of intent on standards and deployment models (noting that this will provide necessary guidance for the development of a more formal regulatory framework)
- A nationally agreed deployment plan for the security management of connected and automated vehicles (including a decision on whether a national SCMS is required for Australia).

¹² The nature of outcomes relating to these two considerations may well come to be policy, system management, system operation or user requirements for the SCMS. These potential outcomes cannot yet be expressed in SCMS requirements, but have been accounted for in initial SCMS policy requirements, developed by TCA in the aforementioned discussion paper and work with Austroroads, relating to government involvement, and system operation requirements related to scalability.

5.2 Policy Decisions for the SCMS Implicit In or Potentially Progressed by the National Policy Framework for Land Transport Technology

The purpose of this document is to articulate the policy drivers and decisions necessary to progress the development of a SCMS in Australia.

In so doing, the report notes that many of these decisions – or least discussions that will lead to these decisions – would ideally take place at a national level.

Importantly, the wording and strategic context of the Framework raises the possibility of a number of additional enabling policy decisions that could potentially arise from decisions related to, or affected by, the critical policy decisions relating to:

- A nationally agreed deployment plan for the security management of connected and automated vehicles (including a decision on whether a national SCMS is required for Australia).

The material laid out in the remaining sections of this document is presented for the consideration of policy and decision makers.

The document also notes that a review and establishment of regulatory policy instruments to support C-ITS local deployment is part of a separate deliverable in Austroads' Cooperative ITS (Stage 2) project.

However, key decisions may be implicit in or could potentially be progressed by the Framework Action Item to develop a nationally agreed deployment plan for the security management of connected and automated vehicles, given that:

- These additional requirements will be critical parts of a national approach to security management
- The wording and strategic context of the Framework is such that these additional enabling policy decisions may be directly or indirectly *addressed* in the process of developing a nationally agreed deployment plan for security management
- These additional enabling policy decisions may be directly or indirectly *affected* by a nationally agreed deployment plan for security management that does not take them into account
- A nationally agreed deployment plan for security management will harmonise with the seven policy principles of the Framework, and with the publication of a statement of intent on standards and deployment models (noting that this will provide necessary guidance for the development of a more formal regulatory framework).

It should also be noted that some of these enabling policy decisions may be captured and/or progressed in regulatory, rather than policy, domains. This report avoids making assumptions along these lines in the presentation of these as issues in need of resolution.¹³

¹³ The initial, high level requirements for the SCMS published by TCA themselves capture the necessity of these enabling policy decisions, without making assumptions regarding their precise outcomes, or the way they will have to be implemented from SCMS policy, operation, management, and user requirement perspectives.

5.3 Cooperative Intelligent Transport Systems (C-ITS) Final Policy Paper (National Transport Commission 2013)

The NTC policy paper puts forward eight recommendations in total that are intended to identify policy and regulatory barriers to the deployment of C-ITS in Australia.

While the NTC paper does not relate explicitly to the SCMS, the first four of these recommendations impact how the matter of privacy should be handled in C-ITS and therefore influence SCMS security management.

The pertinent recommendations advanced by the NTC are:

- **Recommendation 1:** That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.
- **Recommendation 2:** That in the development and implementation of a C-ITS operational framework, in particular regarding standards for data messages broadcast by C-ITS stations, Australian governments seek the highest possible level of anonymity for drivers and that this be a key focus for Austroads in developing the framework.
- **Recommendation 3:** That Australian Ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS. In particular, any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information.
- **Recommendation 4:** In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information

Given that these recommendations relate to C-ITS, rather than the SCMS as such, this report has identified that they are neither sufficiently broad enough in scope, nor granular in detail, to progress the development of the SCMS overall.

Nonetheless, these recommendations have informed initial SCMS requirements developed by TCA, and currently being progressed with Austroads (see 6.2 on Privacy).

5.4 Regulatory Reforms for Automated Road Vehicles (National Transport Commission 2016)

The regulatory reform work being progressed by the NTC on automated vehicles – and increases in vehicle automation in general – will be an important and ongoing considerations for Australia's C-ITS deployment, given that the two technologies will converge (along with Smart Cities and Internet of Things initiatives).

Ministers have agreed to a series of reform initiatives over the next two years that are designed to:

- Facilitate increased testing and trialling of more automated vehicles
- Ensure increased confidence in safe performance of more automated vehicles under Australian conditions
- Provide clarity over insurance coverage in the event of a crash
- Develop a more responsive performance-based approach to the regulation of more automated vehicles.

C-ITS and highly automated vehicles are progressing at different speeds, but will come to be interdependent. As one writer puts it:

Autonomous vehicles that aren't connected to each other is a bit like gathering together the smartest people in the world but not letting them talk to each other. Connectivity enables smart decisions by individual drivers, by self-driving vehicles and at every level of automation in between.¹⁴

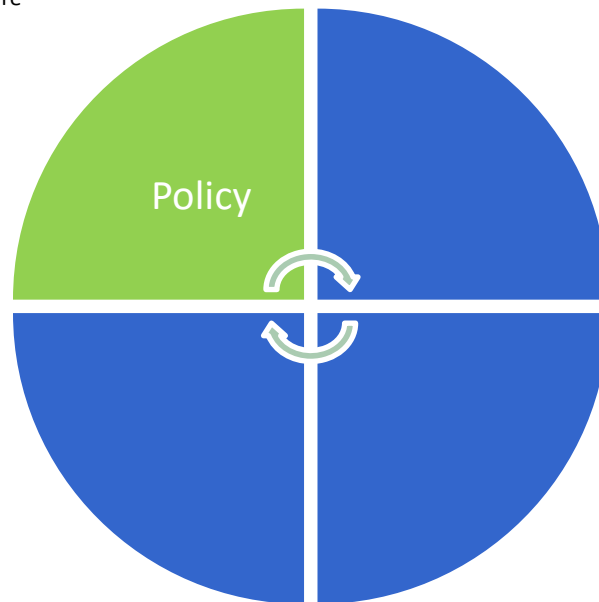
C-ITS connectivity in cars and infrastructure and mobile devices will create a properly connected environment, inclusive of automated vehicles. Moreover, it will supply automated vehicles with information that automated vehicles themselves cannot sense or see within their immediate field of vision.

The work that is being progressed for C-ITS infrastructure from security, standards and interoperability perspectives will be indispensable for automated vehicles and a connected Smart City.

¹⁴ Huei, P. 2016. *Saving lives by letting cars talk to each other*. The Conversation. Available at <https://theconversation.com/saving-lives-by-letting-cars-talk-to-each-other-59221>

6 POLICY

- Architecture
- Privacy
- Legal



Domain role	Establish rules needed to provide guidance for the SCMS, to protect users and businesses, and who makes them
Types of decisions	<ul style="list-style-type: none"> • The underpinning architecture and deployment of the SCMS • How information is gathered, distributed, used and destroyed in a way that it both optimal and compliant • How vehicles will enter the connected SCMS security environment • The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in ensuring this.

6.1 Architecture

6.1.1 Concept

This section presents those policy decisions that are establishing or enabling in nature, and will undergird other key decisions presented in subsequent sections – namely, decisions that will have outcomes related to technical, operational and commercial outcomes.

The policy decisions presented in this part of the document are distinct from those presented in the Strategic Policy section of this document, insofar as:

- No mechanism (e.g. National Policy Framework for Land Transport Technology) has been identified as being the primary mechanism for them to be advanced
- Mechanisms previously identified or forthcoming for progressing these policy decisions may benefit from input from readers of this document.

The purpose of this section is to inform policy and decision makers of the need to answer two fundamental questions:

- What is the desired composition of the Australia deployment of the SCMS – should there be one or multiple?
- What is the desired level of control Australia should have over the SCMS's ability to reflect and operationalise the Australian policy environment in its security outcomes and capability?

This section does not relate to the SCMS architecture as such – this is currently being progressed by TCA with Austroads. Rather, this section relates to decisions that will *underpin* the SCMS architecture.

6.1.2 Root Certificate Authority, SCMS Manager, Public Key Infrastructure (PKI)

To answer these questions, it will be necessary to introduce, at a high level, two important roles in the SCMS, and their significance for policy and decision makers involved in the Australian deployment of C-ITS and the SCMS. These two roles are:

- Root Certificate Authority
- SCMS Manager.

While there is no single point of trust in the SCMS, these two roles are critical for initiating and maintaining the trust that holds the SCMS together. As 'management' components (as opposed to more 'operational' components), they have critical responsibilities in the overall purpose of the SCMS to translate the policy environment into security outcomes for the C-ITS environment.

A SCMS is not possible without a SCMS Manager and a Root Certificate Authority – indeed, in many ways the SCMS Manager effectively is the Root Certificate Authority in overseas SCMS deployments.

The effectiveness of these roles will be affected by issues underpinning SCMS architecture and deployment discussed in this section.

The significance of these roles for the SCMS in general and for the Australian SCMS in particular can be appreciated by understanding the basics of a SCMS architecture based on Public Key Infrastructure.

Public Key Infrastructure (PKI) consists of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of data.

PKI is used to confirm the validity of digital certificates – the electronic 'passports' of users, applications and devices – and that they are coming from a safe and secure source.

PKI is already used in ecommerce, the issuing of new passports, and in telecommunications – environments where confidentiality, integrity, and authentication are essential.

It is also used by government agencies, such as the Australian Tax Office and the Department of Human Service,¹⁵ and in the transport sector for the Intelligent Access Program (IAP).

In the Department of Human Services PKI for example, the Root Certification Authority is called the Human Services RCA, and the operational framework consists of other Certification Authorities (Human Services Organisation Certification Authorities) and End User-Subscribers. The DHS uses PKI to issue certificates to individual healthcare providers and organisations, who can access records systems, professional services, and send secure messages and online transactions.

To take another example, the Australian Tax Office is accredited to operate as a Certification Authority, meeting the evaluation criteria in the Gatekeeper PKI framework (which has also been adopted and adapted for the IAP).¹⁶ The fundamental benefit of PKI is that it handles information about users in such a way that those users can remain *anonymous* to other users (and, indeed, to certain parts of the SCMS) *yet still communicate and be trusted*.

Figure 3 represents a simplified version of a generic PKI trust hierarchy.

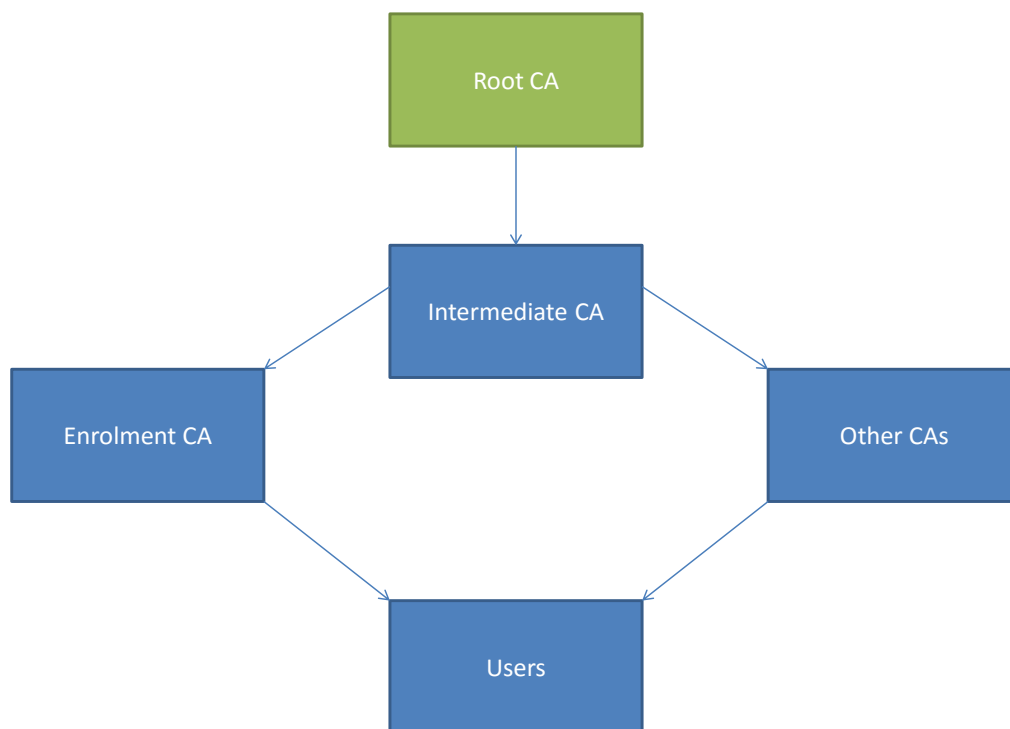


Figure 3 Simplified PKI Trust Hierarchy

¹⁵ See, for example <https://www.humanservices.gov.au/health-professionals/enablers/public-key-infrastructure-pki-policy-documents>

¹⁶ Evaluation criteria can be viewed at <https://www.finance.gov.au/policy-guides-procurement/gatekeeper-public-key-infrastructure/gatekeeper-accreditation-australian-taxation-office/>

The entities represented are:

- **Root Certificate Authority:** The 'trust anchor' for the entire system, from whom all other entities within the PKI inherit their ability to be trusted.
- **Intermediate Certificate Authority:** The physical and cyber safety and security of the Root Certificate Authority is essential. The Intermediate Certificate Authority protects the Root Certificate Authority, and provides flexibility by acting on behalf of the Root Certificate Authority for most interactions.
- **Enrolment Certificate Authority:** The 'entry point' for new users entering the system.
- **Other Certificate Authorities:** The entities that handle day-to-day services for users.
- **Users:** Entities that use the services provided by the system.

6.1.3 PKI as Adapted for SCMS

Figure 4 represents a simplified version of a generic PKI trust hierarchy adapted for a SCMS.

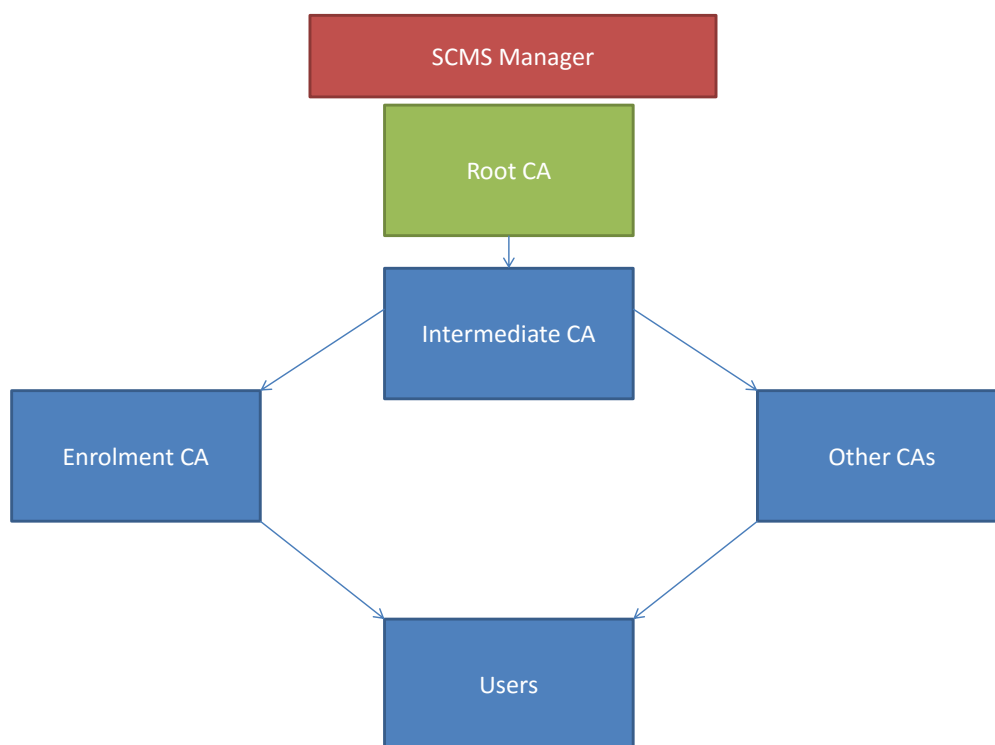


Figure 4 Simplified PKI as Adapted for SCMS

The generic SCMS includes an additional entity to the PKI, the **SCMS Manager**. The importance of the SCMS Manager is discussed throughout this document, and more closely discussed in 9.2.2.

For introductory purposes, the SCMS Manager's role is to:

- Set standards and policies (security and certificate policies, rather than government policy, in coordination with or as the Root CA)
- Ensure compliance with the policy and regulatory environment
- Provide oversight, guidance, consistent interpretation and application of policies
- Liaise between government and industry
- Establish and maintain relationships with international stakeholders and other SCMS Managers.

The SCMS Manager is essential to the deployment of a SCMS:

- Each region that has committed to adopting the SCMS has committed to having a SCMS Manager
- Organisational analyses of SCMS architecture options assume the presence and necessity of a SCMS Manager
- There are key differences in whether a SCMS is publicly or privately operated and managed, or a combination thereof, but there is a SCMS Manager in all of these scenarios
- In overseas deployments, the SCMS Manager effectively is the Root Certificate Authority, and is a public entity.

6.1.4 United States

The differences between the United States and European deployments of C-ITS and the SCMS are noted throughout this report. Both regions have pursued different paths. There is no one reason for this, but overall, the United States is progressing with planned mandating of C-ITS, whereas Europe is progressing a voluntary uptake.

There are subsequently different levels of government and industry involvement in planning and deployment, and different technical approaches to achieving the same or different outcomes.

Both regions are implementing and deploying a SCMS, and their approaches to this have some fundamental differences.

The deployment of the generic PKI for the United States SCMS is represented in Figure 5.

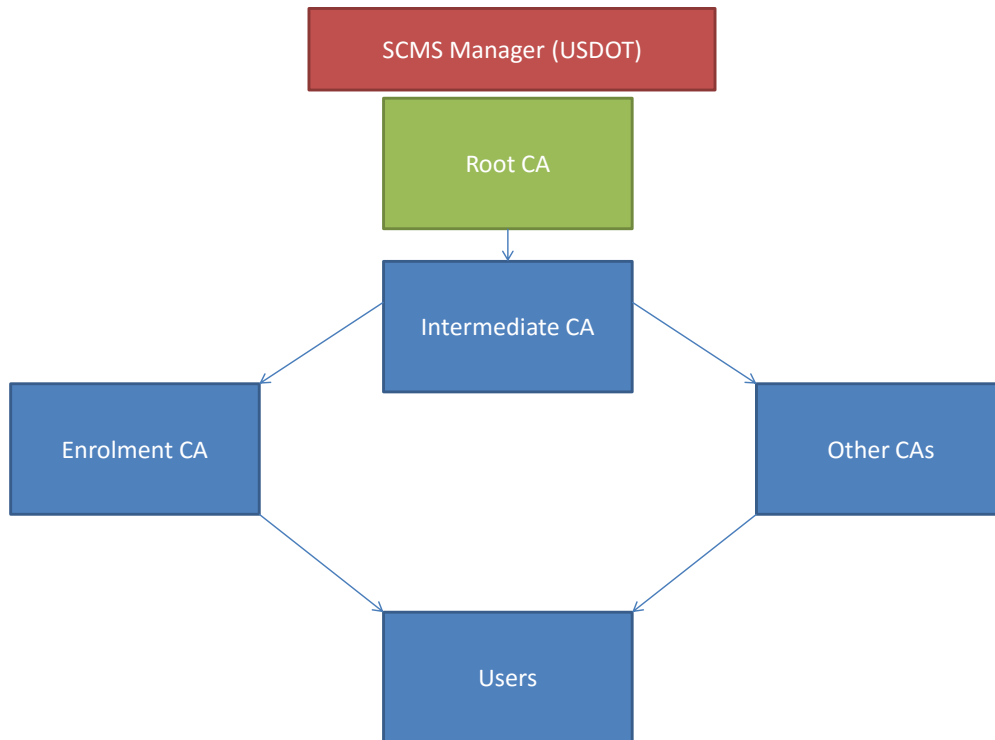


Figure 5 Generic PKI for United States SCMS

The United States have explored SCMS governance, and how best to deploy the SCMS Manager role. The sentiments of industry and the National Highway Traffic Safety Administration (NHTSA)/United States Department of Transportation (USDOT) are captured here:

While agreeing with NHTSA's assertion that a V2V system is not complete without a robust SCMS [the United States deployment of the SCMS], almost without exception, industry commenters vehemently disagreed that a private self-governing industry coalition could be a viable mechanism for SCMS system governance. Commenters believed that a private SCMS could not provide the security, privacy, certainty, stability, long-term functionality, or management of costs and risk required for a nationwide SCMS to support V2V DSRC communications, and lacked the legal authority to address cross-border issues or require industry-wide participation and compliance with uniform requirements. For these reasons, virtually all industry commenters took the position that a strong leadership role for the Federal government in the SCMS would be required for successful deployment.¹⁷

Subsequently, although different governance models may be analysed and trialled, the SCMS will be 'operated for a significant period of time by [US]DOT,'¹⁸ who will take 'a central role in, and direct control over, development of draft policies, procedures and standards that could be the basis for

¹⁷ United States Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications, p. 231. Available at <https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands>

¹⁸ United States Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications, p. 228.

governance of a National SCMS, including draft a Certificate Policy, Certification Practice Statement, Registration Agreements, and Privacy Policy.¹⁹

Additionally, there is little-to-no interest from industry in operating the SCMS Manager component, with private business opportunities identified in operating other SCMS components.

The United States will pursue a centralised SCMS deployment, with the USDOT also operating the Root Certificate Authority component.

Figure 6 provides a more detailed representation of the United States SCMS.

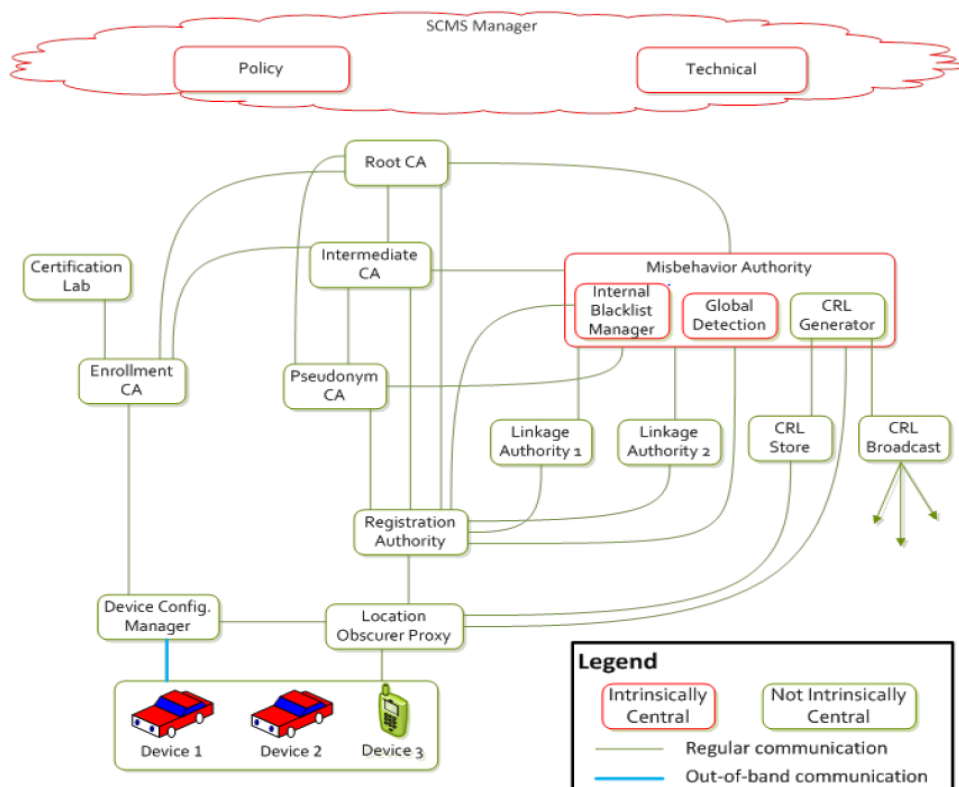


Figure 6 United States SCMS

A detailed understanding of this figure is not important for this document (although it may be useful to refer back to). Note also that the generic entities within a PKI can be identified.

¹⁹ United States Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications, p. 237.

6.1.5 Europe

As discussed, the European SCMS deployment will differ from the United States in many respects. For this section, two key differences need to be understood:

- There are effectively multiple SCMS in that there are multiple Root Certificate Authorities
- The European SCMS Manager has the same responsibilities as the United States SCMS Manager, but for *political* reasons (with technical, operational and commercial consequences) exists as an *equal* – rather than as superior – to the Root Certificate Authorities (and therefore SCMS).

Figure 7 represents a simplified version of the European SCMS deployment:

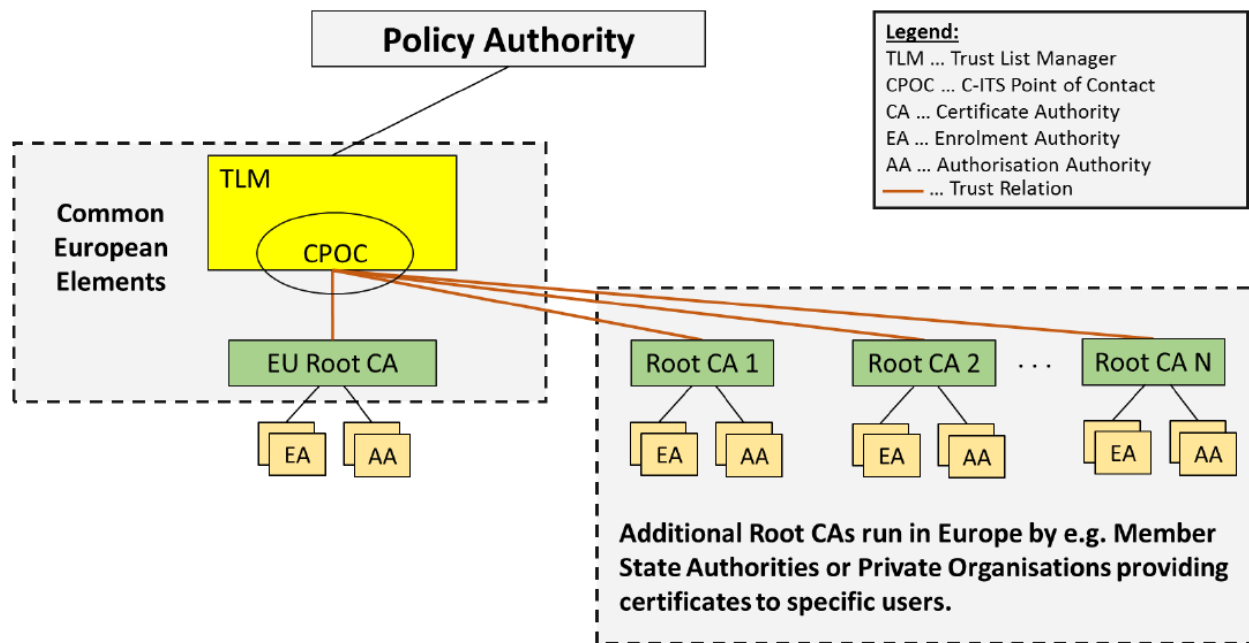


Figure 7 European SCMS Deployment Model

Note: in this model:

- EA (Enrolment Authority) = Enrolment Certificate Authority (ECA)
- AA (Authorisation Authority) = Pseudonym Certificate Authority (PCA)
- The remaining components depicted (Policy Authority, Trust List Manager etc.) are sub-tasks of the overall SCMS Manager role, with the European Commission (JRC) understood to be performing this role²⁰
- Audit function of SCMS Manager is not depicted.

²⁰ See Menzel, G. 2017. C-ITS Deployment in Europe: Common Security and Certificate Policy. Presentation: Third public workshop of the Amsterdam Group and CODECS. Available at <http://www.codecs-project.eu/index.php?id=46>

SCMS in Europe will be controlled by a combination of Member States (two of which are very likely to be Germany²¹ and France), vehicle manufacturers, and *possibly* other industries involved in the C-ITS space.

Internationally and in Europe, there have been substantial efforts to *reduce* the number of SCMS. Whether the European deployment constitutes a successful reduction is debatable, but the outcome nonetheless.

To say that there will be multiple SCMS in Europe is something of an over-simplification. More accurately, Member States and private organisations will have their own Root Certificate Authorities (with the JRC also operating a Root Certificate Authority of its own). Root Certificate Authorities are added into the system and audited by the European Commission. In this sense, Member States and private organisations will be responsible for operating ‘modularised’ SCMS, which together form a European-wide SCMS with a public entity providing oversight and coordination.

For ease of understanding, it is useful to understand this as a federated, multi-SCMS solution, with central European Commission administration and coordination.

The precise number of ‘modularised’ SCMS that will be deployed for day 1 is unknown, as is the extent to which this number could grow over time.

The immediate benefits of reducing the number of SCMS are reduced cost and complexity: a SCMS is a substantial investment, and developing, deploying and maintaining one is a significant challenge.

However, the European outcome demonstrates that SCMS are also *politically* complex – that this outcome is called a ‘federated’ model is itself a politically loaded term.

The European federated model is a product of Europe – unlike the United States – pursuing a non-mandated uptake of C-ITS, and one that is comparatively more driven by industry and public/private cooperation.

However, region-wide deployment of C-ITS is guided the European Commission’s C-ITS Platform (whose reports are cited throughout this document) and by Directive 2010/40/EU of the European Parliament, which notes that:

[D]eployment remains fragmented and uncoordinated and cannot provide geographical continuity of ITS services throughout the Union and at its external borders. To ensure a coordinated and effective deployment of ITS within the Union as a whole, specifications, including, where appropriate, standards, defining further detailed provisions and procedures should be introduced.²²

Unlike the United States, Europe is having to grapple with geopolitical interests, and the labour of having to reach a consistent and acceptable approach for the whole region. The higher level of industry input has also made compromising between public and private interests necessary.

²¹ See 7.3 on Cryptography for the added significance of a German-based CCMS.

²² Directive 2010/40/EU of the European Parliament. 2010. *On the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&from=EN>

Due to a combination of these commercial interests and geopolitical complexities, multiple SCMS will be deployed throughout Europe. This is different from the United States' centralised model, where there is one Root Certificate Authority and one SCMS Manager.

Another reason that a minimal number of SCMS is desirable is because establishing and maintaining inter-SCMS relationship is extraordinarily complex: the benefits of interoperability – of being able to travel between one region's SCMS and another – requires a significant amount of *trust*. Establishing trust is a challenge; maintaining it perhaps more so.

The complexities of this are elaborated throughout this document, especially in 8.2 on Affiliation.

For the purposes of this section, however, it will suffice to note that European SCMS will be required to work together for the benefit of users, the market and policy makers: this relationship is represented by the green band in Figure 8.

The choice *not* to work together – to not have inter-SCMS trust – could be any combination of strategic and political decisions; or technical, policy, commercial or operational inability.

The European Commission has taken an active role in sculpting the role of the SCMS Manager within the SCMS, and is now in the process of exploring the *types* of organisations that could and should operate it. Thus far, they have publicly committed to 'analys[ing] the roles and responsibilities of the European C-ITS Trust Model [i.e. SCMS], and whether some operational functions and governance roles should be taken over by the Commission (as, for instance, in the case of the Smart Tachograph'.²³

The Smart Tachograph is an operational PKI framework for recording driver rest and work activities for compliance control (similar to Australia's Intelligent Access Program (IAP)). In the framework, technical, policy, and certificate processes and functions are managed by the Joint Research Centre (JRC) (a provider of independent scientific advice to support EU policy).

It is highly likely that the Smart Tachograph framework will resemble the deployment of the multi-root, federated SCMS model in Europe, and the role of the JRC will resemble the deployment of a SCMS Manager for Europe.

Figure 8 provides a more detailed version of the European SCMS federated model, depicting three 'modularised' SCMS, each headed by a Root Certificate Authority operated by a Member State or private organisation.

In Figure 7 above, the European Commission/JRC also operates a Root Certificate Authority for states and organisations that cannot, or do not wish to, operate a Root Certificate Authority.

²³ European Commission. 2016. *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, p. 24. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

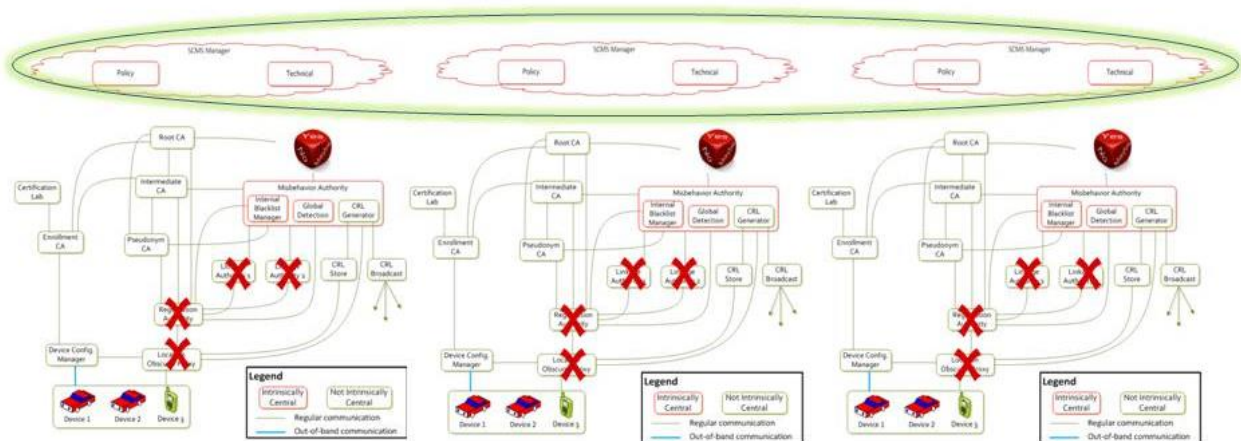




Figure 8 European SCMS Deployment Model Compared to United States

A detailed understanding of this figure is not important for this document (although it may be useful to refer back to). The currently proposed differences between the European and United States SCMS can also be seen. An understanding of these differences is not yet important – these will be made clear in 6.2 on Privacy and 8.1 on Enforcement.

For now, it is important to note that:

-  Denotes SCMS components and functions present in the United States SCMS that Europe is not planning to deploy
-  Denotes SCMS components and functions present in the United States SCMS that Europe is not planning to deploy. However, the 'yes,' 'no,' 'maybe' outcomes represented on the die denote that evolving discussions about these entities and functions are taking place (see 6.2 and 8.1).

Note also that the generic entities within a PKI can be identified.

In their strategy for C-ITS, published December 2016, the European Commission have articulated the challenge in deploying a common security solution for their federated SCMS model:

To develop and establish an EU-wide security framework, based on Public Key Infrastructure technology, for vehicles and public infrastructure elements, including a compliance assessment process, all stakeholders need to be involved. A key challenge will therefore be to set up the necessary governance at EU, national and industry levels involving all main stakeholders, including public authorities (e.g. transport ministries and the responsible national security associations), road operators, vehicle manufacturers, C-ITS service suppliers and operators. Developing a common security solution for the deployment and operation of C-ITS in Europe will in turn lay the foundation for stronger security at higher levels of automation (including vehicle to vehicle and vehicle to infrastructure communication).

The specific actions pinpoint the importance of government involvement in setting the policy environment. Importantly, the second point introduces the possibility that the Commission's JRC will be the SCMS Manager:

- The Commission will work together with all relevant stakeholders in the C-ITS domain to steer the development of a common security and certificate policy for deployment and operation of C-ITS in Europe. It will publish guidance regarding the European C-ITS security and certificate policy in 2017.
- The Commission will analyse the roles and responsibilities of the European C-ITS Trust Model (SCMS), and whether some operational functions and governance roles should be taken over by the Commission (as, for instance, in the case of the Smart Tachograph).²⁴

TCA's working relationship with European stakeholders suggests that their SCMS PKI will be closely based on the Smart Tachograph – an operational regulatory framework similar to the Intelligent Access Program (IAP). The Smart Tachograph records professional driver rest and work activities for compliance control.

While the IAP has some important technical differences to the SCMS, on a framework and policy level, they are more or less identical.

At a high level, there are three main roles and associated responsibilities at the upper management level (which maps onto the SCMS PKI at the Root CA/SCMS Manager level) in the Tachograph operational framework:

- National Root CA – distributes cryptographic keys to Member States
- Administration – provides operational management for 'sub' Root CAs
- Security auditor – audits the Root CA system.

6.1.6 Options

Action Item # 6 in the National Policy Framework for Land Transport Technology reads:

Develop a nationally agreed deployment plan for the security management of connected and automated vehicles.

A key outcome for from this Action Item include a decision on whether a national SCMS is required for Australia.

This decision relates to whether the Root Certificate Authority (the trust anchor for the SCMS, from which all other certificate management entities and C-ITS devices inherit their trust) will be:

- A single Root Certificate Authority located in Australia
- One of multiple Root Certificate Authorities in a multi-SCMS Australian environment
- A Root Certificate Authority located overseas.

²⁴ European Commission. 2016. *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, p. 7-8. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

For Australia, the location of the Root Certificate Authority will have substantial cascading effects for the design, and operation of the SCMS, and will be especially important in determining the level of control over security and certificate policies that will undergird the overall security environment.

The results of the three outcomes are represented below in Figures 9, 10, and 11, with the green arrows representing the chain of trust established by security policies flowing through the SCMS.

Figure 9 represents a single root located in Australia.

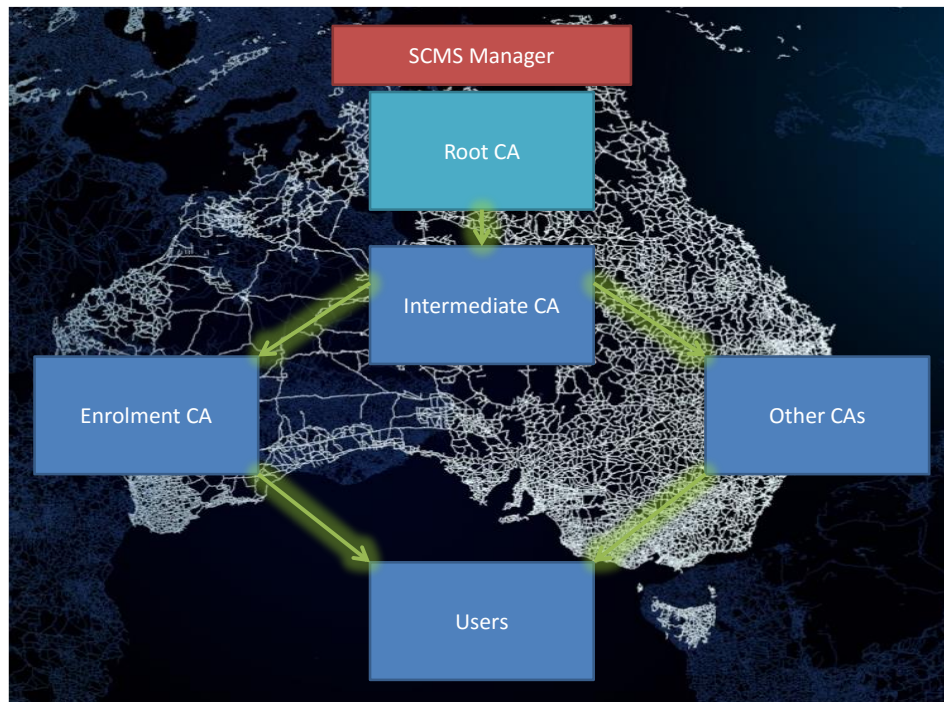


Figure 9 Australian SCMS Deployment, Single Root CA

Figure 10 represents multiple roots in a multi-SCMS Australian environment.

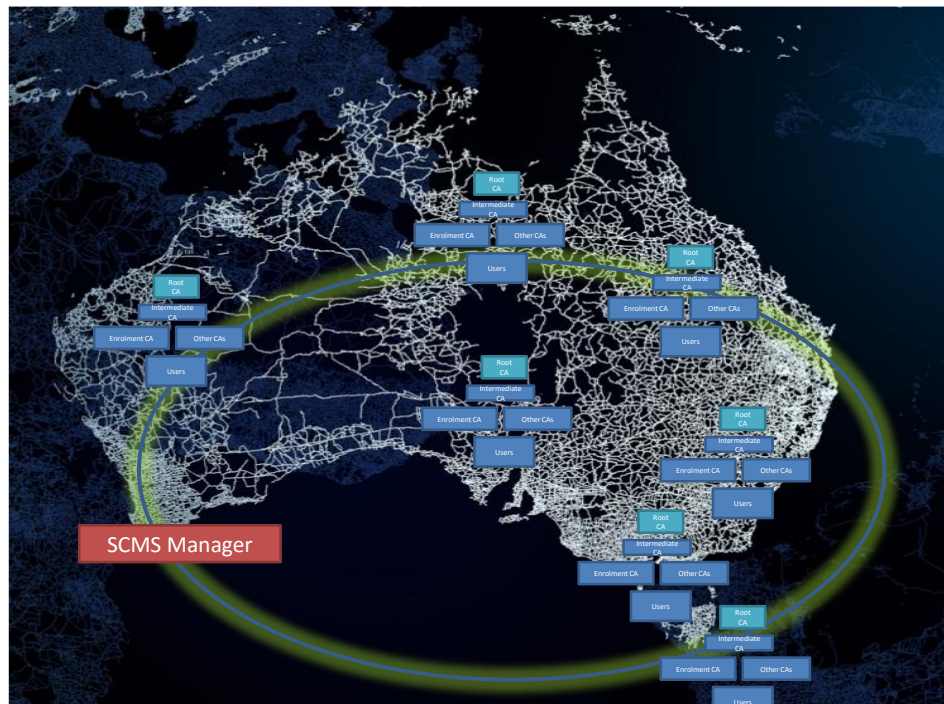


Figure 10 Australian SCMS Deployment, Multiple Root CAs

Figure 11 represents a single root located overseas.

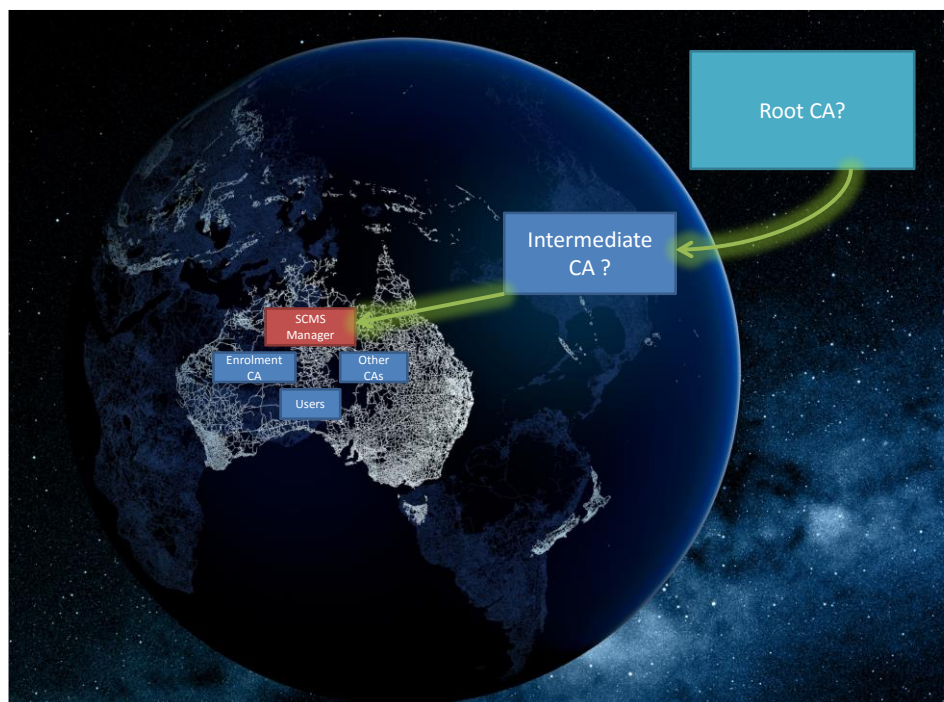


Figure 11 Australian SCMS Deployment, Overseas Root CA

The underpinning Architecture issues for Australian policy and decision makers relate to:

- The desired composition of the Australia deployment of the SCMS – one or multiple?
- The desired level of control over SCMS implementation and responsiveness to the Australian policy environment
- The operational and affiliation risks associated with an overseas Root Certificate Authority.

Figure 9 represents a single, national Australian SCMS – effectively the United States SCMS model, or a single implementation of a European SCMS.

The geographic location of SCMS entities within Australia is not important (provided that functions/entities represented in Figures 6 and 8 are 'centralised' which relates more to oversight than geography).

Figure 10 represents something more akin to the European federated model. For Australia, this would dramatically introduce levels of cost and complexity. Determining, implementing and adjusting a single security policy would be challenging and complex (represented by the green band touching each SCMS) but less so than the European federation model.

A SCMS for each Australian State and Territory would be the least desirable outcome, given that a single SCMS located in one jurisdiction can support multiple jurisdictions – and indeed, the entire nation.

In the scenarios represented in Figures 9 and 10, the SCMS Manager has the principal role of working hand-in-hand with Australian policy and decision makers to implement the operational policy embedded in the highest-order trust certificates issued by the Root Certificate Authority.

The fundamental difference here in Figures 9 and 10 is that the SCMS Manager and policy and decision makers have greater control over:

- *How* the SCMS translates the policy environment into the SCMS policy tools:
 - **Security Policy:** States the rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems.
 - **Certificate Policy:** States what participants, both in the SCMS and users, must do.
 - **Certification Practice Statements:** States practices that a certification authority employs in issuing, managing, revoking, and renewing certificates (discussed in 8.2.4 on SCMS policy tools)
- *How and when* these SCMS policy tools can be changed to reflect changes in the policy environment
- *Which other* SCMS to affiliate with (discussed in 8.2 on Affiliation).

In Figure 11, the Root Certificate Authority is located overseas (and the location of the Intermediate Certificate Authority is undetermined).

In the scenario in Figure 11, depending on the location and or entity of the Root Certificate Authority overseas, the control that policy and decision makers have to make decisions about the operation of the SCMS based on the Australian policy environment, and the affiliations that the Australian SCMS has by extension of using an overseas Root Certificate Authority, may be substantially reduced.

If the Root CA for Australia is overseas (i.e. there is no national SCMS) Australia will have little say in affiliation processes, and SCMS policy tools (Security Policy, Certificate Policy, Certification Practice Statements) will be to a greater extent in the hands of the overseas party.

Indeed, it would mean that these policy tools would be effectively 'off the shelf' rather being tailored to Australia's policy environment, and Australia would largely have to find ways to work around this: there is a possibility that this would be easier for deployment, but changes in the policy and operational environment as it matures would pose significant difficulties.

An overseas Root Certificate Authority and the location of the Intermediate Certificate Authority may also pose day-to-day and long term operational complications for other Certificate Authorities in the SCMS, such as the Enrolment Authority.

A number of entities involved in the automotive, regulatory and administration would also have to interface with an overseas operator – adding administration and complexity.

Having an overseas Root Certificate Authority is not the same decision as having the Root Certificate Authority operated by an organisation that is not also the SCMS Manager.

'Outsourcing' of the Root Certificate Authority *could* be performed on the assumption that the SCMS Manager could audit and intervene both in the event of an emergency, and to tailor the Security and Certificate Policies and Certification Practice Statements (these SCMS policy tools are discussed in 8.2 on Affiliation) as needed to enhance or correct capability or errors.

There are additional considerations here, explored in the Affiliation section. These relate to the extent to which a more technical architecture may be influenced by decisions to align on a policy level with overseas SCMS deployments, such as those in Europe. In one scenario, this may allow Australia to deploy a local multi-Root Certificate Authority environment and model (with some operated by industry, yet with public oversight, as in Europe). Decisions of this magnitude would ideally be informed by more 'first principles' decisions included in this report.

The immediate deployment and long-term complications of having an overseas Root Certificate Authority are not fully known, primarily because no region is considering this option. The European situation, whereby some Member States and other SCMS operators will go through the JRC as the Root Certificate Authority, is not a comparable scenario, given that the JRC is understood to be SCMS Manager.

That an overseas Root Certificate Authority is not being contemplated by any region is largely because a SCMS and C-ITS in general will largely be an unprecedented phenomenon, and the complications of managing the regulatory and commercial are not yet fully known – and will not be fully known for years to come. Whether an overseas Root Certificate Authority would want to fulfil this role for Australia – or any other country – is also unknown.

It is therefore reasonable to conclude that a national Root Certificate Authority is both a political point (a 'sovereign' SCMS seems to be desired by all parties, given that the Root Certificate Authority is the trust anchor for the *entire system*) and a way of managing the potential risks relating to policy control over technical and operational matters.

6.1.7 Parties Responsible for Advancing Decision

TISOC/Austrroads are the lead entities on the Action Item in the Policy Framework for Land Transport Technology, which is to be delivered in mid-2018, that will determine whether a national SCMS is required for Australia.

TCA has also progressed significant work on the more technical aspects of SCMS architecture with Austrroads, including an exploration of additional options for harmonisation and potential integration with the European SCMS environment.

6.2 Privacy

6.2.1 Concept

In the report, *Digital Disruption: What do governments need to do?*, the Productivity Commission note that the introduction of information and communications technology, such as telematics, into vehicles has a number of implications. On the topic of privacy and cybersecurity, they write:

The development of connected and autonomous vehicles and smart infrastructure will generate an increasing quantity of data on road users, raising potential privacy concerns for users, depending on the use and maintenance of that data by data collectors, governments and third parties (either through purchase or unauthorised access to data). In addition to privacy concerns, malicious attacks on operating systems have the potential for substantial economic and safety impacts.²⁵

This excerpt usefully captures the importance of the linkages between privacy, digital security and physical safety – not to mention the economic and user-confidence linkages.

How data is used and maintained in a C-ITS environment, and the role of the SCMS in fostering privacy, is of critical importance. There are a number of ways that this role can be supported by policy and technical design choices, and these need to be explored and established.

In any connected system that receives, stores and issues information to or about an entity (even if that information is de-identified) security and tracking threats are inevitable – this is as true for a workplace, and for C-ITS in general as it is for the SCMS.

It should therefore be an overriding goal that the SCMS not be a net contributor to these threats, while still ensuring that it can provide the required levels of support for C-ITS users and the environment.

The *Information Security Manual* rightly points out that 'Using any cryptographic product, algorithm or protocol is not sufficient in itself to adequately reduce the likelihood of compromise.'²⁶ Section 7.3 of this document draws attention to this in its discussion of the need for ongoing management, maintenance and risk mitigation of cryptographic operations.

However, internal management of privacy is more important than cryptography: 'If [cryptographic] capability is poorly configured, it can lead to an actual reduction in overall security, as the system may be used to carry more sensitive information with little to no improvement to security.'²⁷

²⁵ Productivity Commission, *Digital Disruption*, p. 182.

²⁶ *Information Security Manual, Principles*, p. 53.

²⁷ *Information Security Manual, Principles*, p. 53.

Cryptography is a fundamental part of privacy for C-ITS and the SCMS. But overall privacy measures should aim to be robust enough so that any efforts to circumvent or compromise them are:

- *Difficult* – from a technical and knowledgebase perspective
- *Expensive* – in hours, dollars and computing power
- *Risky* – the consequences of being caught should be clear, whether the breach is successful or unsuccessful (explored in 6.3 on Legal).

Together this should:

- *Prevent* malicious attacks from occurring
- *Discourage* malicious entities from attempting attacks in the first place.

6.2.2 Users and Commercial Operators

In addition to policy, privacy will be an important marketing and communications task to ensure adoption the initial and ongoing participation and confidence of users and industry.

In addition to being assured that their data is safe and secure, users will need to be informed of the uses to which their data will be put. It is inevitable that a portion of users of C-ITS will be suspicious that their in-vehicle C-ITS devices will be used by police for the purposes of issuing traffic infringements.

A clear policy position on what data C-ITS – and, by extension, the SCMS – will receive, store, transmit and discard and destroy will be especially important to alleviate privacy concerns and suspicions that C-ITS and the SCMS together form a ‘tracking’ or government ‘spying’ system.

On the other hand, C-ITS, including the SCMS, is:

just one element of both Smart Cities and Smart Society initiatives and that data from ITS will be integrated to them is important. Thus data that may be considered as “privacy protected” in the limited context of 5GHz co-operative ITS, may have that protection challenged in wider systems where correlation of the ITS data with other behavioural data may serve to identify an individual or a community of individuals.²⁸

This excerpt makes the very useful point that, for policy purposes, C-ITS (and related transformations to the transport network) need to be considered holistically, and as developments that will *converge*. That this convergence may rely on some of the same data resources is a distinct possibility – for practical, technical, commercial and economic reasons.

TCA’s initial SCMS requirements have noted that scalability and extensibility are SCMS requirements from the outset. This points to the need for clear decisions to be made in this area that spell out what data will be used for. The initial SCMS requirements assume the necessity of decisions being made in this area, but do not assume the shape or nature of these decisions themselves.

²⁸ EU-US ITS Task Force Standards Harmonisation Working Group Harmonisation Task Group 1. 2012. *EU-US Standards Harmonisation Task Group Report: Status of ITS Security Standards. Document HTG1-1*. European Commission/United States Department of Transportation, p. 74.

User and government needs and expectations may change over time – and, indeed, users may come to expect that as few data streams are used as possible for the delivery of multiple commercial and regulatory services.

However, for deployment and day 1 purposes, ambiguity will be a hindrance to user take up of C-ITS, and to user trust in the SCMS.

Privacy by design principles have been recommended by the NTC for C-ITS (noted in 5.3) and have been adopted into initial SCMS requirements developed by TCA so as to plan to mitigate deliberate and accidental non-compliance with privacy policy.

6.2.3 Clear Position on Privacy Policy for Users, Industry, and for Inter-SCMS Trust and Interoperability

How a C-ITS deployment handles privacy – as a policy position, implementation decisions, and as something requiring ongoing management – will be scrutinised when trying to establish and foster inter-SCMS relationships, and users and commercial developers do not want to ‘cut off’ from the global C-ITS market or environment (see 8.2 on Affiliation).

For users, a safe and secure system that protects their privacy will be both an assumption and an expectation. The day-to-day experience of a successful system will be reliable, seamless and interoperable digital transactions.

The effort required to meet this assumption and expectation will fall squarely on the organisations that operate and maintain systems like the SCMS.

Initiating, obtaining and maintaining inter-SCMS trust will be a significant and ongoing task to be carried out by SCMS Managers, who are both knowledgeable about the capabilities and requirements of their own SCMS, and the risks posed by others. This is detailed and discussed in 8.2 on Affiliation.

This effort will be invisible to users, but they will experience the results when they can travel between trust domains – that is, between SCMS – with confidence, and with as little interruption as possible.

Privacy is therefore a policy decision. But it is also an implementation decision, and the desired level of privacy will need to be reflected in SCMS development and operation.

6.2.4 United States

Privacy is not just an external threat – there is always the potential for ‘insiders’ to do just as much damage as ‘outsiders,’ either deliberately or accidentally.

The United States have gone a step further than Europe by building measures into the SCMS architecture that ensure as much as possible that, even if a SCMS entity were subject to an intrusion, there would be insufficient information available to the intruder, making an intrusion both *expensive* and *unrewarding*.

In the United States, SCMS entities are effectively ‘blind,’ and no single entity has enough information to identify the full complement of certificates associated with a device.

In addition to entities within the SCMS being 'blind' and the two Linkage Authorities (discussed in 8.1 on Enforcement) the Registration Authority in the United States SCMS 'shuffles' requests for pseudonym certificates, which ensures that the Pseudonym Certificate Authority cannot identify that two separate requests came from the same user.

A second feature in the United States SCMS lacking in Europe is the Location Obscure Proxy function, which ensures that the location of users requesting certificates is not disclosed to SCMS entities.

These are two prominent examples of the additional privacy measures built into the United States SCMS, the overall effect of which ensure that no SCMS entity alone has enough information about a user, or their full complement of certificates.

The approach taken by the United States could be usefully described as 'privacy-by-design'.

Along these lines, the United States SCMS is composed of legally and administratively distinct entities, each with clearly (or soon to be clarified) circumscribed roles and responsibilities.

6.2.5 Europe

The European approach to privacy is strongly linked to their approach to enforcement, as discussed in 8.1.

As noted, the European SCMS does not (currently) have the two Linkage Authorities present in the United States SCMS, nor does it (currently) have Location Obscuration, and its Registration Authority does not (currently) propose to shuffle requests.

Together, these have produced a less complex SCMS than the United States'.

However, European discussions and reports are quickly evolving, and it is likely that internal security will become more robust for day 1 deployment, and increase over time. It is likely that these will not be as advanced as the United States model, but will resemble it in some way nonetheless (and this is likely to progress in unison with any changes to enforcement capabilities, discussed below).

6.2.6 Identifying Information for Enrolment (and thus Participation)

At a high level, privacy threats can be assessed by considering:

- Who or what is identified
- The extent to which they can be reasonably identified by a party
- Who these parties are, and under what circumstances they can make these linkages.

The presence – or level – of user/vehicle information linked to the system for the purposes of enrolment (defined and explained in 4.1) is yet to be determined.

However, it is expected that there will be – at some level – an ability for the linkage of the enrolment with a specific vehicle.

This information could potentially include information directly or indirectly linking the C-ITS device to vehicle identification number (VIN). This would in turn enable linkages to be made to vehicle make/model/year, or potentially, information about the production batch from which the C-ITS device comes. For example, a C-ITS device could potentially contain information such as a VIN or a vehicle registration, depending on the policy decision that has yet to be determined.

This information may or may not be included as a 'canonical identifier,' and it is highly likely that there will be a need for this identifier to be globally unique – that is, associated with a single C-ITS device. There is currently no clear answer as to how these identifiers would be coordinated in a globally controlled way, although both the United States and Europe are highly aware of the problem, and recognise the urgent necessity of a solution.²⁹

The enrolment stage is particularly important, because it is connected to the 'bootstrap' stage of a C-ITS device, which encompasses certificate installation and certification: that is, ensuring that the device is fit for purpose, will work in-service, and is equipped with the materials it will need to participate in the C-ITS environment.

These issues impact critical SCMS requirements to support a C-ITS device across its lifecycle – that is, from the moment it enters the SCMS (i.e. deployed in the C-ITS environment) to when it leaves (no longer used, de-commissioned, disposed of, see 8.3.2 on Lifecycle management).

This process introduces multiple threat opportunities, yet will also be commercially important, given that manufactures will be frustrated if they have to satisfy different enrolment/bootstrap processes and requirements.

Getting the enrolment stage wrong could also have serious operational consequences – an error at this stage may, for example, necessitate a physical recall of the vehicle/C-ITS device for updates (rather than remote updates).

The need for decisions in this area has linkages to the NTC recommendation that *any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information* (Recommendation 3).

There are privacy policy decisions to be made in this area that will affect SCMS operational policies, and may affect the responsibilities of SCMS certificate authorities and entities, the levels of access to information they can have and, to take a likely consequence, their ability to link an enrolment certificate with a vehicle (which may be an authorised or unauthorised operation).

In one possible scenario, the vehicle manufacturer may be required to maintain information linking enrolment with a specific vehicle. In this scenario, the vehicle manufacturer would may an active role in Misbehaviour Management (see 8.1 on Enforcement), recalls and end of life processes.

This potential scenario highlights that SCMS requirements for Misbehaviour Management and end of life processes cannot fully be developed without making a number of critical assumptions about policy decisions that will impact roles and responsibilities both for SCMS entities, and entities affected by the SCMS.

This specific decision is likely to be connected more broadly with the development of a nationally agreed privacy approach for C-ITS.

²⁹ Work in this area is currently being progressed by TCA, the USDOT and the European Commission through HTGs.

6.2.7 Policy and Legislation

It was noted above that privacy measures should aim to be robust enough so that any effort to circumvent or compromise them is *difficult* (from a technical and knowledgebase perspective) and *expensive* (in hours, dollars and computing power) so as to *prevent* and *discourage* malicious entities.

A C-ITS and SCMS deployment will also need to ensure that the legal consequences of infringements are sufficiently clear in order to:

- Deter malicious entities when weighing the benefits of success against the risks and penalties of getting caught (noting that minimising likelihood will be managed by the SCMS Manager)
- Guide the technical implementation and management of the system, to ensure initial and ongoing compliance.

There are number of policy domains and Acts of legislation relevant to the design, implementation, deployment and ongoing operation of the SCMS, explored in 6.3 on Legal.

6.2.8 Options

Privacy is a policy decision *and* an implementation decision. The outcomes sought will affect what privacy measures are made available.

In simplified terms, the United States have pursued a more 'privacy by design approach' where information security is assured by the system itself (the number of components implemented, their roles and responsibilities, how information flows through the system in a defined, technical way.

By comparison, Europe have followed a 'risk management' approach, where information security is not 'built into' the system to the same extent, but implemented by management practices and oversight over components, producing a less technically complex system, with fewer components.

Neither approach is better than the other – and in some cases, they achieve similar outcomes in different ways. However, they are design and architectural solutions to different risk appetites and policy outcomes.

As the discussion above highlights, clarity and consistency will be key for users and industry, and to ensure harmonisation and interoperability. As such, decisions about privacy will be as important as communicating these decisions locally and internationally.

As discussed in 6.3 on Legal, a regulatory environment that applies to, but was not built for, C-ITS exists nationally and on a jurisdiction-by-jurisdiction level. Additional options for consideration are presented in 6.3.

Unlike the United States, Europe must also provide flexibility for Member States, while still implementing a region-wide solution to the greatest possible extent.

It would be advantageous for Australia to pursue a national approach as much as possible.

The material outcome of a multi-regional approach to privacy in Australia would very likely frustrate users and the market, and make inter-SCMS trust difficult to initiate and maintain.

On the topic on enrolment, this document does not make a recommendation for this specific issue, given that at the time of writing, it is understood that it is one currently being grappled with by both the United States and Europe. Moreover, neither is currently expressing a preference or probable outcome – indeed, it would not be inconsistent for the two regions to choose different approaches.

While it would be consistent for Australia to align with the European deployment scenario, care should be taken to ensure that this decision (and those similar to it) align first and foremost with Australian user expectations relating to privacy and security, and is consistent with the interpretation and application of existing Australian legislation to C-ITS in general and the SCMS in particular.

Awaiting an international decision should not deter policy makers from establishing their own clear outcomes and expectations.

6.2.9 Parties Responsible for Advancing Decision

This is a matter where policy thinking and direction will have very significant impacts on the commercial, technical and administrative costs of operating a SCMS – and decisions that will impact Australian deployment of C-ITS.

User and commercial expectations and assumptions are also key factors.

This would ideally be advanced at a national level, involving input from all jurisdictions.

Privacy and data usage measures are directly tied to policy decisions and outcomes, and may have impacts on SCMS architecture. The entity designated as SCMS Manager would be logically positioned to inform policy and decision makers, for day 1, and moving forward:

- What is available
- What the costs would be
- How policy intent can be realised
- Where policy intent may conflict with other requirements, such as privacy.

The evolving discussion in Europe, and the fast pace at which decisions are likely to be made, means that continued involvement in and monitoring of the European situation is critical for Australia. TCA's co-leadership of HTGs provides the ideal forum for this.

Communicating and learning from developments beyond day 1 will be an ongoing stakeholder engagement task for the SCMS Manager.

The roles and responsibilities of vehicle manufactures, and how they relate to the SCMS will need to be progressed with the industry. Technical and administrative questions will arise here, with the SCMS Manager logically positioned to provide technical information in tandem with policy outcomes.

6.3 Legal

6.3.1 Concept

It is the overarching purpose of the SCMS to translate the Australian policy and regulatory environment into technical and operational processes and policies that deliver security support and services for the C-ITS environment.

Relevant legislation will be of critical importance, both for enabling C-ITS, and to make sure that the SCMS – in its design, implementation, deployment and ongoing operation – is compliant.

While other sections of this document detail the paths being taken in the United States and Europe, presenting this comparison, and any options that would arise from it, is largely of little value for policy and decision makers here, given that legislation is specific to Australia.

Short of a detailed comparison, this document makes the observation that the two approaches have produced very different results.

Australia has pursued neither of these paths, and there are multiple pieces of legislation and related policy that are relevant to the SCMS, yet were not written with C-ITS or the SCMS in mind.

This document therefore notes that the interpretation and application of this legislation for C-ITS in general, and the SCMS in particular, has not been tested.

The extent to which it may require a nationally consistent approach remains to be determined, although common sense points to the benefits.

As noted in 6.2 on Privacy, there is an additional need to *deter* malicious entities who may be tempted to launch attacks on the SCMS, and many of the penalties associated with malicious activities will be captured in legislation.

Section 6.2 on Privacy also identifies the need for a decision regarding the extent to which a C-ITS will be linked to the system for the purposes of enrolment – that is, for the purposes of entering into the C-ITS and SCMS environment.

6.3.2 United States

The likely mandating of 5.9GHz DSRC in the United States where all new vehicles would be equipped with C-ITS capability has provided a great deal of focus and momentum in essential areas, and shaped pre-implementation activities.

This is the case such that pre-competitive industry consortiums and cooperatives have been able to resolve and advance technical, managerial and operational problems and decisions, either on behalf of, or to the distinct advantage of governments attempting to sound out regulatory details, desirables and necessities.

In the United States, there is greater market certainty surrounding C-ITS, and regulatory and policy reform have been guided by a single goal, with the SCMS factored into *all* discussions.

6.3.3 Europe

In Europe, much of the enabling policy and legislation for, or relevant to, the SCMS either does not exist, or is inadequate in its existing form.

In Europe, the more market-based approach to C-ITS is guided by directives from the European Commission. These directives have the force of law, but negotiation and compromise across Member States has seen the need for a coherent legislative framework for day deployment is now urgent.³⁰

Nonetheless, the European Commission is acutely aware of the problem at hand. This, and the urgent need for resolution have animated discussion; regionally, Europe have the personnel and resources (and policy guidance) to progress matters accordingly.

In their strategy for C-ITS, published December 2016, the European Commission have identified specific actions to be undertaken for development of a legal framework for C-ITS, namely:

- Ensuring continuity of C-ITS services
- Laying down rules to ensure security of C-ITS communications
- Ensuring the practical implementation of the General Data Protection Regulation in the area of C-ITS
- Ensuring a forward-looking hybrid communication approach
- Laying down rules on interoperability
- Laying down rules on the compliance assessment processes.³¹

6.3.4 Need for Clear and Consistent Interpretation and Application of Existing Legislation for Privacy

As noted above, there are multiple pieces of legislation and related policy that are relevant to the SCMS, yet were not written with C-ITS or the SCMS in mind. Privacy is discussed in 6.2, given its decisive importance for users, industry, and international harmonisation.

In 2013, the NTC released a policy paper that addressed a number of privacy concerns for the introduction of C-ITS. While the NTC has written that there are, in general, no regulatory barriers to the introduction of C-ITS in Australia, this document notes that the NTC did not consider the SCMS in any great detail.³²

For compliance with surveillance regulation, a clear position on how SCMS data can or will – or cannot or will not – be used for enforcement purposes, the conditions under which it can be obtained by enforcement officers (by warrant, for example) will very likely affect user trust in the system and uptake of C-ITS more broadly, and has therefore been identified as an enabling policy decision, and also discussed in 6.2 on Privacy.

³⁰ European Commission. 2016. *C-ITS Platform. Final Report*, p. 66. Available at <http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf>

³¹ European Commission. 2016. *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, p. 11. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

³² Requirements for the completion of a Threat, Vulnerability and Risk Assessment (TVRA) and of a Privacy Impact Assessment (PIA) have been included in TCA's initial set of SCMS system operation and policy requirements, to reflect the necessity of compliance with privacy legislation – as have requirements to maintain confidentiality and privacy.

Beyond enforcement, for example, data collected under certain privacy conditions for the SCMS may have those conditions challenged in another scenario where the data is seen as an enabler of broader Smart Cities and Internet of Things (IoT) initiatives, also discussed in 6.2 on Privacy.

6.3.5 Need for C-ITS Enabled Vehicles to be Compelled to Use and Receive Credentials from the SCMS

Much of the discussion in Australia and abroad has focussed on the types of C-ITS applications that should (either through regulation or policy position) be required to be supported by the SCMS: safety and non-safety applications, and how to determine which applications qualify as safety and non-safety applications.

While noting the value of an application-centric approach to compliance assurance options, and the importance of this for SCMS operations, the enabling policy decision would be to determine more generally how C-ITS devices should be compelled to use the SCMS and be enrolled into the C-ITS environment via the SCMS.

It should also be noted that the bootstrap/enrolment processes have been identified as highly needed for international harmonisation (discussed in 6.2 on Privacy and 8.2 on Affiliation).

For applications, whether the SCMS should be used beyond securing the foundation messages (i.e. Cooperative Awareness Message [CAM], Basic Safety Message [BSM]³³ or Decentralised Environmental Notification Message [DENM]) to include other applications will be driven by a number of factors.

Where interoperability between vehicles and infrastructure is required, a trusted model for security is important.

As an example, the broadcast of a 'heartbeat' Cooperative Awareness Message (CAM) that can be relied upon by receiving C-ITS devices who may choose to operate safety applications based on this information would benefit from requiring the SCMS to provide security services.

Without the use of SCMS security services, it will become difficult to rely on the information being provided: without them, and associated certification and enrolment processes, determining whether the broadcaster of a message should be trusted may not be feasible.

6.3.6 Privacy and Surveillance Regulation and Policy

Government regulation and policy for privacy and surveillance exists at both the Commonwealth and the state and territory level. Separate privacy and surveillance regimes also apply to state and territory public sectors.

Table 6 below provides an overview of the key regulations and policies relating to privacy and surveillance that have implications for the design, implementation and operation of the SCMS.

A more detailed treatment of the material presented in this table has been supplied in TCA deliverables to Austroads.

³³ The European and United States 'heartbeat' messages broadcast by vehicles, respectively. Australia is yet to determine which of these it will implement as a national – or jurisdictional – standard.

Table 6 Privacy and Surveillance Regulation and Policy

Regulation/Policy	Instruments affecting SCMS
Privacy Act 1988 (Cth)	<p>The Privacy Act is the principal piece of Australian legislation protecting the handling of personal information. It regulates the collection, use, disclosure, security and access of personal information. A private sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way. The Privacy Act will not apply if information does not identify an individual.</p> <p>Regulatory instruments under the Privacy Act 1988 relevant to the SCMS likely to include:</p> <ul style="list-style-type: none"> ▪ Australian Privacy Principles Privacy Regulation 2013
State & Territory Privacy Acts	As a general rule, compliance is required with both the Commonwealth and the relevant state/territory laws.
NSW – Privacy and Personal Information Act 1998	
Vic – Privacy and Data Protection Act 2014	
Qld – Information Privacy Act 2009	
SA – no specific privacy Act	
WA – no specific privacy Act	
TAS – Personal Information and Protection Act 2004	
ACT – Information Privacy Act 2014	
NT – Information Act 2000	
Surveillance Devices Act 2004 (Cth)	<p>The Surveillance Devices Act 2004 (Cwlth) sets out conditions for federal law enforcement agencies to use surveillance devices to track locations and to listen to conversations.</p> <p>The NTC final policy paper found that the Surveillance Devices Act 2004 will probably apply to federal agencies seeking to use C-ITS information. However, this does not apply to state road agencies or state police forces.</p>
State & Territory Surveillance Laws	State and Territory-based surveillance laws which are much broader and prohibit covert surveillance of any person and by any public or private entity.

Regulation/Policy	Instruments affecting SCMS
<p>Cooperative Intelligent Transport Systems (C-ITS) Final Policy Paper (NTC 2013)</p>	<p>This policy paper puts forward eight recommendations in total. The first four of these recommendations impact on how the matter of privacy should be handled in C-ITS and therefore influence SCMS security management.</p> <p>Recommendation 1: That Austroads adopt privacy by design principles, including the undertaking of a privacy impact assessment, in the development of the C-ITS operational framework.</p> <p>Recommendation 2: That in the development and implementation of a C-ITS operational framework, in particular regarding standards for data messages broadcast by C-ITS stations, Australian governments seek the highest possible level of anonymity for drivers and that this be a key focus for Austroads in developing the framework.</p> <p>Recommendation 3: That Australian Ministers explicitly consider privacy impacts on drivers in any decision relating to institutional arrangements for C-ITS. In particular, any entity that manages and stores unique identifiers is separate from agencies which hold licensing and registration information.</p> <p>Recommendation 4: In the event that individuals can be reasonably identified from the safety data message broadcast by C-ITS devices, that specific legislative protections are developed to define in what circumstances organisations that are exempt from compliance with privacy principles, including enforcement agencies, may access C-ITS personal information.</p>

6.3.7 Security Regulation and Policy

Government regulation and policy for the security of information and systems exists at both the Commonwealth and State/Territory government levels.

Table 7 below provides an overview of the key regulations and policies relating to security that have implications for the design, implementation and operation of the SCMS:

Table 7 Security Regulation and Policy

Regulation	Instruments affecting SCMS
Criminal Code Act 1995 (Cth)	The Act is the primary source of 'criminal law' at the Commonwealth level. Of relevant to C-ITS and security, it codifies ICT offences, including cybercrime offences.
State and Territory Security Acts	The 'criminal code' contains a comprehensive set of offences to address cybercrime. These offences are based on model laws agreed to by Commonwealth, State and Territory governments. Examples of criminal codes relevant to C-ITS security include: The offences are consistent with those required by the Council of Europe Convention on Cybercrime, and are drafted in technology-neutral terms to accommodate advances in technology.
ACT – Criminal Code 2002	State and Territories have computer and related offences.
NSW – <i>The Crimes Act 1900</i>	
NT - Criminal Code Act 1983	
VIC – Crime Act 1958	
QLD – <i>Criminal Code Act 1899</i>	
SA – Criminal Law Consolidation Act 1935	
TAS – Criminal Code Act 1924	
WA – Criminal Code Act Compilation Act 1913	
Cybercrime Act 2001 (Cth)	Cybercrime refers to crimes directed at ICT (such as hacking and denial of service attacks), and also to crimes where ICT are an integral part of an offence (such as online fraud, identity theft). The <i>Cybercrime Act 2001</i> (Cth) and the mirror State legislation criminalise cybercrime activities. They also impose heavy penalties on offenders and increase police powers of investigation.
Telecommunications (Interception and Access) Act 1979 (Cth)	The primary purpose of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system. The second purpose of the TIA Act is to specify the circumstances in which it is lawful for interception of, or access to, communications to take place.

6.3.8 Consumer Protection Regulation

Government regulation and policy for consumer protection exists at both the Commonwealth Government and the State and Territory government levels.

Consumer protection laws will be one of the key tools for ensuring that fit for purpose products are delivered.

State and Territory Governments have their own consumer watchdogs who perform a similar role to the ACCC for their own jurisdictions.

Table 8 below provides an overview of the key regulations relating to consumer protection that have implications for the design, implementation and operation of the SCMS:

Table 8 Consumer Protection Regulation

Regulation	Instruments affecting SCMS
Competition and Consumer Act 2010 (Cth)	<p>Australian Consumer Law (ACL) is Schedule 2 of the CCA. Consumer protections covered by ACL relevant to C-ITS include:</p> <ul style="list-style-type: none"> • Product is of acceptable quality and fit for purpose • Product matches supplier descriptions • Product safety and information • Conditions and warranties • Liability of manufacturers for goods with safety defects • Spare parts and repair facilities.
	ACL Regulations
	<p>Vehicle safety recalls are conducted under the provisions of the ACL. The Department of Infrastructure and Regional Development (DIRD) carries out safety investigations on behalf of the Australian Competition and Consumer Commission (ACCC). These may be either due to a safety issues that could cause injury within the terms of the ACL, or due to non-compliance with ADRs or other legislative requirements of the MVSA. ACL Regulations also cover conditions and warranties, and the need for suppliers to make spare parts and repair facilities available for a reasonably time after purchase.</p>
	Codes of Practice
State & Territory Motor Car Trader/Dealer Acts	<p>While not regulatory instruments, the key automotive industry associations (incl. FCAI, TIC) have Codes of Practice for the Conduct of an Automotive Safety Recall.</p>
	<p>States and Territories will have various regulatory instruments under their Acts that deal with the rights</p>

Regulation	Instruments affecting SCMS
NSW – Motor Dealers and Repairers Act 2013	and obligations of both motor vehicle traders and purchases. Both new and used vehicles are covered by the regulations. This is important to the lifecycle management of C-ITS devices as performed by the SCMS.
Vic – Motor Car Traders Act 1986	
Qld – Motor Dealers and Chattels Auctioneers Act 2014	
SA – Second-hand Vehicle Dealers Act 1995	
WA – Motor Vehicle Dealers Act 1973	
TAS – Motor Vehicle Traders Act 2011	
NT – Consumer Affairs and Fair Trading Act	
ACT – Sale of Motor Vehicles Act 1977	

6.3.9 Options

The importance of legal certainty for the design, deployment, implementation and ongoing operation of the SCMS cannot be underestimated – it is critical for policy and decision makers, for users and the market, and for international trust and harmonisation purposes.

Australia has pursued neither of the paths taken by the United States or by Europe.

Comparisons between the United States, Europe and Australia are likely to be of limited value for implementation purposes, given the complexity of Australia's legislation, and the markedly different paths each region has taken, and the complexities of their own legislation – be it C-ITS or SCMS specific, or more general in nature.

While the NTC has written that there are, in general, no regulatory barriers to the introduction of C-ITS in Australia, this document notes that the NTC did not consider the SCMS in any great detail. This document therefore notes that the interpretation and application of this legislation for C-ITS in general, and the SCMS in particular in Australia has not been tested.

Options to progress the matters discussed above are broken down below.

Need for C-ITS enabled vehicles to be compelled to use and receive credentials from the SCMS

Options for this matter are explored in more detail in 6.2 on Privacy.

Further consideration could be given to requiring the use of SCMS security services for all safety-related applications and could be enabled for optional use for commercial applications.

The initial set of SCMS requirements developed by TCA requires that the SCMS is capable of supporting applications as needed, and it is therefore an initial requirement that the CMCS be agnostic of communications medium, given that applications will use multiple communications methods.

Consideration could also be given to requiring the use of the SCMS security services for all safety-related applications and could be enabled for optional use for commercial applications.

Need for clear and consistent interpretation and application of existing legislation for privacy

It is entirely feasible that the SCMS could progress and sit within the context of both national and jurisdictional regulation.

A clear (national) position would be important to inform the progression of the SCMS across the diverse range of stakeholders involved (government, industry, international parties and users).

Promoting this position would also make the consequences of attempted or successful malicious behaviour clear to potential bad actors, and serve as a deterrent.

No specific regulatory measures for the SCMS have been proposed, and the need for them has not been identified. Testing this assumption would be advisable.

The details for regulatory compliance would likely be best investigated by an entity strongly associated with the design and deployment of the SCMS, and it would be logical that this entity would also have a stake in the ongoing operation of the SCMS. The SCMS Manager would be ideally positioned to initiate this detailed investigation.

Privacy and surveillance regulation and policy

The Acts above are complex pieces of legislation, and SCMS compliance will be required. Regulations in this area primarily relate to the protection of information, but there are currently no plans for SCMS specific regulations. Testing this assumption would be advisable.

There are numerous issues to consider here:

- Complexity of legislation and level of risk associated with non-compliance
- The presence of *exemptions for enforcement purposes and transport agencies*
- Uneven level of maturity of Australian C-ITS decision-making in this area
- Desirability of aligning Australia's C-ITS and SCMS deployment with overseas activities, where issues are still progressing.

More generally, there is a need for clarity surrounding the interpretation and application of this legislation for the SCMS.

It would be highly advisable that legal advice to clarify the implications of these pieces of legislation be sought by the appropriate entity at the pre-implementation phase.

Given that the NTC recommendations relate to C-ITS, rather than the SCMS as such, this report has identified that they are neither sufficiently broad enough in scope, nor granular in detail, to progress the development of the SCMS overall.

Noting that SCMS requirements that relate to these regulations will need to be progressed when the situation becomes clearer, the necessity of these decisions are captured in the areas of policy decisions relating to:

- An entity to be empowered as SCMS Manager (9.2.2)
- Clarity on extent to which C-ITS device will be linked to vehicle and system enrolment (6.2.6)
- Need for a SCMS business model (9.1)
- Need for clear and consistent interpretation and application of existing legislation for privacy (this section and 6.2 on Privacy)

Security regulation and policy

The Acts above are complex pieces of legislation, and SCMS compliance will be required. Regulations in this area primarily relate to the protection of information, but there are currently no plans for SCMS specific regulations.

Many offences that could potentially be conducted by malicious entities are covered in these Acts. Compliance and alignment with the *Information Security Manual* and the *Protective Security Framework*³⁴ would either be advisable or obligatory.³⁵

It has been noted by Austroads³⁶ that there are potentially significant, widespread and onerous complications associated with the Telecommunications Act for road agency use of C-ITS, and this may very well impact the SCMS.

It would be highly advisable that legal advice to clarify the implications of these pieces of legislation be sought by the appropriate entity at the pre-implementation phase.

Consumer protection regulation

The Acts above are complex pieces of legislation, and SCMS compliance will be required.

There are numerous issues to consider here:

- Complexity of legislation and level of risk associated with non-compliance
- The presence of *exemptions for commercial uses*
- Uneven level of maturity of Australian C-ITS decision-making in this area
- Desirability of aligning Australia's C-ITS and SCMS deployment with overseas activities, where issues are still progressing.

Compliance with these regulations will significantly depend on the role of vehicle manufacturers and suppliers in relation to the SCMS.

³⁴ Attorney-General's Department. *Protective Security Framework*. Australian Government. Available at <https://www.protectivesecurity.gov.au/Pages/default.aspx>

³⁵ As such, compliance with the *Information Security Manual* and the *Protective Security Framework* have been captured in initial SCMS requirements developed by TCA.

³⁶ Austroads. 2012. *C-ITS 5.9GHz Spectrum Management and Device Licensing Regime Report*. Austroads, Sydney: Australia, p. 6.

They may have a range of responsibilities, at different levels, relating to the information for which they are responsible at enrolment. This may relate to Misbehaviour Management and revocation (8.1), which may or may not be linked to repairs and recalls of vehicles and C-ITS devices.

Manufactures may also have a role related to functions relating to Device Configuration Manager³⁷ in overseas deployments – a role that may or may not be expressly present in the Australian deployment.

It would be highly advisable that legal advice to clarify the implications of these pieces of legislation be sought by the appropriate entity at the pre-implementation phase.

Noting that SCMS requirements that relate to these regulations will need to be progressed when the situation becomes clearer, the necessity of these decisions are captured in the areas of policy decisions relating to:

- An entity to be empowered as SCMS Manager (9.2.2)
- Clarity on extent to which C-ITS device will be linked to vehicle and system enrolment (6.2.6)
- Need for C-ITS enabled vehicles to be compelled to use and receive credentials from the SCMS
- Need for outcomes desired on enforcement capabilities (8.1)
- Need for a SCMS business model (9.1)
- Need for clear and consistent interpretation and application of existing legislation for privacy (this section and 6.2 on Privacy).

6.3.10 Parties Responsible for Advancing Decision

This document notes that a documented review of policy and regulatory instruments supporting C-ITS is to be set in place by Austroads by late 2016 as part of its C-ITS Stage 2 work program (Project No. NT1785).³⁸

TCA has progressed some of the material relating to initial SCMS requirements, and security standards and options for surrounding compliance assurance measures with Austroads. Parties responsible for progressing the legal issues identified above are noted below.

Need for C-ITS enabled vehicles to be compelled to use and receive credentials from the SCMS

This matter is explored in greater detail in 6.2 on Privacy.

Jurisdictional applications of existing regulations are likely to be in operation, although a national solution would be ideal, given the likelihood of these frustrating users and the market in equal measure.

³⁷ Device Configuration Manager is a specific entity/function in the United States CCMS, while the European CCMS has the more generic configuration management entity/function. This entity/function coordinates between the C-ITS device and Certificate Authorities, especially at enrolment when the device first enters the CCMS.

³⁸ Austroads. Project Details. Available at <http://www.jr.net.au/Austroads/Project/Details.aspx?ProjectID=1299>

This report does not suggest a preference or policy or regulatory instrument to achieve this requirement, but it does note that this would ideally be part of an integrated, nationally agreed deployment plan for security management, or at least progressed in unison with this deployment plan.

The SCMS Manager would be logically positioned to advise on the how compelling a C-ITS enabled vehicle to use the SCMS would affect other technical, policy, commercial and operational issues for the design and deployment of the SCMS, and where privacy conflicts may arise.

The roles and responsibilities of vehicle manufactures, and how they relate to the SCMS will need to be progressed with the industry. Technical and administrative questions will arise here, with the SCMS Manager logically positioned to provide technical information in tandem with policy outcomes.

It should also be noted that the bootstrap/enrolment processes have been identified as highly needed for international harmonisation.

TCA's current and future participation and co-leadership of international HTGs would be the ideal forum for monitoring this.

Progressing updating, and communicating their availability would be an ongoing task for the SCMS Manager.

Need for clear and consistent interpretation and application of existing legislation for privacy

Jurisdictional applications of existing regulations are likely to be in operation, although a national solution would be ideal, given the likelihood of these frustrating users and the market in equal measure.

This is more generally a matter for C-ITS. Thus, a clear position on C-ITS data management in general, and SCMS data management in particular, relating to access, storage, management and destruction of data would ideally be the result of nation-wide consultation, and progressed as part of, or alongside, a national deployment plan for security management, given the cascading effects to functionality and inter- and intra SCMS security and certificate policy this would have.

As explained in 9.2.2, the SCMS Manager would be logically positioned to advise on the how a consistent interpretation of privacy matters for the SCMS would affect other technical, policy, commercial and operational issues for the design and deployment of the SCMS, and where conflicts may arise.

Privacy and surveillance, security and consumer protection regulation and policy

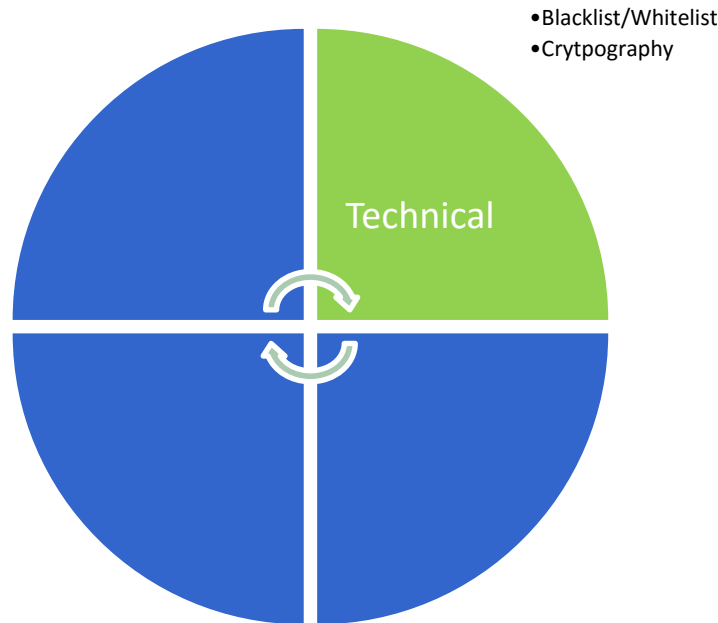
The above sections note that for each domain, it would be highly advisable that legal advice to clarify the implications of these pieces of legislation be sought by the appropriate entity at the pre-implementation phase of the SCMS.

Jurisdictional applications of existing regulations are likely to be in operation, although a national solution would be ideal, given the likelihood of these frustrating users and the market in equal measure.

The SCMS Manager would be expected to ensure system-level compliance with existing legislation in the design, implementation, deployment and ongoing operation of the SCMS, and to ensure SCMS entities' compliance through certificate and security policies and ongoing audit activities.

Empowering an entity as SCMS would allow these activities to progress in consultation with policy and decision makers.

7 TECHNICAL



Domain role	Establish what the SCMS should do, and how it should do it
Types of decisions	<ul style="list-style-type: none"> • How to mitigate risk, and protect the security and safety of users • How information is protected and able to be exchanged, and how user ability to be trusted is confirmed.

7.1 Blacklist / Whitelist

7.1.1 Concept

Trust needs to permeate the C-ITS environment, at each system and at every level.

By the same token, degraded trust – which may be caused by faulty or malicious applications, software, devices and entities – can filter through the C-ITS environment, and cause any number of problems, from minor disruptions and inconveniences, to disasters that threaten current and future operations, and the privacy and safety of users.

The ability to manage threats to the environment, and to reduce the risks associated with degraded trust, is of a very high importance. This ability is necessary both for:

- ***Intra-SCMS operations*** – *trust threats must be able to be managed internally, between SCMS entities.* The SCMS fosters trust; if entities within the SCMS cannot be trusted, this has cascading effects throughout the C-ITS environment.

- **C-ITS devices/users** – a driver's system should only receive and rely on trusted messages from trusted systems. Drivers will be unwittingly vulnerable to breaches and degradations of trust. They themselves may knowingly or unknowingly be the initial source, or have the ability to propagate, a threat to others or themselves.

There are strong policy, technical and organisational/operational linkages and overlaps here with the ability to remove – that is, to *revoke* – misbehaving application, systems and entities, and these are explored below in the discussion on enforcement below in section 8.1 on Enforcement.

These linkages and overlaps present themselves because these are complementary aspects of what needs to be an overall security strategy.

The two options explored in this section are both ways to identity applications and systems whose messages or operations cannot be trusted and acted not upon: Blacklisting and Whitelisting.

The basic difference is how they do this: Whitelisting does it 'pre-emptively'; Blacklisting does it 'non-pre-emptively' – these are not perfect descriptions, although to describe them as either wholly 'proactive' or 'reactive' is something of an over-simplification.

As the names suggest, putting one of either of these two concepts into practice implies simple decisions – white/black, yes/no, good/bad, trust/distrust, allow/disallow. In reality, the matter is more complicated.³⁹

International deployment plans in both Europe and the United States indicate that a combination of Blacklisting and Whitelisting will be used in both regions, both for the SCMS and for C-ITS more generally.

It is important that decision makers are presented with concepts and options so as to inform the development of their strategic planning.

7.1.2 Blacklisting

A Blacklist is a list of applications, systems and devices that have been deployed, and subsequently identified, in an operational environment as a live or potential threat. The threat may be minor or major, and the cause of the threat may be intentional or unintentional.

Anti-virus and malware detection products are common uses of Blacklists. The software may automatically detect malicious software (malware) and either block installation or use, or strongly recommend that the user discontinue use.

In another scenario, a user may notice some suspicious or malicious software, and alert their system administrator, who will then put that software on a Blacklist; meaning that no user in that environment can download or use that software. Alternatively, the system administrator may identify that a user's account has been infected with a virus, and is sending spam to other users.

In these cases, the identification of Blacklisted software is a combination of automated and manual processes, and the user's system has been compromised without their knowledge.

³⁹ In addition to Blacklisting and Whitelisting is 'Greylisting': temporarily blocking or denying something, and then allowing it when certain conditions are satisfied. Greylisting is used, for example, when temporarily blocking or rejecting an email from an unknown sender, or from the same sender sending a large number of emails. The concept and practice of Greylisting could be used, for example, for certain C-ITS applications, applied to other C-ITS systems, or shape security strategies. It is not discussed in this report, but could be considered as a method where neither Blacklisting nor Whitelisting will suffice, and therefore by exception. It should be noted that Greylisting is *not* being widely discussed in overseas deployments.

In an office, a system administrator may Blacklist websites that distract employees (such as Facebook) or may have a Blacklist of known pornographic websites that employees cannot access on their office computer. If the system administrator discovers that a user is accessing websites similar to Facebook, or visiting pornographic sites that are not Blacklisted, they may add those sites to the Blacklist – along with the user. In these scenarios, the Blacklisting process is manual, and is a combination of proactive and reactive.

These familiar examples can be applied to C-ITS: intentionally or unintentionally misbehaving – be they active or potentially misbehaving – applications, systems and devices are identified as and when they pose a threat.

The expectation is that their identification is performed by the SCMS. The SCMS Manager actively monitors – or has oversight over the entity that performs these monitoring duties – the environment, and maintains a Blacklist that is then broadcast to users.

Although proactive steps can be taken, such as when Blacklists are shared between two or more SCMS (not necessarily a given, but could be achieved with very active stakeholder engagement, which is the responsibility of the SCMS Manager) each entity is not screened and vetted before deployment, as is the case with Whitelisting.

Where the threat of malware can range from annoying emails to the extraction of sensitive business and user information, it is largely unfeasible to assume that real or potential threats in a C-ITS environment could be treated as minor inconveniences as far as near-ubiquitous safety applications are concerned.

A misleading message delivered in real-time while driving on the road is likely to be just as dangerous as an altogether fake message – it is important to remember that in C-ITS, *receiving* a message needs to be *exactly the same* as *relying* on a message: a driver cannot take a crash avoidance message as a helpful hint.

If the device is broadcasting a message that cannot be trusted, that device needs to be removed (this is largely the role of revocation, explored in 8.1 on Enforcement). But if an application is misbehaving on one device, there is a risk that this threat may extend to other devices using the same application. In this case, the application needs to be Blacklisted.

For commercial applications with lower user uptake delivering non-safety critical information, however, a higher level of risk may be tolerated by users and governments alike, with the consequences of sub-optimal performance deemed worth the reduced oversight.

In the example above, it was noted that a user may notice some suspicious or malicious software, and alert their system administrator. Whether *users* rather than their *systems* will be able to do this in a C-ITS environment for day 1 deployment is yet to be determined, but is more likely to be a future advancement. That the process will be increasingly automated should be assumed.

For intra-SCMS operations, it may be discovered that a SCMS entity has been compromised, and is issuing certificates to the wrong type of users, or that cryptomaterial has been extracted by a malicious intruder.

In this case, the certificates that this entity has issued should not be trusted, and devices need to be prevented from acquiring new certificates from this entity. These devices may themselves need to be removed from the environment. This is the role of revocation, closely tied to the enforcement operations discussed in 8.1 on Enforcement.

A Blacklist would logically be shorter than a Whitelist, but it is expected that a Blacklist will require rapid updating, to minimise the amount of time a threat can remain in operation.

The primary proposed use of Blacklisting for C-ITS is for Certificate Revocation Lists (CRL) – essentially a list of:

1. Applications that are not to be trusted, and are to be ignored and their use temporarily or permanently discontinued
2. Devices that are not allowed to request new certificates (and thus continue to use C-ITS) and who may be removed, depending on the desired enforcement capability (outlined below in 8.1, although this is likely to be unavailable for day 1)
3. Intra-SCMS or interface entities that have been compromised, and whose operations and users (those issued certificates from the entity) need to cease operations, and cease to be trusted by users.

7.1.3 Whitelisting

A Whitelist is a list of applications, systems and devices that have been identified as being trusted before being deployed in an operational environment. Anything that is not on the Whitelist cannot be used.⁴⁰

As a practice, Whitelisting is newer than Blacklisting, although both are by now well-established parts of a security strategy.

Whitelisting is generally much more effective than Blacklisting. Indeed, Whitelisting of applications is ranked as the most effective (no.1 of a total of 35) mitigation strategies for cyber intrusions, as prepared by the Australian Department of Defence, Cyber Security Operations Centre (as a list of strategies to complement the *Information Security Manual*).

Its effectiveness is ranked as 'essential' on this list of mitigation strategies, and the reason for this is that all applications must be vetted before deployment: there are 'no unknown' applications in a Whitelisted environment.

In an office environment, if a user wanted to use a piece of software that had not been Whitelisted, they would need to contact the system administrator, who would assess the site or software, and then add it to the Whitelist.

From this example, it is easy to see the benefits of Whitelisting. It is considered highly effective because the default status is to distrust everything, and to screen all new entrants into an environment.

The trade-off is that more upfront administrative effort is required, and there are in turn more upfront costs.

The Australian Department of Defence, Cyber Security Operations Centre rates user resistance to Whitelisting as 'medium.' How this would play out for C-ITS application developers is not yet tested, although Whitelisting is widely thought to be looked on favourably by international C-ITS and SCMS

⁴⁰ The more technical description supplied in the *Information Security Manual* defines application Whitelisting as 'An approach in which all executables and applications are prevented from running by default, with an explicitly defined set of executables allowed to execute.' *Information Security Manual, Principles*, p. 62.

stakeholders for some operations (relating to intra- and inter SCMS) and may have the benefit of strengthening international alignments.

The Cyber Security Operations Centre rates the ongoing maintenance costs of Whitelisting as 'medium.' For C-ITS, it is widely thought that Whitelisting will nonetheless require constant permissioning (rather than *ad hoc* de-permissioning for Blacklisting) and will be comparatively slower than Blacklisting.

It would be reasonable to expect that Whitelisting would provide beneficial assurances for non-commercial applications and uses of C-ITS – that is, for safety-critical applications whose misbehaviour may threaten safety and/or user confidence and uptake.

It is expected that a Whitelist will require rapid updates, primarily to reduce the pre-deployment period, and to keep pace with the number of applicants that would otherwise not have to undergo the vetting processes for deployment with Blacklisting. Updates would also be required if misbehaviour was evident or suspected, and Whitelist status withdrawn.

There are two possible uses of Whitelisting for C-ITS, effectively creating Certificate Trust Lists (as opposed to Certificate Revocation Lists):

- Applications: Whitelisting at this level would ensure that only vetted applications are run in a vehicle, and that they are not modified or tampered with
- Intra-SCMS: Whitelisting at this level would ensure that SCMS entities can be trusted. It would be especially important for when a new entity is added to the system, and ensuring that trust is recognised and flows throughout the system.

While the effectiveness of Whitelisting has been noted, it is important to realise that these evaluations have an office or workplace in mind – not the transport *network*, and not the commercial market of C-ITS application developers. This has been discussed internationally, but certification (discussed in 8.3) of applications rather than Whitelisting is the far more probable and effective deployment path.

7.1.4 Options

The comparative Table 9 below captures the differences and similarities between Whitelisting and Blacklisting, and their proposed use for C-ITS:

Table 9 Blacklisting vs Whitelisting

	Blacklist	Whitelist
Control	<i>Consultative</i> Input from multiple intra-SCMS entities and users/devices allows a Blacklist to be developed and maintained on an ongoing basis. The composition of the Blacklist <i>may</i> benefit from input from multiple organisations, although international acceptance and mutual recognition will require a high level of stakeholder management.	<i>Authoritative</i> A single organisation or group of decision makers need to decide what will, or will not, be allowed. It is generally accepted that Whitelisting strengthens international alignment with other SCMS.
Threat identification	<i>Post-discovery, reactive</i> The Blacklist can only be added to once an issue has been identified. Higher likelihood of time-sensitive identification and updating for operational entities. Pro-active when threats identified in one domain are communicated to other domains.	<i>Pre-discovery, proactive</i> New entrants must be vetted before deployment. Added assurance, but can add delay to deployment.
Automation/Effort	<i>Higher automation/Post-discovery effort</i> Higher levels of automation. Resources directed at further investigations. Smaller list overall.	<i>Lower automation/Pre-discovery effort</i> Lower levels of automation. Resources directed at pre-deployment vetting stage. Larger list overall. Sharing Whitelists between domains can reduce time and effort.
Flexibility	<i>Greater</i> Trust levels can be changed more readily to correspond with the severity and reach of the threat. Rapid updates will be required.	<i>Slightly Lower</i> The level of trust is largely determined at the outset, with greater effort, although can be changed relatively easily. Rapid updates will be required.
Trust	<i>Manageable at all levels</i> Trust levels can be managed at all levels with less effort prior to adding to Blacklist. Rapid updates will be required.	<i>Manageable at all levels</i> Trust levels can be managed at all levels with less effort after adding to Whitelist. Rapid updates will be required.

	Blacklist	Whitelist
Deployment of new entrants	Immediate New entrants commence without delay, provided they are not Blacklisted elsewhere (if recognition is enabled and fostered).	Delayed New entrants cannot be deployed unless vetted. Sharing Whitelists between domains can reduce time and effort.
Uses for C-ITS	Certificate Revocation List Applications. Devices. Intra-SCMS.	Certificate Trust List Applications. Intra-SCMS.

How a SCMS and a C-ITS environment in general manage risk will be a cornerstone of a security strategy.

It will also play a strong role in determining how trusted and reliable that environment is for its users, and will impact interregional and inter-SCMS interoperability, trust, perception and alignment.

The rhetorical and practical differences between a Blacklist and a Whitelist imply a binary choice between the two. However, choosing one over the other is very likely to be unwise – both have benefits and disbenefits.

European and United States deployments will use both Blacklisting and Whitelisting – that is, they will use a combination based on risk management principles. Whitelisting will be especially important for establishing trust between Root Certificate Authorities in their federated model, and the SCMS Manager playing coordination role.

This means that Blacklisting may be used at one ‘level’ and Whitelisting will be used at another.

It is therefore more likely to be a choice of how and when to use one over the other, rather than the choice of a single option.

The use of Blacklisting for Certificate Revocation Lists (either for applications, devices or SCMS entities) is common to both European and United States deployments although in *fundamentally different ways* (noting that Blacklisting is also a technical practice and concept relating to enforcement activities, discussed in 8.1).

Whitelisting for intra-SCMS entities, both initial and additional entities, would create a high level of trust for the system that provides security essentials for the C-ITS environment. Certificate Trust Lists for intra-SCMS entities are also common to overseas deployments.

Whitelisting for core (that is, near-ubiquitous and safety critical) applications may have advantages. However, Whitelisting has not been deployed for the transport *network*, nor for the commercial market of C-ITS application developers. This has been discussed internationally, but certification of applications (discussed in 8.3 on Certification) rather than Whitelisting is the far more probable deployment path.

The ongoing costs associated with picking one over the other are yet to be fully analysed. However, it will be important to consider the potential costs (economic, safety, reputation, confidence) of a misbehaving device or application (as captured in the Table 4 at the start of this report).

Although Whitelisting may be comparatively slower than Blacklisting, rapid updates will be necessary for both.

A combined approach is entirely feasible, and will require some careful decision making. It is also entirely possible that an overarching security strategy emphasises one practice over the other, while still using a successful combination.

7.1.5 Parties Responsible for Advancing Decision

This will be a strategic conversation of a policy nature with technical outcomes.

This would ideally be advanced at a national level, involving input from all jurisdictions, and the entity designated as SCMS Manager.

A combined approach to Blacklisting and Whitelisting is entirely feasible, and consistent with international deployments – but combined approaches that differ on a jurisdictional level would severely hamper interoperability, increase administration and user dissatisfaction, and frustrate the market.

A national SCMS would substantially reduce the likelihood of jurisdiction-based decision making.

The SCMS Manager's ability to provide advice and guidance on how to translate policy intent into commercially, technically and operational viable outcomes would be greatly beneficial to decision makers.

Communicating the outcomes of this decision to international stakeholders will be a matter of formal policy position, and an ongoing stakeholder engagement task for the SCMS Manager.

7.2 Cryptography

7.2.1 Concept

Cryptography is the technique of sharing information that is neither accessible nor understandable to unintended parties. Only intended parties can 'crack the code,' and there are no 'eavesdroppers'.

Cryptographic operations are fundamental to the operation of the SCMS, given that it is based on PKI: it ensures that confidential information is not readily available, and is essential to resolving the competing tensions inherent in the system: that is, the ability be *simultaneously anonymous and trusted*.

This section covers two important areas related to cryptography that are yet to be resolved for the Australian SCMS, and for the deployment of C-ITS in general:

- The selection of a cryptographic curve – a common 'secret' language, that enables interoperability, privacy and trust
- The need for cryptoagility – the need to think beyond day one, to ensure that security is a process, not a product.

C-ITS and the SCMS will use a type of cryptography called Elliptic Curve Cryptography, the technical details of which are not especially important for this report.

Elliptic Curve Cryptography is a highly specialised area. The key decisions surrounding it are in some respects quite straightforward. However, some careful thought will be required, given that this topic is bound to geopolitical tensions, especially in Europe.

There are essentially two elliptic curves available for C-ITS cryptographic operations (such as encryption to protect sensitive information, and digital signatures to verify the authenticity of entities without identifying them personally) – NIST and Brainpool (both using 256 key length).

Both NIST and Brainpool curves and the proposed 256 key length are fit for purpose from security perspectives, and for the computer processing power of a C-ITS device used for C-ITS deployment.

While the selection and implementation of a cryptographic curve is a security fundamental, it is worth highlighting that a cryptographic curve can be usefully compared to a language that C-ITS devices and systems like the SCMS will use to communicate with one another.

A decision in this area is therefore essential, not just as a basic security fundamental, but for the purposes of ensuring interoperability.

7.2.2 Europe

Europe in particular has grappled with geopolitical tensions on the topic of selecting a curve. Through the European Commission's C-ITS Platform, Europe is currently approaching a region-wide approach following industry and policy negotiation and comprise. This is taking place against the backdrop for the urgent need for a single security and certificate policy for day 1 C-ITS deployment in Europe.

Debate is being driven by competing geopolitical and industry priorities not present in other regions. To take the most prominent example, in Germany it is illegal to use NIST for critical infrastructure, and Brainpool will therefore be the official cryptographic language.

According to the latest information, Europe will be implementing both Brainpool and NIST. For Day 1, European SCMS components will need to support both curves; C-ITS devices will be required to support NIST, and will have the option of supporting Brainpool as well. Within four years, however, C-ITS devices will be required to implement both curves.⁴¹

7.2.3 United States

In the United States, the adoption of NIST, given the curve's origin (U.S. National Institute of Standards and Technology) and current level of government and industry penetration, is comparatively uncontested, and something of a moot point for policy purposes.

It is not yet clear if the United States would consider adopting a similar approach to that taking shape in Europe. If they did it would be reasonable to assume that would support both NIST and Brainpool, but endorse NIST as their primary curve.

It is clear, however, that the United States is implementing NIST alone.

⁴¹ European Commission. 2017. *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*. Release 1. Available at https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

7.2.4 Cryptoagility

The implementation and maintenance of security in this area will largely be realised through the requirement for cryptoagility (the ability to update and adapt cryptographic operations, policies and backwards capability) rather than the selection of a curve as such.

Requirements for cryptoagility are, in this sense, more important than the selection of curve, but are SCMS requirements, rather than an enabling policy decision.

Cryptoagility is required for a number of reasons, discussed here. However, practical steps cannot be progressed until a decision relating to a curve is made.

The overall PKI framework for the SCMS and C-ITS more generally will rely on cryptographic operations both for encrypting messages and for digital signature processes (signing and verifying the authenticity of users).

Cryptoagility is the ability of a protocol to adapt to evolving cryptography and security requirements. This may include the provision of a modular mechanism to allow cryptographic algorithms to be updated without substantial disruption to fielded implementations.

The European C-ITS Platform has investigated the broad needs for cryptoagility and identified its importance for C-ITS. It has asked the question: what will happen if (in fact *when*) there is a need to update the algorithms or security software used within the context of the SCMS.

Reasons algorithms or software may require an update can include:

- Broken algorithms due to operational failures
- Malicious attacks
- Increasing computer power and advances in mathematics that are capable of breaking algorithms.

Cryptoagility is also important for backwards compatibility. It is unrealistic to assume that 100% of C-ITS devices will receive updates when they are issued. They may, for example, be travelling outside of the SCMS trust domain at the time updates are issued.

In this scenario, the device re-entering the SCMS domain would be running an outdated version of the necessary software. Cryptoagility would allow this device – and perhaps devices from other countries – to still be secured.

If updates are voluntary, some users may elect not to update (as many mobile phone users do) and they too will still expect to have their privacy protected.

Implementation errors and key management issues are more common than broken algorithms, but equally serious threats to the SCMS. Moreover, somewhat like a lock on a door, once an algorithm is broken, the algorithm itself does not minimise the damage that an intruder can do if they are successful in gaining access (this is discussed in material on Privacy in 6.2).

Ongoing management of cryptographic operations therefore requires a high level of system management oversight to mitigate both potentially minor threats, and those that may compromise the SCMS and the entire C-ITS trust domain.

Advancements in quantum computing, however, will almost certainly pose a threat to both curves, and to Elliptic Curve Cryptography in general (and will be an issue for security well beyond the transport portfolio).

Both the United States and Europe have published advice recommending that a post-quantum cryptographic strategy is in place by 2020, and it would be prudent for Australia to do the same.

While it may not be an enabling decision as such, a post-quantum strategy would benefit from being part of, or progressed in unison with, a nationally agreed deployment plan for security management.

7.2.5 Options

Neither the United States nor Europe are considering alternatives to NIST and Brainpool, and for Australia to do so would thoroughly comprise the Australian C-ITS platform.

While both curves have significant penetration in the finance and e-commerce spheres, more detailed analysis of their application for C-ITS is currently underway in Europe.

Involvement in international harmonisation efforts through TCA favourably positions Australia to leverage these analyses, although some dedicated Australian testing and analysis would certainly be advisable.

For policy and decision makers in Australia, the decision would be relatively simple if they were to align with the evolving discussion in Europe: support both curves, but approve, endorse and promote the use of one for the Australian environment.

This would essentially allow policy makers to select and implement a single 'official language' for the Australian deployment, to which devices will automatically conform; any devices speaking the other, 'unofficial language' will be able to be understood and relied upon nonetheless.

However, this would be premature – it is unclear how this emerging discussion and compromise will play out.

Moreover, Europe is having to have this discussion due to the geographic circumstances, and the compromise itself is both a symptom and a solution for the European federated SCMS model.

Australia does not have to contend with these political tensions to nearly the same extent. Developments in Europe, in this case, should be monitored on a county-by-country level, given that Europe may need to implement a regional solution to a local problem.

Having to support both curves would alter some of the fundamental assumptions Australian planners have been making about the deployment of both the SCMS and C-ITS in general.

Moreover, deployment operations (at least for day 1 and the medium-term) using both curves is unlikely to be economically nor operationally feasible, and this would be an expensive path for Australia to take.

The overriding key decision is to determine what cryptographic 'language' Australia should implement and, beyond this, to commit to ensuring its viability through cryptoagility.

The preferred choice between NIST and Brainpool and how this is arrived at it may be more complex. This may require research and review of both curves for their use in Australia, and exploration of implementation options.

It may also require government endorsement (given the public purpose nature of C-ITS and for transport agencies and government organisations using cryptographic operations) and updating of government products and documentation (such as the *Information Security Manual*, for example).

A forward-thinking security strategy that includes post-quantum cryptographic operations would also be highly advisable.

7.2.6 Parties Responsible for Advancing Decision

Having to support both curves would alter some of the fundamental assumptions Australian planners have been making about the deployment of both the SCMS and C-ITS in general.

This is a matter where policy thinking and direction will have very substantial impacts on the commercial, technical and administrative costs of operating a SCMS – and decisions that will impact the Australian deployment of C-ITS.

This would ideally be advanced at a national level, involving input from all jurisdictions, and the entity designated as SCMS Manager.

A national SCMS would substantially reduce the likelihood of jurisdiction-based decision making: a multi-SCMS environment supporting different crypto curves would be the cyber equivalent of different rail gauges.

Europe may have implemented a technical solution to support a geopolitical stalemate, and will have to bear the significant costs associated with this across *all* stakeholders – there is no firm reason for Australia to do this.

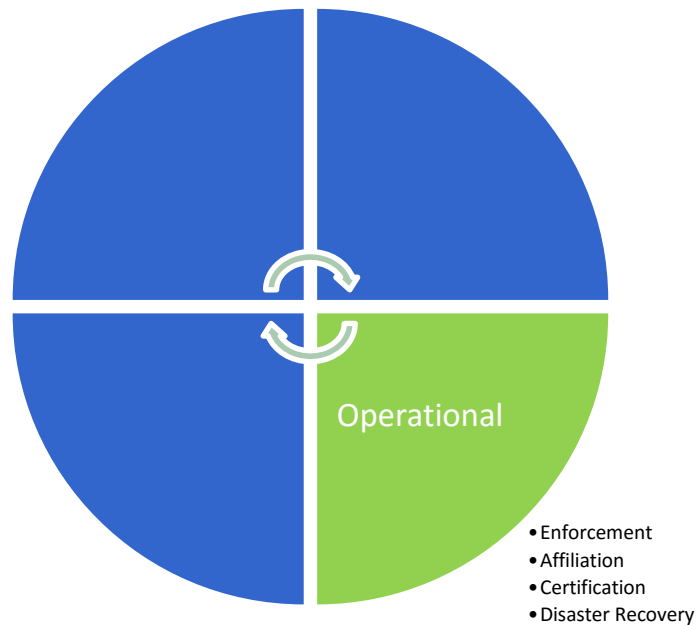
The SCMS Manager's ability to provide advice and guidance on how to translate policy intent into commercially, technically and operationally viable outcomes would be greatly beneficial to decision makers. Continued involvement in and monitoring of the European situation and international developments is critical for Australia.

When decisions are made, the finer points related to communicating Australia's ability to trust and be trusted with the deployment of cryptographic operations will be an initial and ongoing stakeholder engagement task for the SCMS Manager.

Ensuring cryptoagility will largely be undertaken by the SCMS Manager and other SCMS stakeholders, once a decision on a curve has been settled at a higher level.

A forward-thinking security strategy that includes post-quantum cryptographic operations could benefit from being part of, or progressed in unison with, a nationally agreed deployment plan for and strategic policy strategy for security management.

8 OPERATIONAL



Domain role	Establish how the SCMS will work in the real world, today, tomorrow and into the future
Types of decisions	<ul style="list-style-type: none"> • How to mitigate risk, and protect the security and safety of users • How political alignment and engagement can shape technical decisions to boost international cooperation • The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in supporting this • The ability to offer uninterrupted support during disaster or upgrade.

8.1 Enforcement

8.1.1 Concept

This section discusses enforcement measures that the SCMS can undertake to mitigate risks – be they active or potential – within the SCMS and in the operational C-ITS environment.

These are not enforcement activities in the sense of law enforcement as such, although breaches and investigations may result in law enforcement actions being taken. This topic is discussed in 6.3 on Legal.

Risks, as noted in 7.1 on Blacklisting and Whitelisting, may be systems, users, applications or devices that intentionally or unintentionally threaten to deny, degrade, disrupt or destroy the trust, security, safety, privacy of the C-ITS environment.

The methods by which the SCMS may take enforcement action are often collectively and generically called Misbehaviour Management functions. For the purposes of this document, the enforcement method discussed is called revocation.

Revocation is a technically complex operation, because it must be possible to undertake enforcement action within the internal contradiction of the SCMS: that is, the ability to remain anonymous, yet still be trusted. This prevents easy identification of bad actors and threats, yet must be undertaken.

As such, the basic operation of revocation is to identify and withdraw *permission* rather than *people*: a concert ticket gives you *permission* to access a venue, and tells the holder where to sit, but may not identify the *person* who holds the ticket, and revocation can be understood in this fashion.

8.1.2 Revocation

Misbehaviour Management refers to the ability to conduct investigations, perform pattern recognition, and test and search for implausible messages, technical malfunctions and malfeasance. Revocation is an operational function of Misbehaviour Management.

Revocation is a critical part of a security strategy. Allowing threats to exist or propagate has security and safety consequences.

Threats may also be irritating or create enough dissatisfaction that users cease to use or act on the messages they receive altogether (in the same way many people don't answer their phone if they know it's a telemarketer; or ignore a faulty car alarm that always goes off – the alarm is more of an irritant than an alert for potential threats).

As noted in 7.3 on Cryptography and 6.2 on Privacy, cryptography and technical operations alone are not enough to guarantee security. Management processes and ongoing supervision of things like key management and organisation-based access to information are more important and more effective mitigation tasks. Cryptography can provide a lock on the door, but once that lock is breached, the lock itself does not reduce the harm that an intruder is able to do.

If crypto material is compromised, or suspected of being compromised (that is, if it is stolen, accessed by an unauthorised or untrusted party, or widely available) then current, future – and to a reasonable extent, past – communications using that crypto material need to be regarded as compromised.⁴²

Crypto material extracted from a C-ITS device or from a SCMS entity could very feasibly be published or traded online, and similar sites and networks already exist for other operations. Preventing this from happening, and being able to act if it does, is paramount.⁴³

⁴² Department of Defence, Strategic Policy and Intelligence. 2016. *Australian Government Information Security Manual. Controls*. Australian Government, p. 236-257. Available at http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

⁴³ 'Agencies must revoke keying material or certificates when they are suspected of being compromised.' *Information Security Manual, Controls*, p. 257.

Cryptography *may* be broken, and it will *certainly* need to be updated. Broken cryptography is unlikely to be a common occurrence, but the effects of it happening are potentially devastating from a systems operation perspective – and to privacy and safety – and may result in disaster recovery operations (explored in 8.4).

Intentional or unintentional misbehaviour, by contrast, is a more likely occurrence, as it is on the Internet today. The consequences are expected to be less severe from a systems perspective, but not from a user perspective, who may have their safety compromised.

One can deploy two types of revocation: *active* and *passive*.

In **active revocation**, Certificate Revocation Lists (i.e. Blacklists) are routinely compiled and broadcast to devices and other entities informing them that a certain device or application is not to be trusted, and should be ignored.

In **passive revocation (which is *not* revocation as such)** a device is blocked from new pseudonym certificates: once the pseudonym certificates in their current batch expire, they cannot acquire new ones, and the device effectively ‘withers on the vine’ or is ‘revoked by expiration.’

Despite being a less timely response than active revocation, passive revocation may be feasible if the length for which pseudonym certificates are valid is quite short. However, this places a greater burden on the performance of the device and the SCMS – and on the costs: an arbitrary increase in the minimum of certificates used by a single vehicle would scale radically for SCMS operations.

More importantly, car manufacturers are fully expecting to pre-load devices with certificates. The volume is not yet known, but it would not be unlikely for a device to have supply of one, or perhaps two or three months or even years’ worth of certificates. If passive revocation were deployed, a device could therefore be a threat for one to three months or years before it is ‘revoked.’

Misbehaviour Management is an evolving field, and remote *deactivation* of a device rather than revocation may be feasible, but this is making a substantial assumption that devices can or will support this. Even in the United States, where Misbehaviour Management is most advanced, this has largely been earmarked as a future advancement.

8.1.3 United States

The United States is deploying a highly sophisticated approach to revocation and to Misbehaviour Management in general. Compared to Europe, the United States is placing a much higher premium on privacy within the SCMS (as further explored in 6.2 on Privacy).

This premium on privacy, and the likely mandated use of C-ITS, have had a substantial effect on the complexity of the development and planned deployment of enforcement activities and the SCMS architecture.

Entities in the United States SCMS will be effectively ‘blind,’ with no entity having enough information to identify the full complement of certificates and permissions associated with a device. (This is addition to the fact that, as in European and Australian deployments, devices will be routinely changing their identifiers, and will have multiple certificates.)

To enable revocation, there are two entities in the United States SCMS that are not present in the European SCMS.

By combining ‘seed’ information generated through cryptographic key distribution operations, two separate entities called Linkage Authority 1 and Linkage Authority 2 are able to create a Certificate

Revocation List. This operation is extraordinarily mathematically complex, and allows the SCMS to revoke the permissions of bad actors non-retrospectively – that is, it does not reveal the certificates they have used in the past before revocation. This solution is to a great extent a product of a privacy-by-design approach.

Additional privacy measures in the United States SCMS are related to Privacy, and are discussed in 6.2.

8.1.4 Europe

Compared to the United States, the currently proposed European SCMS is focussing on a more ‘passive’ revocation approach, mitigated by reducing the amount of time for which certificates are valid.

Similarly, the internal security proposed for the European SCMS is less robust than the United States SCMS – they do not have the entities and functionality for Linkage Authorities (and other features, discussed in section 6.2 on Privacy).

Together, these have produced a less complex SCMS than the United States’, and one based more on a risk management – rather than privacy by design – approach.

However, European internal discussions and reports are quickly evolving, and it is likely that more advanced and active revocation measures will be deployed for day 1 operations, and will increase in sophistication from thereon.

By the same token, it is likely that internal security will become more robust for day 1 deployment, and increase over time. It is likely that these will not be as advanced as the United States model, but will resemble it in some way nonetheless.

Unlike the United States, Europe is having to grapple with geopolitical interests, and the labour of having to reach a consistent and acceptable approach for the whole region. The higher level of industry input has also made compromising between public and private interests necessary.

The final report of the European Commission’s C-ITS Platform has identified the urgent need for a standardised revocation to be developed,⁴⁴ and the HTGs have identified revocation and Misbehaviour Management as a high priority for harmonisation: a region that does not have a robust or consistent approach is very likely to be shunned by other SCMS, as detailed in 8.2.4 on SCMS policy tools.

8.1.5 Options

Even if revocation were never used (although this would be almost entirely unlikely), it *must* be supported. Without it, there is no way to intervene into the C-ITS environment to remove threats. How robust these measures are is a key decision.

Revocation is a highly technical process. It has not been necessary to elaborate the technical nature of this for this document because, as the discussion on European and United States deployments suggests, the technical approach involved is largely being driven by non-technical decisions.

⁴⁴ European Commission, *C-ITS Platform*, p. 66.

The sophistication of revocation operations in the United States SCMS is a reflection of their policy requirements; while geopolitical and private interests have shaped the current European SCMS, which shows strong signs of being bolstered in some way before deployment.

‘Passive revocation’ or ‘revocation by expiration’ does not pose a particularly robust means of risk mitigation, nor the capability to intervene into the C-ITS environment as such: *threats remain threats* for as long as their certificates are valid. The risk may be mitigated by shortening the time for which certificates are valid, but vehicle manufacturers may play a decisive role here, and cooperation and compliance would need to be ensured.

For Australia, this points to the fact that policy decisions and requirements will have a very substantial role in determining what and how threats can be managed.

A highly sophisticated approach to revocation is *not* required for day 1 deployment: there will not be enough users to warrant it.

However, this report reminds policy and decision makers that, while this may reduce upfront and short-term operational costs, the inability to respond to a security breach can be very expensive on all fronts. Balance will therefore be essential.

Increased levels of (and techniques for) revocation should be planned for, given that the number of users and devices will grow over time, and therefore introduce the potential for more risk and more complexity.

Decisions are therefore required about:

- What should be revoked
- The conditions that need to be met for revocation (noting that these will be built into SCMS policy tools, defined and described in 8.2.4)
- The mechanism for revocation.

An important factor for policy and decision makers will be the current trend in Australia to align with European deployments. Given the non-mandatory uptake of C-ITS in Europe, it is possible that not all European devices in vehicles may support active revocation measures.

For the Australian deployment, this report reminds policy and decision makers that C-ITS devices will be installed in infrastructure controlled by road agencies, not just in vehicles: the SCMS is not just for vehicles, but also for infrastructure.

A compromised piece of infrastructure – one that is hacked or faulty and broadcasts an unreliable or entirely misleading message – would pose a very serious threat to users.

Revocation and associated Misbehaviour Management detection activities will provide road agencies with the assurance that risks to road authority infrastructure assets and reputations are actively managed and monitored, and threats can be removed.

Revocation and blacklisting may be necessary to ensure safety and security, but are likely to be thorny points, both operationally and commercially. Whether industry (a vehicle consortium, for example) *could* or *should* operate Misbehaviour Management components is highly questionable: having industry policing industry would likely be a questionable decision, raising numerous genuine or perceived conflicts of interest (e.g. the revocation of a competitor’s certificates, rightly or wrongly).

It is therefore likely that road and transport agencies would need to be empowered to act as an authority in such matters (for legal reasons, and to assuage genuine or perceived conflicts of interest).

For this and similar reasons, the USDOT summarised industry stakeholders' responses to the United States Notice of Proposed Rulemaking on C-ITS thus:

[I]ndustry commenters vehemently disagreed that a private self-governing industry coalition could be a viable mechanism for SCMS system governance. Commenters believed that a private SCMS could not provide the security, privacy, certainty, stability, long-term functionality, or management of costs and risk required for a nationwide SCMS to support V2V DSRC communications, and lacked the legal authority to address cross-border issues or require industry-wide participation and compliance with uniform requirements. For these reasons, virtually all industry commenters took the position that a strong leadership role for the Federal government in the SCMS would be required for successful deployment of V2V and V2X DSRC communications.⁴⁵

It is entirely feasible for Australia to implement a SCMS with revocation capability that adapts and adopts some of the more desirable aspects of the United States SCMS without:

- Incurring the costs associated with the United States SCMS
- Developing a unique, proprietary and unharmonised system (noting that harmonisation in this area of critical importance, discussed in 8.2).

8.1.6 Parties Responsible for Advancing Decision

This is a matter where policy thinking and direction will have significant impacts on the commercial, technical and administrative costs of operating a SCMS – and decisions that affect the Australian deployment of C-ITS.

This would ideally be advanced at a national level, involving input from all jurisdictions.

Given that revocation measures are directly tied to policy decisions related to privacy, the entity designated as SCMS Manager would be expected to develop these technical measures, and would be logically positioned to tell policy and decision makers, for day 1, and moving forward:

- What is available
- What the costs would be
- How policy intent can be realised
- Where policy intent may conflict with other requirements, such as privacy.

The evolving discussion in Europe, and the fast pace at which decisions are likely to be made, means that continued involvement in and monitoring of the European situation is critical for Australia.

⁴⁵ United States Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications, p. 231. Available at <https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands>

Given the importance of harmonisation in this area, an initial Australian solution would greatly benefit from being internationally scrutinised. Australia's current co-leadership of HTGs through TCA provides an ideal and logical avenue for this and for monitoring the European situation.

Communicating and learning from developments beyond day 1 will be an ongoing stakeholder engagement task for the SCMS Manager.

8.2 Affiliation

8.2.1 Concept

Affiliation has to do with easing the burden of the technical, policy, operational and commercial coordination involved in establishing and maintaining trust between regions in general, and inter-SCMS trust in particular.

Affiliation and harmonisation reduces development, deployment and ongoing costs for governments, and provide a more 'seamless' experience for the global market, and for the mobility of users.

However, implementing and deploying a SCMS does not in and of itself mean that trust between one or more SCMS is possible, or that trust between a certain SCMS is desirable: the decision to trust, and the ability to be trusted, will be the result of strategic and policy decisions.

Options in this area may be highly restricted, depending on architecture decisions detailed in 6.1: whether Australia deploys a national SCMS, or whether the Root Certificate Authority (the trust anchor for the system) is located overseas. It should also be noted that affiliation tasks will need to be duplicated if Australia deploys multiple SCMS, instead of a single, national SCMS (although a multi-root local environment may be feasible).

It has been a theme throughout this document that trust – how it is initiated and maintained – is not a fixed point within the SCMS. There are highly critical functions and entities, such as the Root Certificate Authority, the SCMS Manager, etc., but neither of these alone guarantees trust. This is why, for example:

- Key decisions related to the SCMS are more of a policy nature than they are technical
- The location of the Root Certificate Authority is a significant issue
- An Intermediate Certificate Authority is required to protect the Root Certificate Authority
- The SCMS Manager's effectiveness is contingent on their ability to engage with the international community.

A SCMS has boundaries – these may be geographic (jurisdictional, national or international), political, application-based, or commercial (and temporal, as discussed in 8.4 on Disaster recovery).

For affiliation and inter-SCMS trust purposes, policy and decision makers will need to ask the basic questions, 'Who do I trust?' and 'How much do I trust them?', and then pursue a number of political, technical, and commercial lines of inquiry to arrive at an answer.

How these levels of trust are achieved is a highly-technical process, ranging from major design decisions to comparatively small ‘tweaks.’ Importantly, the decision to trust another SCMS would not be automatically reciprocated – there would need to be mutual agreement and formal recognition.

At a high level, these levels of inter-SCMS can be summarised thus, in ascending order of trust:

1. **No trust:** One SCMS does not trust another, and the user must effectively operate in two SCMS
2. **Registration level trust:** Higher level of trust, duplication of SCMS operations for user, who must be enrolled in both SCMS
3. **Enrolment level trust:** High level of trust, less duplication of SCMS operations for user, who can be enrolled in both SCMS, but does not need to be
4. **Cross certification of root certificates/pseudonym level trust:** The ‘trust anchor’ of one SCMS trusts that of another, pseudonym certificates in one SCMS are trusted in the other, minimal duplication of SCMS operations for user, who can be enrolled in both SCMS, but does not need to be.⁴⁶

Users have been identified as the beneficiaries here, but these benefits extend to a more mobile market with fewer barriers to entry, and ongoing administrative and operational costs for government and operators of the SCMS.

Whether Australia seeks affiliation with Europe and/or the United States is a policy decision.

However, policy makers would have their range of options substantially reduced should the Root Certificate Authority be overseas (i.e. Australia does not have a national SCMS). In this case, affiliation decisions will be largely made offshore, with policy makers having little to no input (see 6.1 on Architecture).

8.2.2 Europe

Inter-SCMS trust, and the cultivation and maintenance of political, technical, commercial and operational affiliation in Europe will need to be the default, rather than an option, due to the federated model that is being deployed.

Nonetheless, there are options for inter-SCMS trust across the region that could be implemented – and indeed, could change.

For example, if a SCMS comes to be deemed untrustworthy, or political relations deteriorate, this can be reflected in the extent to which one SCMS trusts the other.

The European federated SCMS model will see different SCMS establishing relationships across the trust levels identified above.

For this reason, harmonisation and compromise has both progressed and posed challenges to the deployment of C-ITS and the SCMS in Europe.

⁴⁶ These are detailed in EU-US ITS Task Force. Standards Harmonisation Working Group Harmonisation Task Group 6. 2015. *Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonisation. Document HTG6-4.* European Commission/United States Department of Transportation/Transport Certification Australia. Available at <https://ec.europa.eu/digital-single-market/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international>

The role of the SCMS Manager in each SCMS will also place a premium on stakeholder engagement.

8.2.3 United States

The United States will have a single SCMS, and will not have to manage the intricacies and complexities of the European federated model, or the political ambiguity and interests of Member States for a region-wide solution.

Where the United States seeks inter-SCMS trust, it will be along one of the trust levels identified and described above, and a strategic, policy and commercial decision.

The very active participation and investment by the United States in HTG and other global initiatives indicates that they are prepared to consider inter-SCMS trust as and when appropriate.

8.2.4 SCMS Policy Tools

The role of the SCMS is to translate the policy environment into operational policies and systems that provide security support and services for the C-ITS environment.

The importance of a simultaneously robust and continually responsive policy environment is fundamental. Put simply, a change in policy (subsequently reflected in SCMS policy tools) will change the real or perceived level of trust – favourably or unfavourably when pursuing affiliation and inter-SCMS trust.

Although this is achieved in a variety of ways, there are three SCMS policy tools (or ‘operational policies’) that highlight and underpin how the SCMS does this. Proceeding from the general to the particular, these three SCMS policy tools are:

- Security Policy
- Certificate Policy
- Certification Practice Statements.⁴⁷

Figure 12 below captures the purpose of each policy tool, what the tool identifies and describes, and what elements it contains for the purposes of SCMS entity operations, management, compliance, and disaster recovery.

Importantly, these cannot be progressed with any certainty – or in any detail – until the policy environment is been determined, or sends clear signals as to the direction that it will take – a cursory look at the ‘Elements’ column identifies many of the issues requiring decisions presented in this document.

⁴⁷ For more detail see European Commission. 2016. *C-ITS Platform WG5: Security and Certification. Final Report. ANNEX 1: Trust models for Cooperative-Intelligent Transport Systems (C-ITS). An analysis of the possible options of the design of the C-ITS trust model based on Public Key Infrastructure (PKI)*. Available at <https://ec.europa.eu/transport/themes/its/c-its>

SCMS policy tool	Purpose	Identifies and describes	
Security Policy	States the rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its systems.	<ul style="list-style-type: none"> Goals and objectives of the SCMS Roles within the SCMS, and entities interfacing with the SCMS Security requirements (of SCMS entities and of users – what a user must have to obtain a certificate, and what an entity must provide) How risk is assessed How information is classified How information, systems and assets are protected Aspects of compliance. 	Elements contained for SCMS entity operations, management, compliance, disaster recovery
Certificate Policy	States what participants, both in the SCMS and users, must do.	<ul style="list-style-type: none"> Statement of requirements Minimum operating guidelines, including enforcement Inter SCMS authorities, organisations and domains. 	<ul style="list-style-type: none"> Key generation processes Minimum length for the public key and private key pairs Cryptographic algorithms used to generate keys Participants based on role Processes for users enrolment Certificate revocation and suspension procedure Who has the authority to issue revocation and suspension Certificate used, certificates not allowed Legal issues, such as liability, that might arise if the CA becomes compromised Private key management, including requirements for storage on physical devices.
Certification Practice Statements	States practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.	<ul style="list-style-type: none"> The single authority or single organisation to which it (usually) applies How entities and participants in the SCMS implement procedures and controls to meet the requirements stated in the Certificate Policy How the participants perform their functions and implement controls. 	<ul style="list-style-type: none"> Policies, procedures, and processes for issuing, renewing, and recovering certificates Physical, network, and procedural security for the entity Management and operational controls, including processes for audits of SCMS and entity servers, archival of records and compromise and disaster recovery.

Figure 12 SCMS Policy Tools

The European Digital Tachograph and Australia's National Telematics Framework incorporating Gatekeeper⁴⁸ have been fundamental in providing operational transportation-based applications of PKI for HTGs and the European Commission's C-ITS Platform (noting that Gatekeeper PKI alone is not sufficient for the end-to-end administration and provision of security of regulatory programs in Australia, and is supplemented with additional elements in the National Telematics Framework).⁴⁹



Figure 13 European Certificate Policy

Harmonisation efforts thus far have ensured strong linkages between the National Telematics Framework and the European trust model.

As noted in 6.1 on Architecture and 9.2 on Organisation, while the IAP has some important technical differences to the SCMS, on a framework and policy level, they are more or less identical. This has allowed the European Commission's JRC and TCA – as the only two entities who manage large-scale transportation PKI – to profitably compare use cases, requirements and continuities in policy and framework flexibility.

⁴⁸ The Gatekeeper Strategy governs the use of PKI in government for the authentication of external clients (Organisations, Individuals and other entities). The Strategy ensures a whole-of-government framework that delivers integrity, interoperability, authenticity and trust for Agencies and their Clients. Department of Finance. 2009. *Gatekeeper Public Key Infrastructure Framework*. Australian Government. Available at https://www.finance.gov.au/sites/default/files/Gatekeeper_PKI_Framework.pdf. Note: Gatekeeper is now the responsibility of the Digital Transformation Office.

⁴⁹ See European Commission, *C-ITS Platform, WG5 Annex 1*.

These efforts have progressed alongside comparisons of the (to be) ETSI standards-based SCMS developed by the Car 2 Car Communications Consortium (a.k.a PRESERVE, a prominent SCMS model) and the United States SCMS developed by the Crash Avoidance Metrics Partnership (CAMP).⁵⁰

Through TCA's past and current co-leadership of HTGs, Australia has the option moving forward to harmonise with the security and certificate policies currently being drafted in Europe (pictured in Figure 13)

This has ensured that, should Australia choose to affiliate itself with European SCMS and C-ITS deployments, this task will be substantially easier than it otherwise would have been.

These alignment options could be extended to pre-deployment harmonisation with the United States.

For inter-SCMS trust and affiliation, HTG have identified priority areas for harmonisation – although these could arguably be described as a good way to measure some aspects of a SCMS in itself.⁵¹ Many of these areas will be captured in the SCMS policy tools noted above.

The areas of *highest priority* for harmonisation are:

- **Data centre management** – processes and procedures for Root Certificate Authority and Registration Authority
- **Handling of cryptomaterial (credentials/certificates/keys)** – distribution, injection into device, generation, storage; how these processes are documented, the security of communications channels, and disaster management plans
- **Vetting of organisations and entities** – initial and ongoing certification and audit, and the surrounding policies and processes
- **Lifecycle issues** – such as cryptoagility capability, ability to evolve with security requirements processes such as enrolment.

The *important* areas for harmonisation are:

- **Electronic and physical security of telematics devices** – the minimum acceptable requirements for the devices which are the end-point of communications
- **Trust in data** – including the ability to trust time-stamps, data providers, and the data received, in addition to enabling providers to trust data from users.

⁵⁰ There are emerging specifications for European and United States CCMS models, but the standards on which they will be based are currently being developed. In general, generic PKI standards are being used for the development of more bespoke standards.

⁵¹ EU-US ITS Task Force. Standards Harmonisation Working Group Harmonisation Task Group 6. 2015. *Public Key Infrastructure (PKI) Architecture Analysis and Recommendations for Harmonisation. Document HTG6-3*. European Commission/United States Department of Transportation/Transport Certification Australia. Available at <https://ec.europa.eu/digital-single-market/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international>

8.2.5 Options

While Australia can largely leverage the results of work that has been undertaken by Europe and the United States, one of the key lessons for policy and decision makers, and for the SCMS Manager, is that deploying a SCMS will not be a case of ‘build and forget’: trust will need to be initiated, vetted, maintained and strategically re-assessed.

As noted, the decision to trust a SCMS is not an easy one to implement, and it may not be reciprocated. One SCMS wishing to recognise another’s certificates will require a robust cross-certification agreement, a formal commitment and mutual recognition of each other’s certificate policy, and a formal (and informal) appreciation of each other’s SCMS and C-ITS environment.

For example, no certificate policy, however ‘airtight’ on paper, will be able to disguise real or perceived inadequacies in compliance assessment and certification (see 8.3 on Certification) or an operational environment in which hacks and privacy breaches are routine.

A SCMS that is, or is perceived to have been, built ‘on the cheap’ may struggle to form meaningful affiliations. This is an implementation issue *and* a strategic communications task.

The importance of a simultaneously robust and continually responsive policy environment is fundamental. Put simply, a change in policy (subsequently reflected in SCMS policy tools) will change the real or perceived level of trust – favourably or unfavourably.

Whether Australia seeks to affiliate itself Europe and/or the United States will be a policy decision.

There are additional options whereby Australia could harmonise closely with the European SCMS model, and integrating with it while have considerable autonomy over the SCMS Management function and Root Certificate Authority component.

In one scenario, this may allow Australia to deploy a local multi-Root Certificate Authority (with some operated by industry, yet with public oversight, as in Europe). Decisions of this magnitude would ideally be informed by more ‘first principles’ decisions included in this report.

Determining the viability of this option could be one of the outcomes of this report, given that progressing along these lines would require some very fundamental decisions regarding privacy, security and risk appetite to be established.

Depending on the location of Root Certificate Authority for the Australian deployment, however, there may be less choice in the matter.

Options for decisions in this area may be highly restricted, depending on architecture decisions detailed in 6.1: whether Australia deploys a national SCMS, or whether the trust anchor for the system is located overseas. It should also be noted that affiliation tasks will need to be duplicated if Australia deploys multiple SCMS, instead of a single, national SCMS.

If the Root Certificate Authority for Australia is overseas (i.e. there is no national SCMS) Australia will have little say in affiliation processes, and SCMS policy tools (Security Policy, Certificate Policy, Certification Practice Statements) may be to a greater extent in the hands of the overseas party (this is explored in 6.1 on Architecture).

A national SCMS would substantially reduce the uncertainties of this outcome.

Harmonisation efforts thus far have ensured strong linkages between the National Telematics Framework and the European trust model, giving the potential option of affiliations with European SCMS. This could be extended to further alignment with United States SCMS policy tools.

These efforts have progressed alongside comparisons of the ETSI standards-based SCMS developed by the Car 2 Car Communications Consortium (PRESERVE SCMS) and the United States SCMS developed by the Crash Avoidance Metrics Partnership (CAMP).

Through TCA's past and current co-leadership of HTGs, Australia has first-hand experience with the intricacies involved with these priority and important harmonisation areas.

8.2.6 Parties Responsible for Advancing Decision

TISOC/Austrroads are the lead entities on the Action Item in the Policy Framework for Land Transport Technology, which is to be delivered in mid-2018, that will determine whether a national SCMS is required for Australia.

The discussion above of Security Policy, Certificate Policy, Certification Practice Statements highlighted that the development of detailed SCMS policy tools cannot be progressed until further key decisions are made – these are largely the decisions presented in this document.

Once they are, the SCMS Manager and SCMS stakeholders would progress these in consultation with policy and decision makers, and in coordination with Europe and/or the United States, as policy dictates.

As a result of TCA's collaboration with the European Commission, the option to harmonise with the security and certificate policies currently being drafted in Europe. These could extend to future alignments with United States SCMS policy tools.

Ongoing trust management, both nationally and internationally, would be required of the SCMS Manager.

8.3 Certification

8.3.1 Concept

One of the recurring themes in this document is the need for policy and decision makers to ask:

- Who do you trust?
- How much do want to trust them?
- What do others need to do to demonstrate their ability to be trusted?

Certification – or more generically, compliance assurance – is the practice of ensuring this that this trust can be tested and assured. This may involve assessing the satisfactory nature or conformance (often with standards) of a product (or components thereof) a service, or an entity, such as a manufacturer or service provider.

Australia needs to strike the right balance between safeguarding their requirements and the expectations of users against the fact that manufacturers will resist making substantial modifications for smaller markets like Australia.

Developing highly unique compliance assurance process would compromise the commercial viability of Australia's C-ITS deployment.

Compliance can refer to a variety of practices (e.g. type-approval, certification) involving numerous roles, responsibilities and entities (e.g. regulators or industry bodies), although they share the common goal of achieving a desired level of compliance.

In broad terms, compliance provides confidence to regulatory bodies and consumers alike that the product or service meets their standards or needs, and provides industry with a range of benefits, such as access to a wider, sometimes global, market.

The complexity introduced here is that many of the compliance assurance processes the concern the SCMS are effectively *external* to the SCMS, yet will impact SCMS operations and SCMS policy tools.

For this reason, the HTG have stated that:

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 the security management systems and procedures.⁵²

Determining *what needs* compliance assurance – which may include devices and applications – and *what* compliance assurance *involves* will have flow-on effects for the SCMS.

The level of compliance assurance applied to a device or application can involve self-certification, type-approval, third party certification, ongoing audit, etc.

Before a device or application is allowed into the SCMS, the SCMS will need to know:

- The standard it should be checking against
- How that standard can be assessed and confirmed
- The processes for when a device does not meet that standard.

The SCMS policy tools (Security Policy, Certificate Policy and Certification Practice Statements) will be important for reflecting and operationalising the policy environment and its compliance assurance and certification strategy and requirements – as will the SCMS Manager's role in their development, circulation, updating, and enforcing compliance with them.

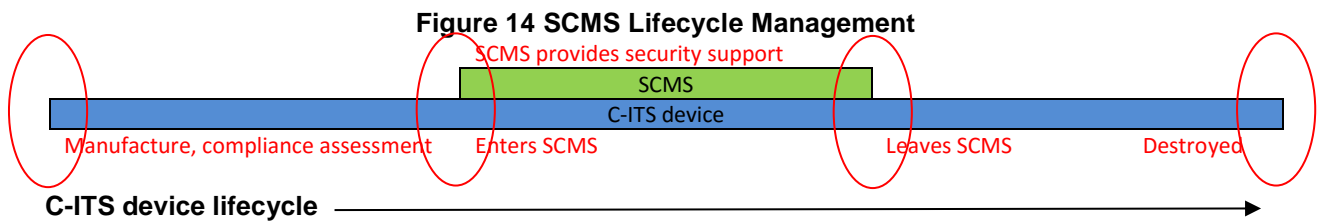
8.3.2 Lifecycle Management

The SCMS will be required to provide lifecycle security and management for the C-ITS device. This is represented in Figure 14: the critical thing to note is that the C-ITS device's lifecycle begins *before* it enters the SCMS, and continues after it *leaves* the SCMS (end of lifecycle).

What exists before the C-ITS device enters the SCMS concerns certification and compliance assurance; what happens after it leaves the SCMS concerns the policies and processes for decommissioning, which may ensure that a C-ITS cannot wrongly re-enter one or more SCMS (the cybersecurity equivalent of 'rebirthing' in the automotive world).

⁵² EU/USDOT/TCA, HTG6, *Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonisation*, p. 9.

Both compliance assessment and end-of-lifecycle management have been identified as key beneficiaries of, and key for ensuring, harmonisation.⁵³



Noting that compliance assurance is a broader necessity and denotes a range of practices throughout the C-ITS environment, certification processes tell the Enrolment Certificate Authority which types of devices can participate in the SCMS, and generally tell the SCMS what types of devices can receive certain types of certificates and permissions.

Who will be responsible for providing this information to be embedded in the device and/or supplied by a party involved in the early stages of the C-ITS device lifecycle.

What the SCMS considers to be compliant is largely determined externally: if the C-ITS device can demonstrate that it is compliant with the decisions made by the policy environment, then the SCMS will consider it to be fit-for-purpose to participate in the SCMS.

Certification is therefore an entry requirement for a C-ITS device entering the SCMS; determining what this entry requirement is a policy decision.

8.3.3 United States

As noted above in 6.3.5, determining what applications should require SCMS oversight and support will be a fundamental decision.

However, it is clear that both the United States and Europe are grappling with the issue of how to ensure a C-ITS device (rather than applications as such) complies with the appropriate standards and to what level assurance must be obtained.

Broadly, in the United States, the governance approach to compliance assurance is not yet firmly in place. However, the policies and procedures are being developed, and compliance assurance options in the form of certification are being progressed in the *immediately* for practical reasons through the ITS Joint Program Office (USDOT).

Government sponsored certification labs are being made available to manufacturers and developers where more scrutiny than self-certification in accordance with NHTSA requirements is called for.⁵⁴

⁵³ In TCA's initial set of SCMS requirements, it is a system management requirement that the SCMS be able to support a C-ITS device over its lifecycle, but these cannot be progressed without the necessary decisions.

⁵⁴ USDOT, *Status of the Dedicated Short-Range Communications Technology and Applications*, p. 4.

It is acknowledged in the United States that safety applications – such as those for crash avoidance – or applications that are expected to bolster essential and emergency services – such as emergency vehicle prioritisation for ambulances and police – require higher levels of security and certification than non-safety, commercial applications.⁵⁵

8.3.4 Europe

The European Commission's C-ITS Platform have noted that 'For the achievement of key public policy goals, C-ITS stations require compliance assessment before being placed on the EU's internal market.'⁵⁶

The European compliance assurance model is placing a premium on regional and international coordination, and is currently being developed by the European Commission's C-ITS Platform, and in coordination and cooperation with the United States-European-Australian HTGs.

In their strategy for C-ITS, published December 2016, the European Commission have stated their intentions for a compliance assessment path, noting that higher levels of assurance are required for safety-critical applications:

The seamless deployment of Day 1 C-ITS services requires an effective compliance assessment framework that allows services to be checked against EU-wide system requirements. Especially for road-safety-related applications, there is a strong public interest in developing such a framework for key elements of the C-ITS network such as security, data protection or interoperability, to ensure that drivers receive consistent warnings in different traffic environments across the EU.

This statement is accompanied by two specific actions:

- C-ITS deployment initiatives should help define a compliance assessment process for Day 1 C-ITS services and publish it to ensure third parties have full access.
- The Commission will support the deployment initiatives in developing a fully-fledged common compliance assessment process for all key elements to ensure the continuity of C-ITS services and take into account potential service extensions.⁵⁷

8.3.5 Options

In TCA's initial set of SCMS requirements, it is a system management requirement that the SCMS be able to support a C-ITS device over its lifecycle.

However, the SCMS's ability to do so will be greatly affected by compliance assessment processes.

Progressing plans on certification requirements will have a variety of material benefits that include:

⁵⁵ USDOT, *Status of the Dedicated Short-Range Communications Technology and Applications*, p. 9.

⁵⁶ European Commission, *C-ITS Platform*, p. 66.

⁵⁷ European Commission. 2016. *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions :A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, p. 10-11. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

- Safety applications, or applications that deliver stronger public purpose outcomes, are available only for their intended use, and work as intended
- Compliance activities can be directed at applications that have a higher risk profile if they are available to users for whom they were not intended
- Compliance activities are not unreasonably required of low-risk/non-safety applications, and those that are not specifically intended/being relied upon to deliver public benefit.

Australia needs to strike the right balance between safeguarding their requirements and the expectations of users against the fact that manufacturers will resist making substantial modifications for smaller markets like Australia.

Developing highly unique compliance assurance process would compromise the commercial viability of Australia's C-ITS deployment.

Australia's current interest in aligning with European deployments would make engagement with the European Commission's C-ITS Platform (through the relevant Working Group facilitating international cooperation) highly beneficial, if not essential.

TCA's continued participation with the HTGs would allow further involvement in and awareness of compliance assurance standards in general, and particularly those critical to the SCMS as they evolve.

Moving forward, this could facilitate the ability recognise and leverage compliance assessment processes C-ITS devices and applications undergo in Europe and the United States (and potentially other regions) thus easing the compliance assessment effort required for Australia to develop and perform.

Together, these options would ensure that Australia's compliance assurance framework, when it is developed, is consistent (where appropriate and beneficial) with those overseas.

8.3.6 Parties Responsible for Advancing Decision

There are two Action Items in the National Policy Framework for Land Transport Technology relevant to policy and decision makers in this area: Action Items # 5 and # 6.

Action Item # 5 reads:

Publish a connected vehicle (Cooperative ITS) statement of intent on standards and deployment models.

The Framework highlights that the statement of intent will provide industry with guidance on:

- Non-regulatory deployment models possibly adopted by convention in Australia
- Regulatory standards which may form part of the formal regulatory framework in Australia.

Action Item # 6 reads:

Develop a nationally agreed deployment plan for the security management of connected and automated vehicles.

This Action Item will explore options for meeting security management requirements, factoring in costs, risks, feasibility, timing, and overseas experience. The overall output for this Action Item will be a nationally agreed plan for security management, which will also concern the SCMS and the broader security strategy that it is a part of.

TISOC/Commonwealth are the lead entities on Action Item # 5, which is to be delivered in early 2017.

Outcomes of this Action Item will be informed by other work TCA is progressing with Austroads, in relation to security and identifier standards for C-ITS devices. An application-centric approach has been used (i.e. the level of compliance assessment required for the security and identifier standards to be used in the C-ITS device is measured against the types of applications it will likely to be using in the SCMS and more generally).

TISOC/Austroads are the lead entities on Action Item # 6 which is to be delivered in mid-2018.

The SCMS Manager will play an important role in translating the chosen compliance assurance strategy and requirements into SCMS operations and SCMS policy tools, and engaging the SCMS Manager in the development of the compliance assurance framework would be ideal.

8.4 Disaster Recovery

8.4.1 Concept

Planning for disruptions caused by upgrades and disasters (and ensuring business continuity and uninterrupted security support) is part of any robust security strategy, and therefore a critical consideration for deployment of a SCMS. Generically referred to as 'disaster recovery,' this is one of the necessary support systems for the SCMS.

In addition to having geographic, political, application-based or commercial boundaries (see 8.2 on Affiliation) a SCMS has *temporal* boundaries. That is, it provides security support for users by issuing and revoking digital certificates, and by providing credentials; credentials, in turn, serve as third party (i.e. Root Certificate Authority) attestation regarding the validity of the C-ITS device, and its ability to be trusted and relied upon by other users.

The time for which these certificates are valid can vary, and some will be more readily disposable than others. SCMS support needs to be *continuous*: gaps or 'downtime' in support, due to a disaster or upgrade could have very serious security and safety consequences.

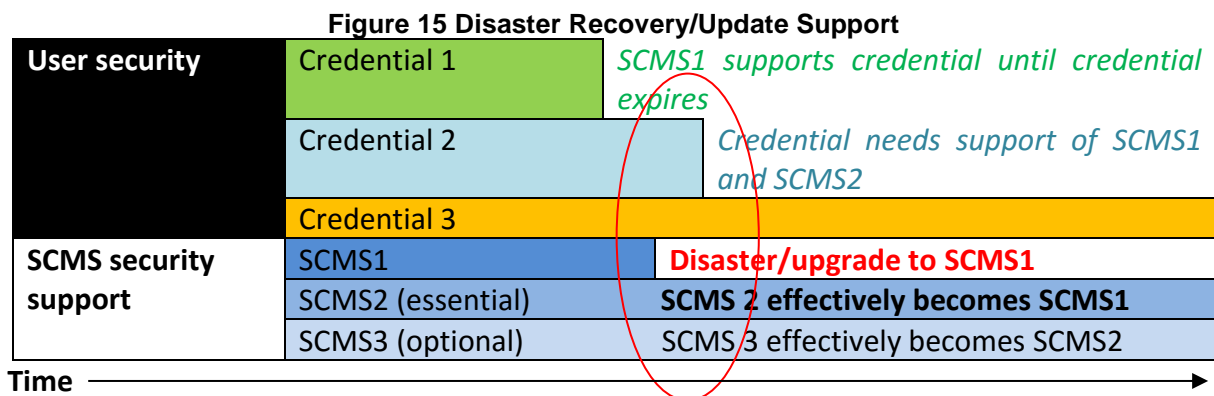
For this reason, a SCMS is, by definition, a collection of people, processes, policies and systems *and at least one more* SCMS (which in this case, refers only to necessary ICT elements, rather than a second set of organisations and entities) that can take over if the first one needs to be temporarily taken offline, or (in the worst case scenario) permanently decommissioned:

Given disaster recovery and resultant responses and upgrades, **a SCMS must be defined to exist in an environment where it must communicate with at least one other SCMS**: the original and a SCMS implemented as part of disaster recovery, or as part of a system upgrade.⁵⁸

⁵⁸ EU/USDOT/TCA, HTG6, *Cooperative-ITS Credential Management System Functional Analysis and Recommendations for Harmonisation*, p. 10.

Figure 15 below represents the need to de-operationalise a primary SCMS, and make operational a backup SCMS, due to an upgrade or disaster.

In this scenario, the credentials could be held by a single device, two devices, or three devices. This serves to illustrate the extent to which the effects of a temporarily or permanently offline SCMS could scale: all devices in the C-ITS environment would be affected, but the impacts of this could be vast.



In the scenario depicted in this figure, a second SCMS (SCMS2, which in this case, refers only to necessary ICT elements, rather than a second set of organisations and entities) is required when the operation of SCMS1 (the primary and currently operating SCMS) needs to be temporarily taken offline, or (in the worst case scenario) permanently decommissioned.

Users (of credentials) have been identified as the affected party in this scenario, but an offline SCMS would also suspend commercial operations for the duration of SCMS downtime.

In this scenario:

- Credential 1 is unaffected, given that it has expired before the disaster/upgrade
- Credential 2 is affected: there is 'handover' between SCMS1 and SCMS2, given that the credential has not expired, and SCMS2 provides the support that SCMS1 can no longer provide before the credential expires
- Credential 3 is affected: there is 'handover' between SCMS1 and SCMS2, given that the credential has not expired, and SCMS2 provides the support that SCMS1 can no longer provide; the credential continues to be supported by SCMS2 (with SCMS3 becoming the 'backup')
- SCMS2 continues to offer permanent support as the primary SCMS, or reverts to 'backup' when SCMS1 is returned to operation.

Without *at least one* other SCMS as a redundancy, the C-ITS environment could be vulnerable to a variety of threats posed by the lack of security support and services.

These could be minor inconveniences, or events that could threaten the safety and security and users. These may be responses to threats discussed in 7.3 on Cryptography or 8.1 on Enforcement, or of a different nature altogether. Updates, rather than threats, may also be required for reasons discussed in 7.3.

A SCMS deployment without *at least one* other SCMS as a ‘backup’ would be making several *dangerous assumptions*, chiefly:

- The integrity and capability of the SCMS will never be threatened (either internally or externally)
- An upgrade (either reactive or proactive) of a size requiring the SCMS to go ‘offline’ will never be required
- The *method* of a threat or successful attack can be easily *diagnosed*
- The *extent* of damage caused by a successful attack can be easily *assessed*
- The damage caused by a successful attack can be easily *fixed*
- The safety, monetary and reputational costs of system downtime are worth the risk
- System downtime will only be a brief interruption
- Users will be sympathetic to excuses.

Any threat or incident experienced in a deployment without a backup SCMS could easily resemble prominent cybersecurity and service scandals and disruptions experienced in 2016 alone, including:

- The Australian census
- The hacking of the Bureau of Meteorology
- Multiple lapses in Telstra's service provision.

A failure of security for and reliability of safety-critical services for the transport network, however, could have much more serious consequences for users, governments and SCMS operators.

8.4.2 Options

Deployment of a SCMS without *at least one additional* SCMS is practically unfeasible – the risks are too great.

The broader policy and strategy informing business continuity is, however, a local (ideally national) policy decision: its presence – and that of at least one additional SCMS – is assumed by the international C-ITS and SCMS community, but the precise shape of it is up to policy makers.

This would ideally be progressed by a national discussion, involving input from all jurisdictions and related transport network stakeholders.

This could harmonise or leverage international developments currently being progressed through HTG and in the SCMS space and/or harmonise with Australian security management resources and cybersecurity strategies.

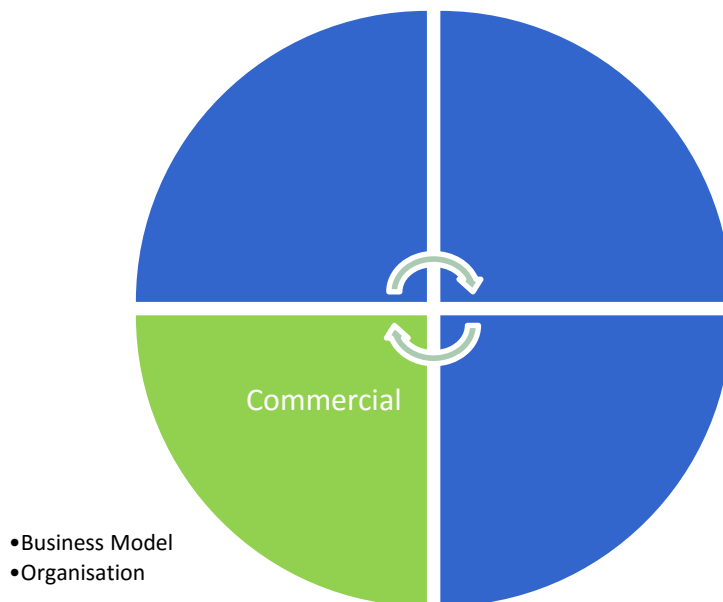
8.4.3 Parties Responsible for Advancing Decision

The direction and scope of business continuity for the SCMS will likely be part of a broader security strategy for the C-ITS environment. However, there will likely be decisions specific to the SCMS in need of policy direction and decisions.

The technical and operational provisions for disaster recovery will be the responsibility of the SCMS Manager, and tailored to suit the overarching security strategy developed at government policy level.

If the decision is made to harmonise more closely with overseas developments, the SCMS Manager would be logically positioned to inform policy makers of best practice in either Europe and/or the United States.

9 COMMERCIAL



Domain role	Establish the commercial decisions required for the SCMS, the impacts to government and industry, and who will benefit
Types of decisions	<ul style="list-style-type: none"> • Decisions underpinning initial and ongoing economic and organisational composition and viability of the SCMS • Nominating the entity who will translate the policy environment into SCMS technical policy design and operations, ensure compliance, and engage national and international SCMS stakeholders.

9.1 Business Model

9.1.1 Concept

In his article, *Innovation Nation*, Lachlan Blackhall writes that:

Entrepreneurs are good at optimising new technology and business models to deliver the best outcomes, but they cannot hit a moving target created by political, policy, or regulatory instability.⁵⁹

⁵⁹ Blackhall, L. 2016. Innovation nation? Why supporting science could help Australia to becoming something more than just the lucky country. *APPS Policy Forum*. Available at <http://www.policyforum.net/innovation-nation/>

This comment usefully points to the certainty that government agencies can provide for disruptive and transformational technologies.

The necessity of clear and consistent policy and regulation is an initial and ongoing theme throughout this document. The novelty of C-ITS in general has seen all regions grappling with the need to deliver policy that both enables innovation and provides the necessary safeguards for users and the market – and governments themselves have an interest in securing their own interests, and protecting their assets (see 8.1 on Enforcement).

That these interests and assets are themselves subject to disruption and change makes the task even more challenging.

This section highlights the need for decisions on the business model for the SCMS, which will be critical both to its deployment and longevity – and therefore the deployment and longevity of Australia's C-ITS deployment.

C-ITS will give rise to new business models, and will fundamentally change existing business models. The participation of telecommunications companies in what has previously been the relatively exclusive domain of the automobile industry is an obvious example of this.

Financing schemes for the SCMS, and identifying which parties will support or contribute to its development and operation are important to determine from the outset.

How the SCMS will operate as a collection of roles and responsibilities will be greatly determined by policy/legal and administrative decisions.

The level of investment in the SCMS and the funding and business models that enable it will also greatly affect *what* the SCMS is capable of: SCMS functions, such as enforcement, and requirements, such as privacy, are not 'bolt ons' – what they will provide for day 1 deployment and a strategy for their future development will need to be factored in.

The SCMS, as part of the C-ITS environment, will itself be based on a new business model, or on the adaptation of an existing business model.

The composition of the SCMS will be driven by desired policy outcomes, and governance decisions relating to the initial and ongoing funding for the SCMS will also be driven by enabling policy decisions.

In addition to the Certificate Authorities and entities comprising the SCMS, there will be additional organisations and business models that, although not part of the SCMS, will be impacted by SCMS rules and operations (see 6.2.6 on Enrolment and 8.3 on Certification).

The development of a business model and industry context for the SCMS in general will be a starting point for the development of SCMS requirements that reflect the standards, policies, levels of compliance assurance and expectations (and how to meet these) of the relevant industry players involved.

A more obvious example of the necessity of a business model would be to determine how the SCMS would be funded.

9.1.2 United States

While the *functions* of the United States SCMS have been mapped out, *who* will perform them is yet to be determined (with the exception of the USDOT, serving as SCMS Manager for a significant period of time).

The composition of the United States SCMS model has not been fully determined – indeed, the rulemaking on C-ITS may either expand, but more likely narrow, the number and types of entities that can be involved. Conflicts of interest and privacy risks are two high level things that will need to be considered.

Importantly, the SCMS is not just the Certificate Authorities featured in a generic PKI (as represented in Figure 6). Rather, there are a variety of organisations and industries that will interface, affect and be affected by the SCMS (such as those involved in compliance assessment and certification, suppliers and manufactures for enrolment and configuration, etc.). This means that these organisations and industries will interface with the SCMS in an operational setting, but also on a *policy level*; while Certificate Authorities are a type of service provider.

9.1.3 Europe

At a high level, the business models in the European SCMS are in many ways likely to be similar to that of the United States, with entities assuming the roles of SCMS functions, including service providers, and industry and other interfaces from the vehicle industry, and certification and enrolment processes.

With the exception of the JRC, understood to be supplying technical and policy consistency in their capacity as SCMS Manager, how the business models for different SCMS within the federated European model is not yet apparent (or at least publicly available – it is more than likely that private companies have mature business cases and deployment plans).

For Europe, a clear picture of the details for SCMS business models is less of a problem (noting the above, however, mature business models are likely to be in place, although confidential) given that they are aware of the complex, federated environment in which they will be operating. The latest strategy published by the European Commission in 2016 no doubt will make their business models sharper.

9.1.4 Options

Monitoring the United States and European business models will provide some useful learnings. However, their business models are quite different, given the mandated approach being progressed by the United States include high levels of government involvement and a privately operated (although not managed) SCMS. There are likely to be a variety of smaller models emerging from Europe, although these are not yet public. Automotive manufactures will likely play a significant role and will have their own commercial decisions made or in preparation.

The baseline level of infrastructure for C-ITS overall and the SCMS in particular is substantial: this is so for all C-ITS deployments, and there are levels of upfront investment and implementation that are required regardless of the number of users in the environment.

TCA is progressing indicative costings with Austroads, by leveraging United States and European models, and making balanced assumptions.

Greater clarity surrounding key decisions relating to levels of desired privacy and security would allow greater technical specification and needs assessment, and greater refinement in costings.

For example, the desired levels of Privacy (6.2) and Enforcement (8.1) may necessitate additional SCMS entities; expand the role of, and resources required by, a SCMS entity; or increase the number of certificates (how often they rotate and how long they are valid) required by a vehicle (noting that a modest increase per vehicle would scale dramatically for the system).

Knowledge of a clearer funding model would also flow in the opposite direction, given that level of funding available may expand or contract the options available.

Additionally, knowing how these costs could be apportioned (or an initial exploration of this matter) would be valuable, yet cannot be progressed without a business model.

9.1.5 Parties Responsible for Advancing Decision

How a SCMS would be funded, and costs apportioned between governments and industry, will be a critical discussion to advance on a national level: industry in particular will want operational, administrative and commercial certainty and consistency.

Engaging with service providers that will comprise SCMS entities and Certificate Authorities would be undertaken by the SCMS Manager, once appointed. The appointment of SCMS entities will need to take into account privacy requirements and the entity's ability to meet these requirements.

The SCMS Manager would also be expected to guide the development of the business environment once a business model has been established on a policy level.

9.2 Organisation

9.2.1 Concept

The role of the SCMS Manager has been cited on numerous occasions in this report as a key entity that will be responsible for progressing key decisions identified in this report, and for the integrity and competent management of SCMS operations.

This document has also stressed that the SCMS is a collection of roles and responsibilities, performed by different entities. The *goals* for these roles, responsibilities and entities is to a great extent determined by policy decisions; making *implementation decisions* that realise these goals is the task of the SCMS Manager and SCMS stakeholders.

Indeed, at a high level, the SCMS Manager is expected to progress issues related the SCMS at the planning stage, and be responsible for ensuring that the SCMS effectively translates the policy environment into operational policies and systems that provide security services and support for the C-ITS environment.

Providing initial advice, and acting to mitigate operational risks, will also be an area in which the SCMS Manager is ideally placed: for example, operations of service providers will need to be initially vetted (and then subjected to audit) and allocation of SCMS functions introduces security risks associated with exposed SCMS interfaces.

Determining the grouping, level of centralisation and entities and functions; engaging with potential service providers; developing criteria for initial and additional entities, and assuming responsibility

for change management – these are all operational and administrative decisions made by the SCMS Manager in order to achieve policy goals.

How the SCMS works from an organisational and operational perspective is a critical step to progressing the SCMS – and empowering an entity as SCMS Manager is a key decision.

9.2.2 SCMS Manager

The SCMS Manager is fundamental:

- Each region that has committed to adopting the SCMS has committed to having a SCMS Manager entity
- Organisational analyses of SCMS architecture options assume a SCMS Manager
- There are key differences in whether a SCMS is government operated, privately operated, a or combination thereof, but there is a SCMS Manager in all of these scenarios
- In overseas deployments in the United States and Europe, the SCMS Manager is also effectively the Root Certificate Authority.

Identifying and empowering an entity as the SCMS Manager will be an important step in achieving the right balance between security, privacy, cost and complexity, and the SCMS Manager will be a critical entity in identifying where scalability is required from the outset, and where capability can be accommodated at a later stage.

Broadly, the SCMS Manager is a centralised entity that:

- Sets standards and policies (security and certificate policies, rather than government policy, and potentially in coordination with the Root CA – see 6.1 on Architecture and 8.2 on Affiliation)
- Ensures compliance with the policy and regulatory environment
- Provides oversight, guidance, consistent interpretation and application of policies
- Liaises between government and industry
- Establishes and maintains relationships with international stakeholders and other SCMS Managers.

Empowering an entity as SCMS Manager has been identified as a critical decision because:

- The role is expected to lead the translation of the policy environment into technical and operational policies and systems that provide security – including providing technical advice and assistance of information needed to progress the key decisions identified in this document
- It is a decisive role in the development and ongoing operation and maintenance of the SCMS overall
- The SCMS Manager will be responsible for developing, implementing, circulating, maintaining and enforcing SCMS entities' compliance with clear and consistent security and certificate policies (see 8.2.4 on SCMS policy tools).

SCMS policy tools (security and certificate policies and certification practice statements) are expected to comprise the majority of policy requirements for a SCMS, and are contingent on enabling key decisions outlined in this document.

These system-level policy tools will also need to be informed by, and performed in consultation with, government and industry stakeholders, standards development organisations, the international C-ITS community, and the international community of SCMS Managers.

Beyond security and certificate policy, the implementation decisions necessary for the SCMS to reflect the key decisions above will be initiated and progressed by the SCMS Manager.

The SCMS Manager is also expected to lead international stakeholder engagement, coordination, affiliation, and knowledge transfer with international stakeholders and SCMS Managers.

Important here, although yet to be resolved in Australia, is the matter of the SCMS Manager being empowered to carry out its role, and this will be dependent on the entity/entities that operate this component and the SCMS governance structure. For example, although the United States is aiming to have a level of industry involvement in SCMS management, it has been pointed out by the USDOT that:

For example, both the Alliance and Mercedes [as two industry representatives] described the SCMS as a “core government responsibility.” Noting that “for V2V to work effectively, every vehicle manufacturer will have to participate in the SCMS and abide by its rules,” the Alliance explained that: “a private organization, such as a voluntary coalition of manufacturers, cannot compel unwilling manufacturers to join the organization, and cannot enforce deviations from the organization’s rules except by expelling misbehaving members. There is no effective mechanism to ensure the universal participation of all manufacturers and to compel their obedience to the necessary common SCMS requirements...”⁶⁰

9.2.3 United States

The United States SCMS industry will be privately run, with exception of the SCMS Manager, who will be the USDOT for a significant period of time.

The United States is in a position to have a privately run SCMS because government and industry have collaborated out of necessity due to the forthcoming rulemaking on C-ITS and the SCMS.

With this guidance from policy makers, pre-competitive industry consortiums and cooperatives have been able to resolve and advance technical, managerial and operational problems and decisions, either on behalf of, or to the distinct advantage of governments attempting to sound out regulatory details, desirables and necessities.

As SCMS Manager for a significant period of time, policy and decision makers, through the USDOT, will have the ability to establish the policy outcomes for the technical environment, and influence and respond to any development that require a change in operational policy to reflect the policy environment.

Although an industry run model is being advanced in the United States, where some SCMS functions administratively and legally sit – and who operates them – is not finalised due to, for example:

⁶⁰ Department of Transportation. 2016. Federal Motor Vehicle Safety Standards; V2V Communications, p. 231. Available at <https://www.transportation.gov/briefing-room/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands>

- User information linked to the system (which would affect Enrolment Certificate Authority entity/operations)
- Transparency issues for Misbehaviour Management and revocation (effectively: whether industry *can* or *should* monitor industry)
- Whether industry operating some SCMS functions is commerciality attractive (this will depend on the business model).

Through HTGs and other international initiatives, the USDOT is performing some of the key roles of the SCMS Manager.

9.2.4 Europe

As noted in 6.1 on Architecture and throughout this report, the European Commission's JRC is understood to be the SCMS Manager spanning the European federated SCMS Model.

In their strategy for C-ITS, published December 2016, the European Commission have articulated the challenge in deploying a common security solution for their federated SCMS model:

To develop and establish an EU-wide security framework, based on Public Key Infrastructure technology, for vehicles and public infrastructure elements, including a compliance assessment process, all stakeholders need to be involved. A key challenge will therefore be to set up the necessary governance at EU, national and industry levels involving all main stakeholders, including public authorities (e.g. transport ministries and the responsible national security associations), road operators, vehicle manufacturers, C-ITS service suppliers and operators. Developing a common security solution for the deployment and operation of C-ITS in Europe will in turn lay the foundation for stronger security at higher levels of automation (including vehicle to vehicle and vehicle to infrastructure communication).

This quotation usefully highlights:

- The range of stakeholders that will be involved in the SCMS deployment
- The need for a common, consistent approach
- The necessity of getting security right for C-ITS, in order to undergird future developments.

The specific actions pinpoint the importance of government involvement in setting the policy environment. Importantly, the second point introduces the possibility that the Commission's JRC will be the SCMS Manager:

- The Commission will work together with all relevant stakeholders in the C-ITS domain to steer the development of a common security and certificate policy for deployment and operation of C-ITS in Europe. It will publish guidance regarding the European C-ITS security and certificate policy in 2017.
- The Commission will analyse the roles and responsibilities of the European C-ITS Trust Model, and whether some operational functions and governance roles should be taken over by the Commission (as, for instance, in the case of the Smart Tachograph).⁶¹

⁶¹ European Commission. 2016. *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility*, p. 7-8. Available at http://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

TCA's working relationship with European stakeholders suggests that their SCMS PKI will be closely based on the Smart Tachograph – an operational regulatory framework similar to the Intelligent Access Program (IAP). The Smart Tachograph records professional driver rest and work activities for compliance control.

While the IAP has some important technical differences to C-ITS, on a framework and policy level, they are more or less identical. As noted in 8.2 on Affiliation, this has allowed a productive working relationship to develop between Australia through TCA and the European Commission.

At a high level, there are three main roles and associated responsibilities at the upper management level (which maps onto the SCMS PKI at the Root CA/SCMS Manager level) in the Tachograph operational framework:

- National Root Certificate Authority – distributes cryptographic keys to Member States
- Administration – manages the national 'sub' Root Certificate Authorities
- Security auditor – audits the Root Certificate Authority system.

Through HTGs and other international initiatives, the European Commission is performing some of the key roles of the SCMS Manager.

9.2.5 Options

The empowering of an entity as SCMS Manager would ideally be part of a nationally agreed deployment plan for security management, or at least progressed in unison with this deployment plan.

Effectively, both SCMS Managers for the United States and Europe are already actively involved in harmonisation and stakeholder engagement efforts through HTGs and associated initiatives, and these are duties that will be required of the Australian SCMS Manager.

For the management of the SCMS, there are risks and benefits associated with:

- Accountability – where the entity is strategically and commercially oriented between government and industry
- Expertise with PKI systems, environments and policies, and associated regulation (security, privacy, etc.)
- Ability to effectively engage overseas stakeholders (both for deployment and on an ongoing basis)
- Transparency issues for Misbehaviour Management and revocation (effectively: whether industry *can* or *should* monitor industry)
- Establishment costs – whether an entity needs to be built from the ground-up, or expand their existing role
- Ability to provide consistency to a variety of industry bodies, both within and interfacing with the SCMS
- Level of oversight required by governments.

The complications of a private sector SCMS Manager have not been widely explored, given that this option is not being considered in the United States and Europe.

The United States is aiming to have a privately operated SCMS, but the USDOT will be the SCMS Manager for a significant period of time; Europe will have private sector SCMS, but the European Commission's JRC is understood to be the SCMS Manager (comparable to the operational PKI compliance environment of the Smart Tachograph).

That a private sector SCMS Manager is not being contemplated by any region is largely because a SCMS and C-ITS in general will largely be an unprecedented phenomenon, and the complications of managing a SCMS are not yet fully known – and will not be fully known for years to come.

It is therefore reasonable to conclude that a level of government oversight is being understood as a political responsibility, and a way of managing the potential risks relating to policy control over technical and operational matters.

9.2.6 Parties Responsible for Advancing Decision

Using this report, and other resources, the determination of a SCMS Manager could be progressed by policy makers on a national level.

Appendix A: SUMMARY OF DOCUMENT

Table 10 Summary of Document

Key decisions	Policy		Domain role						
			Establish rules needed to provide guidance for the SCMS, to protect users and businesses, and who makes them						
		Types of decisions	SCMS specific	No.	Key Decision	Urgency ⁶²	Rationale	Options	Parties responsible for progressing
		<ul style="list-style-type: none">• The underpinning architecture and deployment of the SCMS• How information is gathered, distributed, used and destroyed in a way that it both optimal and compliant.• How vehicles will enter the connected SCMS security environment.• The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in ensuring this.	Architecture	1	Determine whether AU has one or multiple SCMS	High	<ul style="list-style-type: none">• US will have one SCMS; EU will have multiple: this is due to different levels of government involvement in C-ITS (mandatory in US) and geopolitical interests (EU).• SCMS are complex and expensive, and require local and international coordination – the <i>minimum</i> number is desirable.	<ul style="list-style-type: none">• Australia has one SCMS.• Australia has multiple SCMS.	<ul style="list-style-type: none">• TISOC/Austrorads (via National Policy Framework for Land Transport Technology).
2	Determine whether AU has a national SCMS (Root CA location)			High	<ul style="list-style-type: none">• Both US and EU will have ‘sovereign’ SCMS.• Local/overseas location of Root CA will affect alignment and level of policy, technical and operational control.• Overseas Root Certificate Authority not being contemplated by any other deployment.	<ul style="list-style-type: none">• Australia has a national SCMS (i.e. local Root CA).• Australia does not have a national SCMS (i.e. overseas Root CA).	<ul style="list-style-type: none">• TISOC/Austrorads (via National Policy Framework for Land Transport Technology).		
Privacy	3		Develop clear position on data usage and privacy policy	Medium	<ul style="list-style-type: none">• Privacy is a policy decision and an implementation choice, and critical for users and industry.• How data is used will guide SCMS day-to-day operations, required architecture, and enforcement implementation and capability.• Both EU and US have vision of outcomes, which are driving SCMS progress.	<ul style="list-style-type: none">• Determine policy outcomes, and how best to use data in a manner that is both optimal and compliant relating to:<ul style="list-style-type: none">◦ SCMS data usage: receive, store, discard and destroy.◦ Settings for levels of inter-SCMS access to data and privacy.◦ Harmonisation benefits.• Determine under what conditions data may be used for law enforcement e.g. warrant.• Develop national approach, harmonise on jurisdiction level.• No national approach.• Outcomes for potential use of data for non-SCMS purposes in future (Smart Cities, Internet of Things).	<ul style="list-style-type: none">• State/Territory Road Agencies, Cth.• SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.• Austrorads Project No. NT1785 Stage 2.• NTC (report published).		
	4		Determine user information for enrolment in SCMS	Low	<ul style="list-style-type: none">• User/vehicle information and linkages will affect SCMS roles and enforcement capabilities.• Technical and organisational measures to protect user/vehicle information are of equal importance.• US and EU still arriving at decisions.	<ul style="list-style-type: none">• Determine what information is desired/required at enrolment – what user will need ‘up front.’• Determine any impacts/conflicts with:<ul style="list-style-type: none">◦ Levels of privacy required.◦ Enforcement outcomes required.◦ Harmonisation benefits.	<ul style="list-style-type: none">• State/Territory Road Agencies, Cth.• Vehicle/device manufactures.• SCMS Manager optimally placed to inform discussion re impacts on SCMS operations, scalability, and industry impact.• Monitor and engage with US and EU deployment through appropriate channels and entities.		
Legal	5		Clarify and form consistent interpretation and application of existing privacy legislation	Low	<ul style="list-style-type: none">• No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.• US situation clearer; EU situation urgent and evolving.• Applicable regulations were not made with C-ITS/SCMS in mind. Exemptions may present complications.• Implications for SCMS can be assessed by appropriate entity at pre-implementation.	<ul style="list-style-type: none">• Determine policy outcomes, and how best to use data in a manner that is both optimal and compliant.• Develop national approach, harmonise on jurisdiction level.• No national approach – jurisdictions based.	<ul style="list-style-type: none">• State/Territory Road Agencies, Cth.• SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.• Implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.• Austrorads Project No. NT1785 Stage 2.• NTC (report published).		
	6		Compel vehicles to use SCMS	Medium	<ul style="list-style-type: none">• All stakeholders are anticipating the use of a SCMS – <i>how</i> users will be required to participate is important to establish.• US will be mandatory; in EU use will be more or less automatic and inventible.• Deployment applications using SCMS clear or progressing in US and EU; other uses also evolving.	<ul style="list-style-type: none">• Determine regulatory mechanism to compel vehicles to use SCMS.• Determine non-regulatory mechanism to compel vehicles to use SCMS.• Determine uses for SCMS (e.g. safety applications, non-safety applications).	<ul style="list-style-type: none">• State/Territory Road Agencies, Cth.• Vehicle/device manufactures.• SCMS Manager optimally placed to inform discussion re impacts on SCMS design, operations and scalability.• Monitor US and EU deployment through appropriate channels and entities.		

⁶² The urgency with which a policy decision is required to progress the Australian SCMS deployment is a relative ranking: all of these decisions are urgent, but some are of a higher urgency compared to others.

				7	Clarify implications of privacy and surveillance regulation and policy	Low	<ul style="list-style-type: none">No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.US situation clearer; EU situation urgent and evolving.Applicable regulations were not made with C-ITS/SCMS in mind. Exemptions may present complications.Implications for SCMS can be assessed by appropriate entity at pre-implementation.	<ul style="list-style-type: none">Determine policy outcomes, and how best to use data in a manner that is both optimal and compliant.Develop national approach, harmonise on jurisdiction level.No national approach – jurisdictions based.	<ul style="list-style-type: none">Government.SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.Implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.Austrroads Project No. NT1785 Stage 2.
				8	Clarify implications of security regulation and policy	Low	<ul style="list-style-type: none">No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.US situation clearer; EU situation urgent and evolving.Applicable regulations were not made with C-ITS/SCMS in mind. Exemptions may present complications.Implications for SCMS can be assessed by appropriate entity at pre-implementation.	<ul style="list-style-type: none">Determine policy outcomes, and how best to use data in a manner that is both optimal and compliant.Develop national approach, harmonise on jurisdiction level.No national approach – jurisdictions based.	<ul style="list-style-type: none">State/Territory Road Agencies, Cth.Implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.Austrroads Project No. NT1785 Stage 2.
				9	Clarify implications of consumer protection regulation	Low	<ul style="list-style-type: none">No regulatory barriers to C-ITS identified, and no SCMS-specific legislation planned in AU.US situation clearer; EU situation urgent and evolving.Applicable regulations were not made with C-ITS/SCMS in mind. Exemptions may present complications.Implications for SCMS can be assessed by appropriate entity at pre-implementation.	<ul style="list-style-type: none">Determine policy outcomes, and how best to use data in a manner that is both optimal and compliant.Develop national approach, harmonise on jurisdiction level.No national approach – jurisdictions based.	<ul style="list-style-type: none">State/Territory Road Agencies, Cth.SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.Implications for SCMS can be assessed by appropriate entity (possibly SCMS Manager) at pre-implementation.Austrroads Project No. NT1785 Stage 2.
Technical		Domain role							
		Establish what the SCMS should do, and how it should do it							
	Types of decisions	SCMS specific	No.	Key Decision	Urgency	Rationale	Options	Parties responsible for progressing	
	<ul style="list-style-type: none">How to mitigate risk, and protect the security and safety of usersHow information is protected and able to be exchanged, and how user ability to be trusted is confirmed.	Blacklist/Whitelist	10	Determine whether SCMS will use Blacklisting, Whitelisting, or both	Low	<ul style="list-style-type: none">Both common to US and EU deployments, although at different levels. Blacklisting is closely linked to Enforcement; Whitelisting to Certification.Opportunities to optimise cooperation and affiliation make national consistency and strategy desirable.	<ul style="list-style-type: none">Establish threat mitigation strategy (levels for Black/Whitelisting: applications, intra-/inter SCMS).Use Blacklisting.Use Whitelisting.Use both Blacklisting and Whitelisting.Determine linkages to Enforcement outcomes, and Certification processes.	<ul style="list-style-type: none">State/Territory Road Agencies, Cth.SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.Monitor US and EU deployment through appropriate channels and entities.	
		Cryptography	11	Determine cryptographic curve for use in AU	Low	<ul style="list-style-type: none">Fundamental decision – national approach highly desirable; jurisdictional approach close to unfeasible (economically/commercially, operationally, technically) but not impossible.US deployment unambiguous; EU will need to be monitored – highly technical decisions subject to political environment.Policy decision will trigger more complex work (lead by SCMS Manager) to ensure deployment and ongoing viability.A commitment to future security strategy prudent and desirable.	<ul style="list-style-type: none">Determine which cryptographic algorithm is most suited for AU: stakeholder outreach, test, trial, harmonisation.Determine level of oversight for adoption and use (regulatory, non-regulatory, endorsement).Use NIST.Use Brainpool.Use both NIST and Brainpool.Develop national approach, harmonise on jurisdiction level.No national approach – jurisdictions based.Commit to post-quantum strategy.	<ul style="list-style-type: none">State/Territory Road Agencies, Cth.SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.Monitor and engage with US and EU deployment through appropriate channels and entities.SCMS Manager will be responsible for cryptoagility.SCMS Manager will be responsible for leading post-quantum strategy.	
Operational		Domain role							
		Establish how the SCMS will work in the real world, today, tomorrow and into the future							
	Types of decisions	SCMS specific		Policy Decision	Urgency	Rationale	Options	Parties responsible for progressing	
	<ul style="list-style-type: none">How to mitigate risk, and protect the security and safety of users.How political alignment and engagement can shape technical decisions to boost international cooperation.The vetting processes to ensure products are safe and secure, meet expectations, and the SCMS role in supporting this.	Enforcement	12	Determine outcomes for enforcement and threat mitigation	Medium	<ul style="list-style-type: none">Both EU and US have mature visions for enforcement capabilities for deployment and beyond; developing capabilities are planned or being discussed. Both are being driven by desired policy outcomes.	<ul style="list-style-type: none">Determine security strategy.Adopt/adapt:<ul style="list-style-type: none">EU.US.Desirable aspects of US (without creating proprietary system).Determine outcomes for day 1:<ul style="list-style-type: none">What should be revoked.Conditions to be satisfied for revocation.	<ul style="list-style-type: none">State/Territory Road Agencies, Cth.SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.Monitor and engage with US and EU deployment through appropriate channels and entities.	

	<ul style="list-style-type: none"> The ability to offer uninterrupted support during disaster or upgrade. 					<ul style="list-style-type: none"> Revocation mechanism. 	<ul style="list-style-type: none"> Determine appetite for future enforcement capability. 	
		Affiliation	13	Determine whether Au should affiliate/plan to affiliate with EU, US, or both	Medium	<ul style="list-style-type: none"> EU will have to affiliate, but it will be a significant initial and ongoing challenge; US in a position to affiliate as desired. Harmonisation work undertaken by TCA gives AU the option to affiliate with EU more easily; this could be progressed with US. Doing the formal and informal groundwork at pre-deployment desirable. Will also inform/be informed by architecture decisions. 	<ul style="list-style-type: none"> Affiliate with EU (day 1 or future). Affiliate with US (day 1 or future). Affiliate with both EU and US (day 1 or future). Determine desired trust levels for affiliation (day 1 and/or future). 	<ul style="list-style-type: none"> State/Territory Road Agencies, Cth. SCMS Manager optimally placed to lead stakeholder engagement and affiliation groundwork (stakeholder, policy, highly technical). SCMS Manager optimally placed inform discussion re impacts on SCMS operations and scalability. Monitor and engage with US and EU deployment through appropriate channels and entities.
		Certification	14	Determine desired levels of compliance assurance	Medium	<ul style="list-style-type: none"> Balance required. Desired levels of trust essential to protect and assure government, industry and users; market will not tailor itself for AU needs. Decisions will affect devices before and after participation in SCMS. Progress in US well under way; urgent in EU. 	<ul style="list-style-type: none"> Determine non-regulatory deployment model. Determine regulatory standards (potential or actual). Determine uses of SCMS (e.g. safety applications/non-safety applications). Determine whether to leverage compliance assessment regimes from EU, US or both. Determine end of life process for devices. 	<ul style="list-style-type: none"> TISOC/Commonwealth (via National Policy Framework for Land Transport Technology). TCA has progressed security and identifier standards with Austroads.
		Disaster Recovery	15	Determine disaster recovery and business continuity management	Low	<ul style="list-style-type: none"> Essential but local (desirably national) decision. Redundancy and disaster recovery measures can be progressed by SCMS Manager; broader business continuity management approach to be set at policy level. 	<ul style="list-style-type: none"> Deploy at least one additional backup SCMS. Develop business continuity management approach. 	<ul style="list-style-type: none"> State/Territory Road Agencies, Cth. SCMS Manager to lead disaster recovery once business continuity management strategy set by government policy. SCMS Manager optimally placed to inform discussion re impacts on SCMS operations and scalability.
Commercial	Domain role							
	Establish the commercial decisions required for the SCMS, the impacts to government and industry, and who will benefit							
	Types of decisions	SCMS specific		Key Decision	Urgency	Rationale	Options	Parties responsible for progressing
	<ul style="list-style-type: none"> Decisions underpinning initial and ongoing economic and organisational composition and viability of the SCMS Nominating the entity who will translate the policy environment into SCMS technical policy design and operations, ensure compliance, and engage national and international SCMS stakeholders. 	Business Model	16	Determine SCMS business model	High	<ul style="list-style-type: none"> US and EU know how SCMS will work not just politically, but organisationally and commercially. Level and method of SCMS funding will affect overall technical design and operational capability – these matters can only be progressed so far without certainty of business model. Policy outcomes need to be guided by what is economically feasible. 	<ul style="list-style-type: none"> US and EU models likely to be divergent, given different mandated/voluntary approaches. AU federated model will make national agreement highly desirable. Costings to guide decisions are indicative – policy decisions in other areas will need to be anticipated/factored in. 	<ul style="list-style-type: none"> State/Territory Road Agencies, Cth.
		Organisation	17	Determine SCMS Manager	High	<ul style="list-style-type: none"> Both the US and the EU have incumbent or effectively incumbent SCMS Managers (USDOT and EC Joint Research Centre); governments in US and EU will play leading roles in setting SCMS policy. For pre-deployment, SCMS Manager role is able to inform policy development by telling decision makers: <ul style="list-style-type: none"> What is available. What the costs would be. How policy intent can be realised. Where policy intent may conflict with other requirements and capabilities. Incumbent SCMS Managers serve as a point of contact for progressing technical matters, and in EU and US are liaising with industry and international stakeholders. SCMS Manager can take the lead, or help to progress issues of Medium or Low urgency. 	<ul style="list-style-type: none"> Government managed Industry managed Industry managed with government oversight (development and monitoring). Private sector SCMS Manager has not been widely explored, given that this option is not being considered in the United States and Europe. 	<ul style="list-style-type: none"> State/Territory Road Agencies, Cth.

