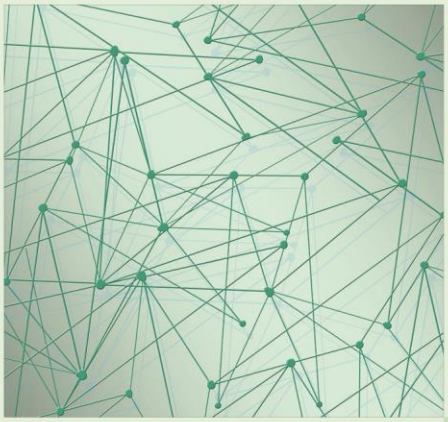
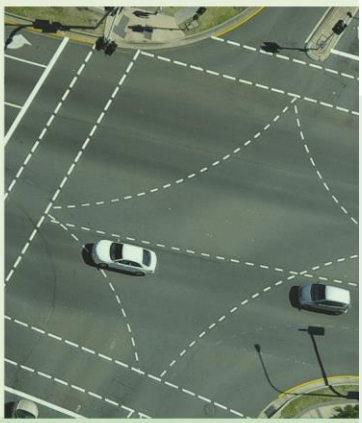
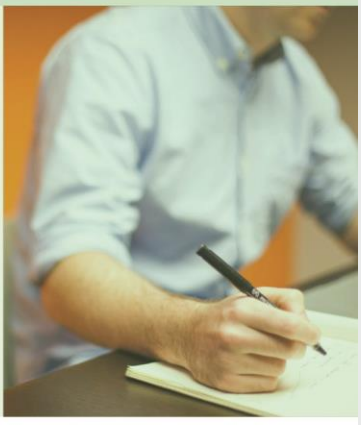
Transport Certification Australia

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





EXECUTIVE COMPANION



www.tca.gov.au

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	Executive Companion: Key Decisions to Progress Australian Deployment of a SCMS
Document Number	TCA-B066
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

EXECUTIVE SUMMARY

The purpose of this document is to serve as an Executive Companion to the Full Report, *Key Decisions for Progressing the Deployment of a Security Credential Management System in Australia*, available on request from TCA.

This document and its counterpart intend to contribute to the existing body of knowledge, and to facilitate national collaboration on security management for cooperative and connected vehicles.

Background

Connected vehicles are being deployed to make our roads safer and smarter. The benefits of this technology are widely discussed; less so the risks. These risks are familiar to the ICT/cybersecurity sphere; but they are safety threats for the connected transport network.

A Security Credential Management System (SCMS) is the generic term adopted internationally for the system (encompassing people, policies and processes and technologies) that provides security for the C-ITS environment.

In this way, it can be understood as a security management environment that needs to be designed and deployed, managed on an ongoing basis, and interface with other security environments and systems.

A SCMS provides security for the 'internet of cars' and is being deployed in the United States and across Europe. Australia has worked in close collaboration with international policy and technical experts to create the SCMS, and an interrelated, harmonised security policy framework (and other key resources) that stand to benefit all regions.

Australia is now proposing to implement its own SCMS. This document is intended to contribute to that process, by outlining the key issues for the consideration of decision makers.

TCA's role

TCA is the nominated Australian agency to work with United States and European agencies to achieve international harmonisation of key aspects of connected vehicles (or Cooperative Intelligent Transport Systems, C-ITS). In particular, Harmonisation Task Group (HTG) 6 deals with harmonisation of security solutions and frameworks.[1]

TCA hence has an obligation to keep its Members (and other selected national agencies) informed of progress, developments and issues arising from this work.

[1] HTGs bring together and draw on the expertise of vehicle and equipment manufacturers, technical standards development organisations, and government bodies. The co-leads are the United States Department of Transportation, the European Commission. TCA has joined the two specific HTGs as a co-lead for security matters. 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.

This work builds upon TCA's discussion paper entitled *Towards a national vision for a secure, connected future through Cooperative Intelligent Transport Systems (C-ITS)*.[2] This document condenses the material presented in the Full Report so that policy and decision makers can have the issues at their fingertips.

Each section presents a snapshot of what are complex decisions that will need to be made for the Australian deployment of a SCMS: it bypasses the detail and captures the core nature of the problem to be solved.

Therefore, this Executive Companion document should not be the basis for *decisions*, but rather for *discussion*.

Progressing an Australian SCMS

Cooperative Intelligent Transport Systems (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).

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

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

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.

[2] 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

A SCMS is not just a technical system. Nor is it an off-the-shelf product or a ready-made solution. Like any piece of digital/physical 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 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.

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.

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.

Contents

1 SCMS BASICS

1.1 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.

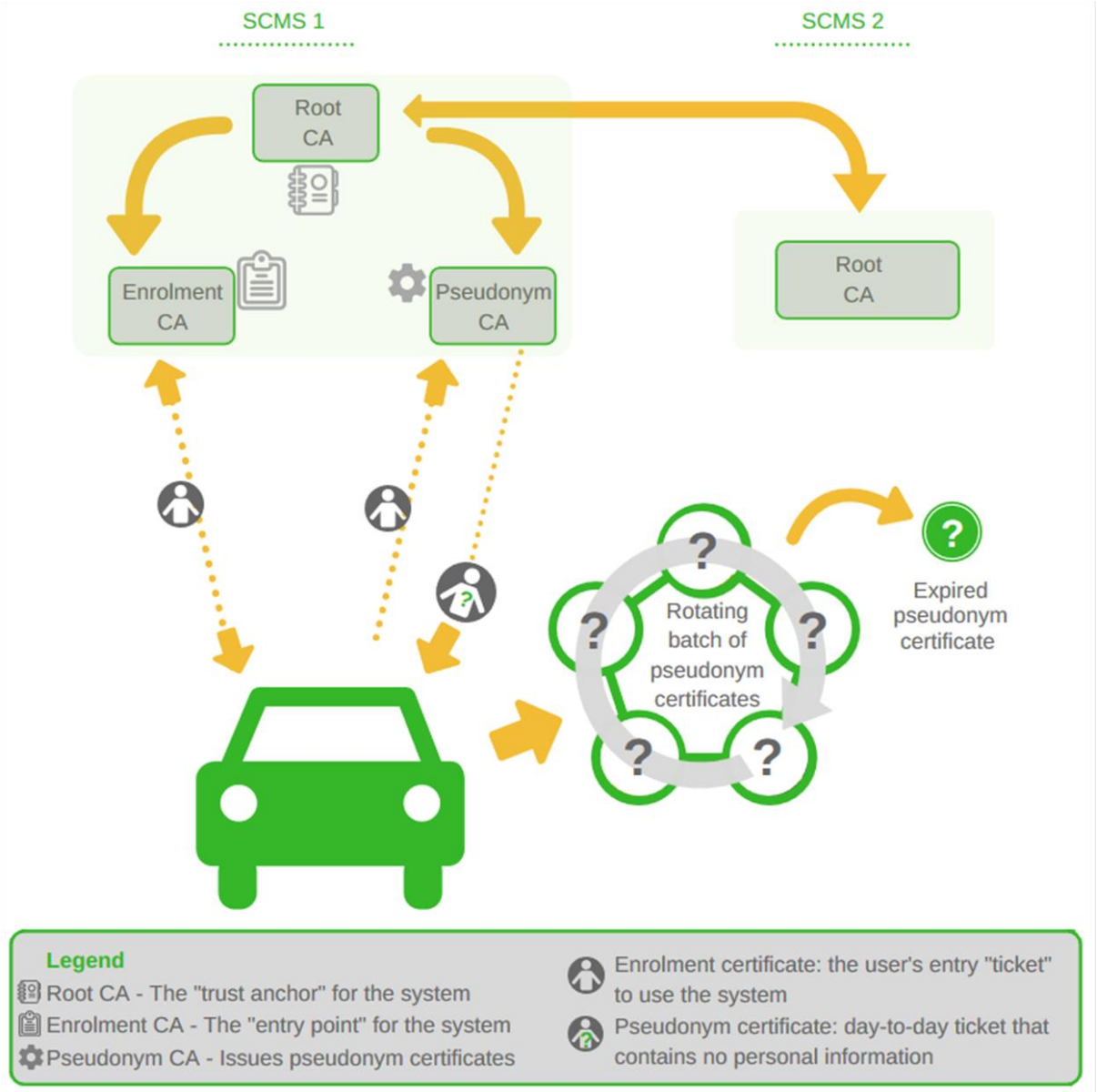
- Vehicles (and devices in pieces of infrastructure, etc.) have to be enrolled or registered into the system by authorised bodies known as Enrolment Certificate Authorities.

- 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.

1.2 Operation

The figure below represents a distilled presentation of how a SCMS operates.



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 certificate[3] – a very important item that allows the user to participate in the SCMS.

[3] All 'signatures' and 'certificates' are digital; these processes are 'online' and automated.

- 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.

2 FREQUENTLY ASKED QUESTIONS

The table 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.

Why does security matter for cars?

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.

It is also very possible to intercept messages on a computer network.

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.

What does a SCMS create?

A SCMS creates trust for a specific security domain. A security domain can be defined as:

> 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.[4]

A SCMS security domain can be defined by at least one or a combination of the following:

- 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?

Yes. But not for very long, and not for more than a handful of users.

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.

Added to this: the SCMS and security in general will keep you safer on the road.

All parties, from governments to vehicle manufacturers are aware of and are planning to use a SCMS.

What is 'trust' in the context of C-ITS and the SCMS?

Trust is multifaceted. Basically, it means being able to know you can rely on the users around you, without knowing who they are.

The United States Department of Transportation writes that trust is:

> 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

[4] 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.[5]

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.

[5] 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.

3 WHAT THIS REPORT PROVIDES

The Full Report provides readers with the strategic context, and the key decisions that 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: these key decisions will impact the ability of the SCMS to provide security support and services that deliver policy outcomes, and meet user expectations and needs.

This Executive Companion to the Full Report presents the decisions according to their domain: policy, technical, operational and commercial.

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
	• 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 • Privacy • Legal
Technical	Domain role	
	Establish what the SCMS should do, and how it should do it	
	Types of decisions	SCMS specific
	• 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	• 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
	• 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.	• 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
	• 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 • Organisation

IN THE FULL REPORT...

Concepts

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 deployments

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.

The key decisions to progress the deployment of the SCMS in Australia are ranked into High, Medium or Low in Urgency. The full rationale for this ranking is contained in the Full Report, but the following has been taken into consideration:

- 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.

Where this document identifies evolving discussions overseas, this does not indicate that key decisions should be reserved, or that expressing clear 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 ranked as 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.[6]

These key decisions are captured in the table below. There are:

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

[6] 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.

	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

4 KEY POLICY DECISIONS

4.1 Architecture

Decision type	No.	Key decision to progress SCMS	Urgency
Architecture	1	Determine whether AU has one or multiple SCMS	High
	2	Determine whether AU has a national SCMS (Root CA location)	High

The United States and European SCMS deployments have pursued different paths. There is no one reason for this, but overall, the United States is progressing with a planned mandating of C-ITS, whereas Europe is progressing a voluntary uptake: this has resulted in different technical and political results and solutions.

The United States is progressing with one SCMS for the country. The United States Department of Transportation (USDOT) will be the SCMS Manager – the entity that translates policy outcomes into technical and operational systems and processes – for a significant period of time.

The main difference in Europe is that there will effectively be multiple SCMS, some of them run by Member States, some by vehicle manufacturers, and perhaps other entities. There are many reasons for this outcome, but the main one is political: countries in Europe will need to work together for the benefit of users and the market, but many Member States want to preserve their autonomy by having their own SCMS.

Nonetheless, the European Commission's Joint Research Centre (JRC) is anticipated to become the SCMS Manager for such a federated European SCMS deployment.

The 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.

Nonetheless, Europe will have a 'federated' SCMS environment – although this 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). These Root Certificate Authorities will be added into the 'overall' European SCMS 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. For ease of understanding, it is useful to understand this as a federated, multi-SCMS solution, with central European Commission administration and coordination.

Australian policy makers will need to decide whether there is one or multiple SCMS. This is a not just a question of funding, but will involve technical, organisational and commercial considerations. These are complex, and explored throughout the Full Report. Overall though, a SCMS for each 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.

The second decision is whether Australia has a national SCMS. This will be determined by the location of the Root Certificate Authority: there are lots of entities in the SCMS, but they all inherit their trust and ability to trust others from the Root Certificate Authority; the Root is the 'trust anchor' and holds the network together. In the United States, the USDOT as SCMS Manager will oversee the Root Certificate Authority; in Europe, there will be multiple roots, understood to be overseen by the JRC, and the JRC will serve as the Root Certificate Authority for some SCMS.

In the United States and Europe, the SCMS Manager is also effectively the Root Certificate Authority.

For Australia, the decision is whether the Root Certificate Authority is in Australia or overseas – effectively whether the Australian has a 'national' SCMS. 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.

In the national SCMS scenario, 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.

With an overseas Root Certificate Authority, depending on the location and or the entity, 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. For security and certificate policies (the technical 'rulebooks' for the SCMS) they may have to be 'off the shelf.'

Having an overseas Root Certificate Authority is not the same decision as outsourcing work to an organisation. It *may* be acceptable that a SCMS Manager would delegate the task of Root Certificate Authority to a third-party (although this does not seem to be considered an option elsewhere). Outsourcing of the Root Certificate Authority would be performed on the assumption that they could audit and intervene both in the event of an emergency, and to tailor management and operational polices and processes as needed to enhance or correct capability or errors. This ability may be significantly diminished with an overseas Root Certificate Authority.

It is also important to note that 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 comparable scenario, given that the JRC is also understood to be the SCMS Manager.

There are additional considerations here, explored in the Affiliation section (6.2). 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 (with some Root Certificate Authorities 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.

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 these systems are not yet fully known – and will not be fully known for years to come. (The issue of 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.

TISOC/Austroads 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.

4.2 Privacy

Decision type	No.	Key decision to progress SCMS	Urgency
Privacy	3	Develop clear position on data usage and privacy policy	Medium
	4	Determine user information for enrolment in SCMS	Low

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. 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.

Privacy measures should:

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

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

Policy makers may also wish to factor in future developments, whereby 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.

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, no single entity has enough information to identify the full complement of certificates associated with a device.

By comparison, Europe has a more risk-based approach to internal privacy and security: they will have fewer SCMS roles, and a less sophisticated data management approach. However, European internal discussions and reports are quickly evolving, and it is likely that internal security will become more robust for deployment, and increase over time.

In simplified terms, the United States has 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 has 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 necessarily 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 defined policy objectives.

Privacy policy considerations will also extent to the enrolment process when a device/user first enters the SCMS. Enrolment information and processes will determine the extent to which user, C-ITS device and vehicle information is linked, who stores it, and how it is used, such as for Enforcement. For example, a C-ITS device could potentially contain information such as a VIN or vehicle registration, or information about the device production batch.

Enrolment details are still being worked out by the United States and Europe, but the design of the United States SCMS will make this less of a concern than in Europe, who must provide flexibility for Member States, while still implementing a region-wide solution to the greatest possible extent.

Awaiting an international decision should not deter policy makers from establishing their own clear outcomes and expectations. It would be advantageous for Australia to pursue a national approach as much as possible: 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.

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.

The European 'risk management' approach is the product of extensive collaboration and compromise – both from political and technical perspectives. Articulated privacy and security outcomes for Australia would allow analysis of whether with a European solution could be explored in more detail.

Privacy and data usage measures are directly tied to policy decisions and outcomes, and may have impacts on SCMS architecture, and the SCMS Manager would be logically positioned to inform policy makers:

- 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.

4.3 Legal

Decision type	No.	Key decision to progress SCMS	Urgency
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

Relevant legislation will be important to ensure that the SCMS – in its design, implementation, deployment and ongoing operation – is compliant. 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.

The likely mandating of C-ITS in the United States has provided a great deal of focus and momentum and shaped pre-implementation activities. 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 necessitates. 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.

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. 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 a much more uneven development approach, and the need for a coherent legislative framework for day deployment is now urgent. Nonetheless, the European Commission are acutely aware of the problem at hand. This, and the urgent need for resolution have animated discussion. In their December 2016 strategy document, the Commission have stated specific actions to be undertaken for development of a legal framework. [7]

While the United States is progressing with the C-ITS mandate, which will require vehicles to use the SCMS, Europe is progressing a voluntary adoption, presenting problems with determining what the SCMS will be used for, whether it be safety or non-safety applications, types of vehicles, emergency response, etc.

No specific regulatory measures for the SCMS have been proposed, and the need for them has not been identified. Policy makers will need to determine how C-ITS devices should be compelled to use the SCMS and be enrolled into the C-ITS environment via the SCMS, be it regulatory or non-regulatory. 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.

There is also a body of existing regulation and policy that will affect the SCMS concerning privacy and surveillance, security, and consumer protection. Some of this is national legislation, while there is a wide variety or jurisdictional legislation and policy. In addition to assessing the details, there is a need for clarity surrounding the interpretation and application of this legislation for the SCMS.

[7] 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

This is more generally a matter for C-ITS. 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.

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. This would likely be best investigated by the SCMS Manager. The SCMS Manager would also 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.

5 KEY TECHNICAL DECISIONS

5.1 Blacklist/Whitelist

Decision type	No.	Key decision to progress SCMS	Urgency
Blacklist/Whitelist	10	Determine whether SCMS will use Blacklisting, Whitelisting, or both	Low

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 for:

- Internal operation of the SCMS: the SCMS fosters trust; if entities within the SCMS cannot be trusted, this has cascading effects throughout the C-ITS environment
- Devices/users: 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.

Two strategies and practices are of relevance here: Blacklisting and Whitelisting.

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.

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.

Blacklisting is a more reactive approach common in ICT environments (e.g. anti-virus software); Whitelisting is more proactive, and requires up-front assessment of applications before they are allowed to be deployed (and has not been tested or used before for something like the entire transport network).

There are administrative differences in how the two are used, but their effectiveness will both rely on rapid updating. There is also potential for these lists to be shared or referenced between SCMS, if other trust requirements are met.

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. 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. 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.

5.2 Cryptography

Decision type	No.	Key decision to progress SCMS	Urgency
Cryptography	11	Determine cryptographic curve for use in AU	Low

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,' and it protects privacy. Devices and an environment that use the same cryptography speak the same 'language' – an unknown cryptographic language will not be understood or trusted.

C-ITS and the SCMS will use a type of cryptography called Elliptic Curve Cryptography, the details of which are not important here. Elliptic Curve Cryptography is a highly specialised area, but policy decisions surrounding it are in some respects quite straightforward.

There are essentially two elliptic curves available for C-ITS cryptographic operations – NIST (US in origin, but used globally) and Brainpool (more European). Both are fit for purpose from security perspectives, and for the computer processing power of a C-ITS device.

The United States is implementing NIST (U.S. National Institute of Standards and Technology) alone, while Europe has grappled with geopolitical tensions (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.

Once a decision is made on a curve, the SCMS Manager will need to plan for cryptoagility: the ability to adapt to requirements and threats, plan for updates and support users running old systems – some of these are a matter of *when* rather than *if*.

Quantum computing will also pose a threat to cryptography, and will be an issue for security well beyond the transport portfolio. Both the United States and Europe have recommended post-quantum cryptographic strategies by 2020, and it would be prudent for Australia to do the same.

Both curves have significant penetration in the finance and e-commerce spheres, and more detailed analysis for C-ITS is 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. Australia should also monitor developments in Europe, likely on a county-by-country basis level, given that Europe may need to implement a regional solution to a local problem.

Having to support both NIST and Brainpool 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. Deployment (at least for day 1 and the medium-term) using (and supporting) both curves is likely to be neither economically nor operationally feasible.

Selecting a curve would ideally be advanced at a national level, involving input from all jurisdictions, and the entity designated as SCMS Manager: a multi-SCMS environment supporting different crypto curves would be the cyber equivalent of different rail gauges.

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. Continued involvement in and monitoring of the European situation and international developments is critical for Australia.

6 KEY OPERATIONAL DECISIONS

6.1 Enforcement

Decision type	No.	Key decision to progress SCMS	Urgency
Enforcement	12	Determine outcomes for enforcement and threat mitigation	Medium

Enforcement refers to measures that the SCMS undertakes to mitigate risks – be they active or potential – within the SCMS and on the road. These are not law enforcement activities, although breaches and investigations may result in law enforcement actions.

Enforcement methods are called Misbehaviour Management functions, and the most important one is revocation. Revocation is difficult and complex: users need to be anonymous, yet threats need to be handled. Revocation *must* be supported. Without it, there is no way to remove threats to privacy and safety. How robust these measures are is a policy decision. There are basically two types of revocation:

- **Active:** Revocation Lists 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.
- **Passive (which is *not* revocation as such):** a device is blocked from getting new certificates: once their current batch expires, they cannot acquire new ones, and the device effectively 'withers on the vine' or is 'revoked by expiration.'

The United States is deploying a highly sophisticated approach to revocation. Compared to Europe, they are placing a higher premium on privacy within the SCMS, and therefore need a more complex solution with additional entities.

Europe is currently focussing on a more 'passive' approach, mitigated by reducing the amount of time for which certificates are valid. However, European internal discussions and reports are quickly evolving, and it is likely that more advanced and active revocation measures will be deployed.

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 European SCMS.

'Passive revocation' or 'revocation by expiration' is not very robust, and cannot intervene into the C-ITS environment: *threats remain threats* for as long as their certificates are valid – vehicle manufacturers may give cars enough certificates to keep them on the road for a one, two or three *months or years*: essentially, there could be threats on the road for a long time.

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

Governments should note that C-ITS devices will be installed in infrastructure controlled by road agencies, not just in vehicles. 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, and would greatly benefit from revocation capability.

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. [8]

Policy makers need to decide, as part of a security and risk management strategy:

- What should be revoked
- The conditions that need to be met
- The mechanism for revocation.

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

Given that revocation measures are directly tied to policy decisions, 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.

[8] 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

6.2 Affiliation

Decision type	No.	Key decision to progress SCMS	Urgency
Affiliation	13	Determine whether AU should affiliate/plan to affiliate with EU, US, or both	Medium

Affiliation and harmonisation has to with easing the burden of the technical, policy, operational and commercial coordination involved in establishing and maintaining trust between regions. They reduce development, deployment and ongoing costs for governments, and provide a more 'seamless' experience for the global market, and for the mobility of users.

For the CCMS, it is essentially about how 'compatible' one SCMS is with another – although compatibility refers to the technical aspects of the system, and to the policy that guides it. This compatibility can be across several levels – from 'full' compatibility, to medium to low.

For Australia, this means affiliating with either Europe, the United States, or both. This would involve a policy decision, and then substantial technical work by the SCMS Manager, using a combination of major design decisions, minor tweaks, and significant stakeholder engagement.

Because Europe will have multiple SCMS, they will have to compatible – maybe not fully, but compatibility will the default, and the level will be set by technical elements, but also commercial, political and strategic motivations.

The United States will have a single SCMS, and will not have to manage the intricacies and complexity of the European federated model, or the political ambiguity and interests of Member States for a region-wide solution.

A policy decision to affiliate would lead to substantial work the SCMS Manager, mainly in how they develop and align three specific policy tools:

- **Security Policy:** 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:** what participants, both in the SCMS and users, must do
- **Certification Practice Statements:** very technical tool stating what a certification authority does when issuing, managing, revoking, and renewing and updating certificates.

These three policy tools are technical instructions that reflect policy decisions: if the policy says that a device must do a particular thing, or meet a certain standard, these policy tools reflect that in technical terms, and all entities and users must abide by them. These cannot be progressed until the other key decisions in this document are given attention.

If Australia wants a high level of control over these tools – to establish and update them as necessary – it will have to consider that having an overseas Root Certificate Authority (the trust anchor of the *entire system*) will limit these options.

Through TCA, Australia now has the option moving forward to harmonise with the security and certificate policies currently being drafted in Europe, as both TCA and the European Commission have been able to share knowledge about developing these policy tools for transportation based PKI.

This has ensured that, should Australia choose to affiliate itself with European SCMS and C-ITS deployments, this task will be substantially easier. These alignment options could be extended to pre-deployment harmonisation with the United States.

Either way, these relationships will need to endure, and a national SCMS would make the ongoing task easier.

There are additional options whereby Australia could harmonise closely with the European SCMS model, and integrate with it while have considerable autonomy over the SCMS Management function and Root Certificate Authority component. 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.

TISOC/Austroads 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.

Once a decision is made, the SCMS Manager would progress these in consultation with policy and decision makers, and in coordination with Europe and/or the United States, as policy dictates.

6.3 Certification

Decision type	No.	Key decision to progress SCMS	Urgency
Certification	14	Determine desired levels of compliance assurance	Medium

Certification – or more generically, compliance assurance – is the practice of ensuring that trust can be tested and verified. 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. C-ITS devices will require a level of certification, and it is expected that some applications will too.

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.

The complexity here is that certification practices will be effectively *external* to the SCMS, but will *affect* SCMS operations and SCMS policy tools. 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 will be required to provide lifecycle security and management for the C-ITS device. 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).

Both the United States and Europe are grappling with the issue of how to ensure compliance for devices, and what levels of assurance will be needed.

The United States is rapidly progressing with these policies and procedures, and compliance assurance options for devices. They have also acknowledged 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.

The European compliance assurance model is placing a premium on regional and international coordination, and is currently being developed. In their strategy for C-ITS, published December 2016, the European Commission has stated their intentions for a compliance assessment path, noting that higher levels of assurance are required for safety-critical applications.

International engagement will be key for Australia, such as with the European Commission's C-ITS Platform, and TCA's continued participation with the Harmonisation Task Groups (HTG). Both could facilitate the ability recognise and leverage compliance overseas assessment processes, easing the effort required for Australia.

Together, these options would ensure that Australia's compliance assurance framework, when it is developed, is consistent (where appropriate and beneficial) with those overseas.

TISOC/Commonwealth and TISOC/Austroads are the lead entities two actions items in the National Policy Framework for Land Transport Technology that will advise on regulatory and non/regulatory standards and deployment models, and a plan for the security management of connected vehicles. TCA has also been progressing work on security standards and compliance assessment options with Austroads.

6.4 Disaster recovery

Decision type	No.	Key decision to progress SCMS	Urgency
Disaster Recovery	15	Determine disaster recovery and business continuity management	Low

Planning for disruptions caused by upgrades and disasters 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.

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.

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.

Deployment of a SCMS without *at least one additional* SCMS is practically unfeasible – the risks are too great. A 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.

The broader policy and strategy for business continuity is a local (ideally national) policy decision. 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.

The technical and operational provisions for disaster recovery will be the responsibility of the SCMS Manager, and tailored to suit the policy.

7 KEY COMMERCIAL DECISIONS

7.1 Business model

Decision type	No.	Key decision to progress SCMS	Urgency
Business Model	16	Determine SCMS business model	High

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.

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 organisational 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.

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: enforcement and privacy are not 'bolt-ons' – what they will provide for 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.

In the United States, while the *functions* of the SCMS have been mapped out, *who* will perform them is yet to be determined (with the exception of the USDOT as SCMS Manager for a significant period of time). 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.

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). The latest strategy published by the European Commission in 2016 no doubt will make their business models sharper. While there will be substantial industry involvement in the European model – indeed, in some cases more than in the United States model – the key difference can be drawn along the lines of 'management' components and 'operational' components. The management components – including the Root Certificate Authority/Authorities and the SCMS Manager – in both models are either operated or managed by public bodies.

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. Automotive manufactures will likely play a significant role and will have their own commercial decisions made or in preparation.

TCA is progressing indicative costings for the SCMS 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, desired levels of Privacy and Enforcement may necessitate additional SCMS entities, capabilities and resources. Knowledge of a clearer funding model would also flow in the opposite direction and give a greater idea of the options and how costs could be apportioned.

Engaging with service providers that will comprise SCMS entities will be undertaken by the SCMS Manager, who will need to take into account security and privacy requirements and the entity's ability to meet them. 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.

7.2 Organisation

Decision type	No.	Key decision to progress SCMS	Urgency
Organisation	17	Determine SCMS Manager	High

The SCMS Manager will be one of the key entities responsible for progressing the design and implementation of the SCMS, and can take the lead once policy decisions are made. They can also provide technical input into the policy making process, as in the United States and Europe.

The SCMS Manager is broadly responsible for ensuring that the SCMS effectively translates the policy environment into operational policies and systems that provide security services and support. 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 outsourcing 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.

The SCMS Manager is fundamental, and all regions that are progressing a SCMS will have one. 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 technical standards and operational security policies
- 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.

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. As SCMS Manager, 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 developments that require a change in operational policy to reflect the policy environment.

It is understood that the European Commission's JRC will serve as the SCMS Manager spanning the European federated SCMS Model. In their strategy for C-ITS, published December 2016, the European Commission has introduced the idea (without explicitly stating) that the JRC will be the SCMS Manager, and will work similar to the Smart Tachograph – an operational regulatory framework similar to the Intelligent Access Program (IAP).

In the United States and Europe, the SCMS Manager is also effectively the Root Certificate Authority (although this is more complicated in Europe, whereby the SCMS Manager will oversee a federated model comprising multiple 'modularised' SCMS, each with a Root Certificate Authority operated by a Member State or private organisation).

Both incumbent (USDOT) and effectively incumbent (JRC) 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 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.

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. This is likely because SCMS and C-ITS 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 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.

Important here, although yet to be resolved in Australia, is 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 are 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…"[9]

Using this report, and other resources, the determination of a SCMS Manager would be progressed by policy makers on a national level.

[9] 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

Transport Certification Australia