Transport Certification Australia

DISCUSSION PAPER

Towards a national vision for a secure, connected future through Cooperative Intelligent Transport Systems (C-ITS)

About TCA

Transport Certification Australia (TCA) is a national government body responsible for providing assurance in the use of telematics and related intelligent technologies, to support the current and emerging needs of Australian Governments and stakeholders.

TCA is a 'cross-cutting' organisation which works across different policy streams, surface transport modes, and government and industry sectors.

TCA is governed by a Board of Directors, which consists of senior representatives from road and transport agencies of the Commonwealth, State and Territory Governments.

Our vision is to be the Australian leader of Advice, Accreditation and Administration services, and to be an essential partner to government organisations to achieve public outcomes through the use of telematics and related intelligent technologies.

TCA provides independent Advice, Accreditation and Administration services for a suite of transport-based policy reforms, and national and international initiatives that use telematics and intelligent technologies and transport systems. TCA provides:

- **Advice** founded on a demonstrated capability to design and deploy operational systems and services as enablers for reform
- **Accreditation** in the type-approval and certification of systems and services that give confidence to all stakeholders
- **Administration** of programs for, and on behalf of, TCA's Members and other government organisations.

TCA collaborates nationally and internationally with key organisations on emerging technology and policy issues to ensure Australia's interests are reflected as these issues develop, and that Australia is positioned to engage and influence in the long term.

Transport Certification Australia

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	Discussion Paper: Towards a national vision for a secure, connected future through Cooperative Connected Transport Systems (C-ITS)
Document Number	TCA-B047
Version	1
Version Date	July 2016
Printing Instructions	Double sided, colour

Document History

Version	Date	Description
1	July 2016	Final

EXECUTIVE SUMMARY

Cooperative Intelligent Transport Systems (C-ITS) enable real-time wireless communication between vehicles, roadside infrastructure, mobile devices and back-office systems. They have been developed as a way to deliver a safer and more efficient transport network that is less congested and more environmentally friendly.

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.

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.

The common error is to view these transformations as a collection of technical problems requiring technical solutions.

As one submission recently articulated the problem: 'The main issue is how we actually do this paradigm shift into the technology space. So far the approach has been on a project-by-project basis... But at the national level we are lacking a national vision.'[1]

Governments have a pivotal role to play in this space – now, and in order to guarantee its future.

TOWARDS A NATIONAL VISION FOR A SECURE, CONNECTED FUTURE THROUGH C-ITS

This discussion paper prepared by Transport Certification Australia (TCA) is intended to inform and provoke discussion, and contribute to the development of this national vision. It builds on previous papers published by TCA with a view to advancing Australia's interests in adopting C-ITS in a manner that delivers safe, secure, and commercially and operationally sustainable results.

By focussing on security, this paper addresses the lack of discussion – and in some cases, the total silence – in this space.

The security solution for the connected, C-ITS environment that has emerged out of international collaboration is called a Cooperative Credential Management System (CCMS). The concept of a CCMS is a central pillar to enable security across systems.

A CCMS is both an institutional framework and a piece of infrastructure, encompassing human/management, electronic and physical elements –it is 'cyberphysical.' Like any piece of infrastructure, its development needs to be approached as a long-term investment: the product of

[1] Standing Committee on Infrastructure and Communications. 2015. *Smart information and communications technology in the design and planning of infrastructure.* Proof Committee Hansard. Commonwealth of Australia, p. 26 Available at http://www.aph.gov.au/Parliamentary_Business/Committees/House/ITC/Smart_ICT

careful policy, planning and consideration as to its capability and longevity, and the organisational elements necessary to operate and maintain it.

This paper articulates why 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.

This discussion paper is aimed at governments, policy and decision makers, and industry stakeholders.

This paper is also intended to be accessible and understandable to members of the public, and those that have an interest in key developments that will shape the automotive and transport sectors, and our cities.

In so doing, this paper recognises that the public are the most important stakeholder. In the cooperative and connected environment, whether they are drivers, passengers, cyclists or pedestrians, everyone will be an end user.

Cities, roads and transport networks are, above all, made for people, and they depend on governments to get it right.

AUSTRALIAN FOUNDATIONAL REQUIREMENTS FOR A NATIONAL CCMS

TCA has published and made publically available the Foundational Requirements for a National CCMS in Australia. These Foundational Requirements have been developed by TCA, drawing on leading Australian work, and its international collaboration and co-leadership of efforts with United States of America and the European Union.

These Foundational Requirements envision a nation-wide security solution for C-ITS, in the form of a national CCMS, to support deployments from day one, through to a mature, interconnected environment that interfaces with those around the globe.

They are intended to be a resource for those responsible for decision making and planning in this space, and to enable informed discussion and cooperation amongst Australian stakeholders.

There are 52 Foundational Requirements for a national CCMS, which can be classified into five broad, Principle Categorisations:

Table 1: Principle Categorisations for CCMS Requirements

	Principle Categorisation	Foundational Policy Explanation
1.	Confidentiality, Integrity and Availability	The CCMS shall provide Confidentiality, Integrity (encompassing authentication and non-repudiation) and Availability on an ongoing basis, as expected by the C-ITS and connected environment.
2.	Future Thinking	The CCMS shall be the initial and ongoing security product and enabler of national and international alignment and harmonisation for C-ITS.
3.	Flexibility and Interoperability	The CCMS shall ensure interoperability, and be communications agnostic, supporting the lifecycle of devices, and maximising safety and productivity afforded

		by critical messages.
4.	Smart Cities Scalability	The CCMS shall be highly scalable and flexible, supporting Australia's C-ITS needs for transport systems, across all levels of participation, that support devices in operation for at least 10 years.
5.	Management and Accountability	The CCMS Manager shall be accountable for the implementation, operation and maintenance of the CCMS.

PURPOSE OF THIS DOCUMENT

The purpose of this discussion paper goes beyond articulating the issues at hand, and presenting the requirements for a CCMS.

Rather, it is intended to set in motion a national discussion that will:

- *Build awareness* – that change is coming rapidly, and that action needs to be taken on issues that are not traditionally associated with the automotive and transport space, yet will soon be of central significance.
- *Stimulate debate* – amongst governments, industry, the public, and traditional and non-traditional stakeholders. The connected and cooperative environment will not arise spontaneously, and its development will not be led by a single organisation.
- *Generate consensus* – resolve differences of opinion, and synthesis disparate priorities into a manageable platform with clear goals and signposts to measure progress and success.
- *Establish a national vision* – formalise consensus into a shared, national vision; one that is as ambitious as it is practical.
- *Move forward* – implement the national vision: think big, start small, scale effectively.

TCA is seeking feedback on the discussion questions posed in this paper.

The discussion questions relate to the provision of security, and to the establishment of the connected environment.

Stakeholders are invited to send their submissions to **tca@tca.gov.au**

Contents

1 WHAT ARE COOPERATIVE INTELLIGENT TRANSPORT SYSTEMS (C-ITS)? 1

2 WHY SECURITY IS ESSENTIAL 2

2.1 The changing nature of security in the automotive world 2

2.2 The Internet of cars 2

2.3 Security is a task for governments, and an assumption for users 4

2.4 Safety and security are one and the same 4

2.5 Conclusion 5

3 SECURITY THAT IS AGNOSTIC, HARMONISED, ENABLES INTEROPERABILITY, AND SUPPORTS THE MARKET 6

3.1 Security that is agnostic 6

3.2 Security that enables interoperability 7

3.3 Security that is harmonised 7

3.4 Security that supports the market 8

3.5 Conclusion 8

4 SECURITY AS A MATTER OF POLICY: STATE AND TERRITORY, NATIONAL AND INTERNATIONAL 9

4.1 State and territory 9

4.2 National 9

4.3 International 10

4.4 Conclusion 11

5 AUSTRALIA AND THE INTERNATIONAL COMMUNITY ARE WORKING TOGETHER ON SECURITY 12

5.1 International Harmonisation Task Groups 12

5.2 Security policy through international collaboration 12

6 NECESSITY OF HARMONISATION FOR AUSTRALIA 13

7 THE C-ITS SECURITY SOLUTION: COOPERATIVE CREDENTIAL MANAGEMENT SYSTEM (CCMS) 14

7.1 What is a CCMS? 14

7.2 Establishing an entity responsible for providing security: CCMS Manager 14

7.3 Three pillars of security: Confidentiality, Integrity and Availability 15

7.4 Why we need to start talking about cryptography 16

7.5 Public Key Infrastructure (PKI) 17

7.5.1 How PKI works 18

7.5.2 Why the CCMS will use PKI 18

7.6 How does a CCMS provide security? 18

7.6.1 The CCMS manages digital certificates and misbehaviour 19

7.6.2 The CCMS provides lifecycle management 19

7.6.3 The CCMS provides assurance and access 19

7.6.4 Conclusion 19
8 CRITICAL LINKAGES TO OTHER DEVELOPMENTS IN THE CONNECTED AND COOPERATIVE SPACE 20
8.1 Internet of Things (IoT) 20
8.2 Automated vehicles 20
8.3 Smart Cities 21
9 AUSTRALIAN FOUNDATIONALREQUIREMENTS FOR A NATIONAL CCMS 23
9.1 General 23
9.2 Categorisations for CCMS Requirements 23
9.3 How to use these Foundational Requirements 24
9.4 Australian Foundational Requirements for a National Cooperative Credential Management System (CCMS) 27
9.4.1 Confidentiality, Integrity and Availability 27
9.4.2 Future Thinking 31
9.4.3 Flexibility and Interoperability 33
9.4.4 Smart Cities Scalability 35
9.4.5 Management and Accountability 38
10 FURTHER DISCUSSION QUESTIONS 42

FIGURES

Figure 1: C-ITS enabled vehicles and infrastructure require trust and security 3

TABLES

Table 1: Principle Categorisations for CCMS Requirements 3
Table 2: Principle Categorisations for CCMS Requirements 23

1 WHAT ARE COOPERATIVE INTELLIGENT TRANSPORT SYSTEMS (C-ITS)?

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

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-centre (V2C) connectivity – will see the progressive introduction of a 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.

AT A GLANCE...

Cooperative Intelligent Transport Systems (C-ITS) will transform vehicles, roads and cities, by having multiple devices communicate with one another.

2020 is the commonly expected horizon for deployment of C-ITS in the US and the EU, and Australia needs to keep up.

The connected environment – including vehicles – will be part cybernetic, part physical – it will be **cyberphysical**.

Like any built environment, connected cities will require **infrastructure** in the form of cyberphysical systems.

Like the cyberworld, connected cars will require **cybersecurity**.

The security solution that has achieved international consensus is the **Cooperative Credential Management System (CCMS)**.

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.

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

2 WHY SECURITY IS ESSENTIAL

The importance of security for C-ITS is neatly summarised in the European Union's *C-ITS Platform*: 'No security, no C-ITS.'[2]

The meaning of the term 'security' may seem commonsensical, but it differs depending on the area in which it is used. Security requirements in different areas may share common traits, but will also denote specific practices, expectations, assumptions and responsibilities.

An office may be accessible with a swipe card, and a house can be opened with a key, and both may have alarms. In this sense, they are similar. But, unlike a house, an office might be inaccessible after 6pm and on weekends – employees still have their 'key', but the key will only work at pre-established times. Similarly, at home, we can access all the files on our computer; at work, we may not be allowed to access the company accounts.

The meaning of security, and what it involves, both change over time.

2.1 The changing nature of security in the automotive world

Security in the automotive world has traditionally been associated with hardware (keys, remote central locking, alarms and immobilisers). Safety too has been primarily associated with hardware (airbags, anti-lock breaking systems etc.).

C-ITS will see cars becoming part of a connected, ICT environment – that is, a combination of hardware and software.[3]

Unlike the largely proprietary software currently used in the automotive industry, C-ITS will require high levels of interoperability and confidence in the content and security of messaging – this is especially important for safety-critical applications, such as crash-avoidance alerts.

C-ITS rely on the cooperative exchange of data. Users of C-ITS – or, more specifically, C-ITS devices themselves – are only able to work if they can trust the data they receive and, by the same token, the data they transmit can be trusted by others.

2.2 The Internet of cars

The provision of security for vehicles and other C-ITS devices is closely related to the cybersecurity policies, practices and technologies of ICT environments. For this and similar reasons, connected and cooperative vehicles, road networks and infrastructure have been popularly called the 'internet of cars.'[4]

---

[2] European Commission. 2016. *C-ITS Platform. Final Report*. Available at http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[3] This is accompanied by the need for new approaches to certification, signalled by the 'cheating software' used in a number of diesel cars, most notably by Volkswagen, that disguised vehicle non-compliance with emissions standards The Environmental Protection Agency are now moving to conduct on-the-road testing of diesel cars. See Environmental Protection Agency. 2015. EPA Update on Recent Volkswagen Announcement. Available at http://yosemite.epa.gov/opa/admpress.nsf/bd4379a92ceceeac8525735900400c27/6579a74e2ed0039185257ecb004f34cf!OpenDocument

[4]Koslowski, T. 2013. Forget the Internet of Things: Here Comes the 'Internet of Cars.' *Wired.* Available athttp://www.wired.com/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars/

Insufficient or compromised security in the ICT world has many serious consequences, such as loss of control and denial of access, and theft of personal or business information. When online banking, for example, compromised security can result in minor inconveniences (a temporary inability to access their online services) to major disruptions (identity or monetary theft).

Security is paramount for C-ITS because, unlike in the previous example, most users of C-ITS will be driving on the road. Insufficient or compromised security can range from a minor incident (temporary denial of non-essential service), compromised privacy (an intercepted payment for parking using C-ITS) to personal injury or life-threatening incidents (unreliable crash-avoidance or safety-critical communications, remote hacking, identify spoofing etc.).

It is only with security in place that a C-ITS environment can be considered reliable, resilient and trustworthy, and it is on this foundation that the benefits of C-ITS can be realised. How this trust can be established, though, is a significant challenge. It is also an opportunity for governments to make sure they get it right the first time.

Unlike data exchanges between known users, a C-ITS device will be constantly encountering – and exchanging data with – C-ITS devices with which it has no prior relationship: think of how many cars pass by when driving around an unfamiliar suburb, or even pulling out onto a busy road. In a C-ITS environment, these cars would need to trust each other – as would a car passing a piece of infrastructure, and vice versa (Figure 1).

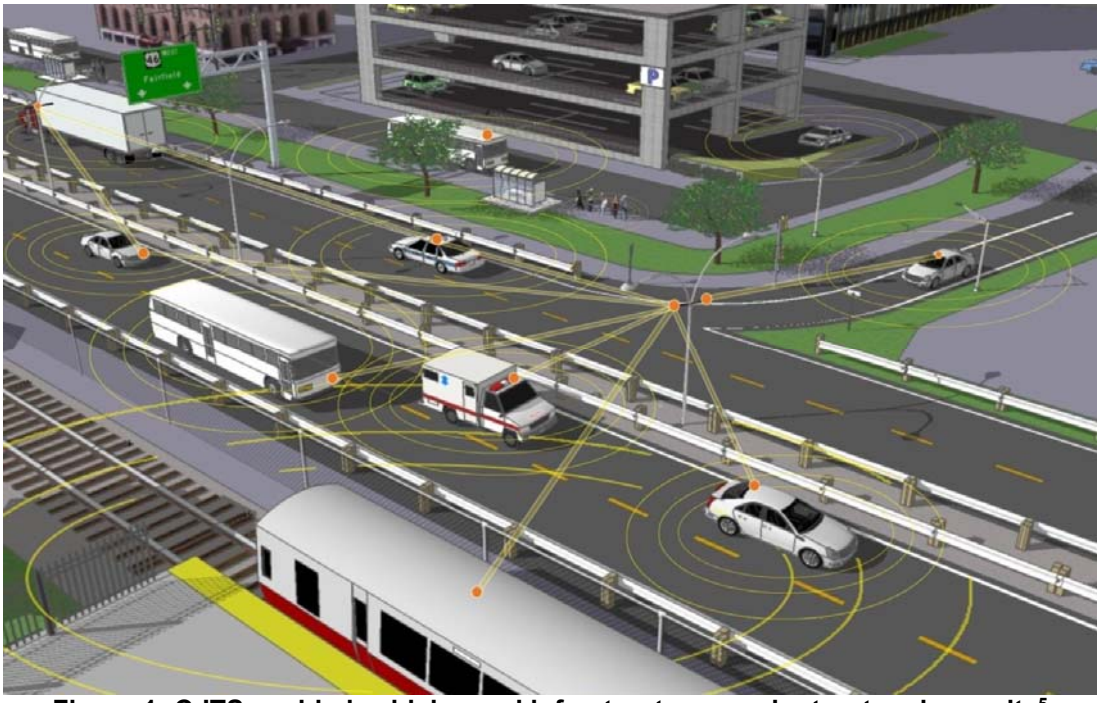

Figure 1: C-ITS enabled vehicles and infrastructure require trust and security[5]

[5] United States Department of Transportation. 2011. *V21 for Safety: Roadmap, Accomplishments & Constraints*. Available at http://www.its.dot.gov/presentations/pdf/L_V2I_Safety2011.pdf

2.3 Security is a task for governments, and an assumption for users

Security, as enabled by policy decisions, cryptographic protocols, the division of responsibilities, and the implementation of and conformance with standards, is the immediate and future task for governments and industry.

For consumers and users of C-ITS – people driving cars and using mobile phones – security is an *expectation* and, by default, an *assumption*.

While security is part of the planning and implementation of C-ITS deployments for governments and decision makers, consumers and users will 'assume the cyber security is perfectly adequate, much as they might expect their car to come equipped with airbags.'[6]

Like airbags, then, security is as much about the tailoring of traditional automotive and ICT goals (confidentiality, integrity, availability) for the connected and cooperative environment, as it is about safety. And, like airbags and seatbelts, security should be a universal feature rather than an added extra.

2.4 Safety and security are one and the same

In the automotive and transport world, emphasis has traditionally fallen on safety rather than security. This is now a false distinction: 'Transportation modes are now correlating security and safety; one can't have a safe system without it being a secure system.'[7]

A computer crash is very different from a car crash – but both can be caused by minimal lapses in security, and in the connected and cooperative world, safety is a direct outcome of security.

In the United States of America, the National Highway Traffic Safety Administration highlighted the importance of security for C-ITS, noting that: 'Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from malicious attacks, unauthorised access, damage, or anything else that might interfere with safety functions.'[8]

Safety is increasingly contingent on security processes. This point was made in a recent report released by the European Union Agency for Network and Information Security (ENISA), relating to the application of C-ITS to public transport: 'Cyber security and physical safety can no longer be treated as separate concerns: When attackers can affect the physical operation of ICT-enabled vehicles and other physical assets, network cyber security and physical safety become interdependent.'[9]

---

[6] Automotive World. 2016. *Special Report: Connected Cars*, p. 17. Available at http://www.automotiveworld.com/research/special-report-connected-cars/

[7] National Highway Traffic Safety Administration. 2014. *A Summary of Cybersecurity Best Practices*, p. 28. Available at http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity

[8] National Highway Traffic Safety Administration. 2015. NHTSA and Vehicle Cybersecurity. Available at http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity

[9] ENISA. 2015. *Cyber Security and Resilience of Intelligent Public Transport: Good practices and recommendations*, p. 19.Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/intelligent-public-transport/good-practices-recommendations.

2.5 Conclusion

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

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 technologies and management processes used in information communications technologies (ICT), and will be addressed further in this report.

Security that provides protection for communications, devices, and the overall environment is a common need in any C-ITS deployment.

This is signalled, first, by the internationally cooperative work being undertaken at Harmonisation Task Groups (HTGs), co-led by the European Commission, the United States Department of Transportation (USDOT), and TCA and; second, by the subsequent commitment by the European Commission and the USDOT to adopt the security solution that has emerged out of these HTGs – that is, the CCMS.[10]

The provision of security extends to a 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.

[10] HTG Reports relating to security are available at European Commission. 2015. Harmonized security policies for cooperative Intelligent Transport Systems create international benefits. https://ec.europa.eu/digital-agenda/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

SECURITY IS ALREADY AN ISSUE

In an incident widely reported in the media in July 2015, cybersecurity researchers demonstrated the ability to remotely hack into a Jeep via its online entertainment system.*

This is by no means an isolated example, as evidenced in the recent joint announcement by the Federal Bureau of Investigation (FBI) and National Highway Traffic Safety Administration (NHTSA).**

This was a controlled incident, but an eye opening one nonetheless. Technically, the security protocols were not C-ITS, but for the general public, undermining a connected vehicle's security undermines confidence and trust.

This is as much a technical issue as it is a policy and political one: security is already part of the public discussion – long before what governments and industry would consider "implementation" phases of cooperative and connected vehicles.

Governments need to send strong signals to industry and users that security is being handled from the outset.

*Australian Broadcasting Corporation. 2015. Australian motorists warned only a 'small hole' needed to access car's computer. Available at http://www.abc.net.au/news/2015-07-22/hackers-warn-smart-car-owners-of-potential-risks/6638784. For more on this matter and vehicle cybersecurity see Brown, D. (2016). *Responsibility for Vehicle Security and Driver Piracy in the Age of the Connected Car*. IDC. Available at http://www.veracode.com/sites/default/files/Resources/Whitepapers/idc-veracode-connected-car-research-whitepaper.pdf

**Federal Bureau of Investigation. 2016. Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits. Available at http://www.ic3.gov/media/2016/160317.aspx

3 SECURITY THAT IS AGNOSTIC, HARMONISED, ENABLES INTEROPERABILITY, AND SUPPORTS THE MARKET

3.1 Security that is agnostic

The C-ITS environment will be one based on fast, reliable, interoperable, secure and private communications between vehicles, infrastructure, mobile phones and other enabled devices.

The initial method of communication for C-ITS applications such as V2V and V2I will be dedicated short range communication (DSRC).

While this appears to be emerging as the primary – or at least initial – method of communications, it is important to note that C-ITS can use multiple wireless communications, including 3G, 4G (and beyond), Wi-Fi and Bluetooth etc.

Ensuring interoperability – the ability of one system to work with another – is key to realising the benefits and basic functioning of a C-ITS environment. It is therefore important that any piece of governing security infrastructure, including the CCMS, be communications 'agnostic', supporting any communications medium requiring it, and caters to innovation and evolution in communications technologies.

The ability to provide an agnostic, secure communications solution will be an important step in enabling a C-ITS environment that caters to the long-term needs of governments, industry and users.

3.2 Security that enables interoperability

Like security and safety, interoperability and security are overlapping concerns. It is especially important to mitigate against local solutions to what is a global challenge.

Connected vehicle technology is developing rapidly – far more rapidly than the development of the cyberphysical infrastructure needed to support this technology from a 'day 1' security perspective, and to foster a safe and secure, connected city – not to mention one that is operationally and commercially sustainable.

Providing security is an immediate and future task for governments and industry.

For consumers and users of C-ITS, security is an **expectation** and, by default, an **assumption**.

From a communications-operational perspective, without cooperation along these lines, it is entirely possible that 'drivers may end up in situations where they own vehicles they can't drive outside of their own State.'[11] From a security perspective, the critical task is to ensure the provision of a 'trust model' or 'trust network' – the ability for a device that is trusted in one area to be trusted in another (this could be a different state or a different country).

As mentioned above, the US and the EU have both committed to adopt the CCMS security infrastructure solution, which emerged out of the internationally collaborative efforts of HTGs. In Europe, this is likely to be called the E-SCMS (European C-ITS Security Credential Management System),[12] while the US will adopt the term SCMS, and prototypes have been developed in both regions.

These two types of CCMS have some important differences, mainly in the standards to which they adopt, and the architecture of the system.

3.3 Security that is harmonised

That the EU and US versions of the CCMS are somewhat different is not especially problematic. What is important, however, is *harmonisation*, which entails the common adoption or compatibility of key elements (be they technical, operational, policy, commercial or organisational) that enable interoperation and trust between different CCMSs and the C-ITS devices for which they provide oversight.

This holds true for Australia and, once again, here there are technical and organisational issues that hinge on policy decisions.

These can range from certificate policy (how digital certificates are structured), the non-duplication of identifiers (serial numbers that tell other C-ITS what application is being used, what services can be provided, and determine how they can be accessed quickly and easily) and

[11] Automotive World. 2016. *Special Report: Connected Cars*, p. 9. Available at http://www.automotiveworld.com/research/special-report-connected-cars/
[12] European Commission. 2016. *C-ITS Platform: Final Report*. Available at http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

having formal agreements between regions that allow the security management provided by one region to be trusted in another.

A lack of harmonisation and interoperability in this final scenario would be the digital equivalent of, for example, Victorian authorities not recognising a Queensland vehicle license plate, or arriving in a foreign country, only to have the validity of your passport rejected. Indeed, the security solution proposed for C-ITS will leverage the trust existing model upon which international passports are issued and trusted.

Each region will have its own version of a CCMS, but harmonisation ensures a cross-regional solution whereby, for example, a C-ITS enabled car under one CCMS can travel to a region with a different CCMS (be it national or international) and still have security (i.e. confidentiality, availability and integrity) provided and, where available, make use of the same applications.

3.4 Security that supports the market

Security is one of the fundamental ways different regions establish and communicate their trust in each other's systems and devices. This is essential for establishing a commercially sustainable global market for C-ITS.

For the private sector, standards harmonisation facilitates the ability of industry to make their products internationally availability, with only minimal changes – reducing development costs, and costs for end users.

> **"Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this."**
>
> Australian Cyber Security Centre Threat Report, 2015, p. 2

Fostering interoperability ensures a common approach, which promotes effectiveness of systems; and a common approach across the market promotes efficiency.

For application developers, standards serve as a quality control mechanism and a barrier to entry into the C-ITS market. Common, harmonised standards make this process easier, and encourage investment and participation.

Importantly, the cooperative and connected environment, inclusive of automated vehicles, smart cities and the Internet of Things, will give rise to new business models – models that are yet to be invented.

The task for governments is to implement policies and policy settings that enable the levels of trust that will underpin this new business environment.

3.5 Conclusion

The goal is a C-ITS environment that works safely, securely and seamlessly.

For the market, users and those responsible for oversight, security promotes cost effectiveness, efficiency, assurance.

Harmonisation fosters and maintains trust, ensuring that not only are the levels of security assurance achieved, but that they are achieved in a manner that ensures existing and new systems and devices continue to provide confidence to all users.

4 SECURITY AS A MATTER OF POLICY: STATE AND TERRITORY, NATIONAL AND INTERNATIONAL

Ensuring security for C-ITS will be an outcome of implementing the right policies, plans and practices. It is therefore important that steps are taken to align with and bolster the immediate plans and future vision for our transport networks and cities.

This matter spans state and territory, national and international policy platforms.

4.1 State and territory

By investing in new projects or modifying existing infrastructure, Australian Governments and Road Authorities are using telematics, ITS and related intelligent technologies to harness data, deliver real time information, and achieve safety, productivity and environmental outcomes.

Through ITS, managed motorways are being used to reduce stop-start travel, and make travel times more predictable. In Melbourne, for example, the Monash Freeway uses managed motorway technology to reduce travel times and greenhouse gas emissions by 42% and 11% respectively, and saves $2 million per day by cutting travel time and delays.[13]

In their strategic planning, governments are looking ahead to how these technologies will enable smarter, safer, and more connected cities driven by integrated transport.

As States and Territories implement their own strategic plans, it is important that they simultaneously advance an overarching vision for Australia's transport, infrastructure, and cities.

4.2 National

Since 2012, Australia's adoption and advancement of ITS has been formalised and guided by the *Policy Framework for Intelligent Transport Systems in Australia*. The Framework's objectives are to:

- guide the consistent implementation, integration and uptake of ITS nationally across all land transport modes
- promote innovation and competition through interoperable and, where possible, open access and open architecture ITS solutions
- provide standardisation for important national and interdependent supplier/provider systems
- facilitate the efficient and rapid uptake of ITS that meet consumer demands, driven by the perceived usefulness and benefits of the technology.

Security and its linkages with privacy is also identified as a key issue in the Framework, which highlights the need to adopt security as an initial consideration: 'Privacy and risk management issues should be addressed at the design stage for ITS projects and security measures should

[13] Standing Committee on Infrastructure, Transport and Cities. 2016. *Smart ICT: Report on the inquiry into the role of smart ICT in the design and planning of infrastructure*. Commonwealth of Australia, Canberra, p. 34

also be considered to prevent modification, misuse or disclosure of private-personal information.'[14]

Telematics and ITS are now part of Australia's long term infrastructure, regional and metropolitan planning.

The *Australian Infrastructure Plan* highlights the ability of ITS to triple asset utilisation, and to enable better management of infrastructure, vehicles and new ways of generating, collecting, sharing and analysing data to help guide investment.[15]

Smart Technology is one of three pillars in the Commonwealth's *Smart Cities Plan,* in part a response to the *Australian Infrastructure Plan*, which highlights their potential to improve the efficiency, sustainability and services of infrastructure networks.[16]

Security is key to realising this national vision, as is alignment with international developments – indeed, these two go hand-in-hand.

Australia's Cyber Security Strategy identifies the necessity of global linkages, and points to connected vehicles as precursors to the 'internet of everything.' The Strategy uses the hacking of connected vehicles as an example of the security threats and vulnerabilities to which newly-connected devices are exposed.

The Strategy pinpoints security as an enabler of innovation, growth and prosperity[17] – aims shared by the implementation of security for C-ITS.

TELEMATICS refers to integrated systems of information, communications and sensors to exchange data and information between vehicles and other locations, including:

- Vehicle to infrastructure (V2I) applications
- Vehicle to vehicle (V2V) applications
- Vehicle to elsewhere (V2X) applications.

The application of telematics and related intelligent technologies is increasingly being used across surface-based transport to improve the mobility of people and freight by improving safety, productivity and efficiency outcomes. This includes those outcomes that facilitate:

- Monitoring and reporting of vehicles and infrastructure
- Providing information to and from vehicles
- Connected and cooperative vehicles
- Automated and autonomous vehicles.

4.3 International

The interrelated nature and importance of security and international alignment has been well known in the ITS space for some time now. In their examination of the policy issues surrounding C-ITS, Austroads – the association of Australasian road transport and traffic agencies – have noted that 'overseas experience demonstrates that privacy and security are issues that need to be addressed from an early stage in the design, development and regulation of cooperative ITS applications.'[18]

[14] Standing Council on Transport and Infrastructure. 2012. *Policy Framework for Intelligent Transport Systems in Australia* (Cth).
[15] Infrastructure Australia. 2016. *Australian Infrastructure Plan: Priorities and reforms for our nation's future*. Australian Government, p. 7. Available at http://infrastructureaustralia.gov.au/policy-publications/publications/files/Australian_Infrastructure_Plan.pdf
[16] Department of the Prime Minister and Cabinet. 2016. *Smart Cities Plan*. Commonwealth of Australia, p. Available at https://cities.dpmc.gov.au/smart-cities-plan
[17] Department of the Prime Minister and Cabinet. 2016. *Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity.* Australian Government, p. 18. Available at https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
[18] Austroads. 2011. *Examination of Major Policy Issues Relating to Introduction of Cooperative ITS in Australia*. Sydney, Australia. p. vi.

Incorporating this security recommendation and others, the *Policy Framework for ITS in Australia* highlights the necessity if Australia's strategic international alignment, noting that 'as a relatively small player in the global ITS space, it will be essential for the Australian [ITS] architecture to be consistent with global developments.'[19]

In 2013, the then Standing Council on Transport and Infrastructure approved the National Transport Commission's policy findings and recommendations pertaining to Australia aiming for the 'highest level of privacy protection in the standards set for C-ITS safety systems ... in keeping with international standards' and that Australian governments 'seek the highest possible level of anonymity' for drivers.[20]

These matters recently came to the fore with release of *Smart ICT: Report on the inquiry into the role of smart ICT in the design and planning of infrastructure*, prepared by the Standing Committee on Infrastructure, Transport and Cities. The report acknowledges that the collection and management of data is the key to the development of smart infrastructure.

Numerous government and industry submissions identified security as prominent issue, including instances of vulnerabilities in cryptography and the use and management of digital certificates. As one submission put it, 'as cars get "smarter" (meaning more digital and more connected), they are also at greater risk.'

Critically, the report highlights TCA's role in this space, drawing attention to its cooperative involvement with the European Commission and the United States Department of Transportation on Harmonisation Task Groups (see below), and to its administration of telematics and ITS applications of the *National Telematics Framework* – namely the Intelligence Access Program (IAP) and On-Board Mass (OBM) monitoring – both of which enable better management of the road network, and are underpinned by strong security assurances.[21]

4.4 Conclusion

Aligning, harmonising and bolstering these policy platforms – state and territory, national and international – will be a significant task for all stakeholders. But it is a necessary task.

Where it is not mentioned explicitly, security is one of the fundamentals we assume when we envision the connected vehicle environment, one with roads and cities that are safer, smarter, and more efficient and environmentally friendly – and, above all, one that puts people first.

[19] Standing Council on Transport and Infrastructure. 2012. *Policy Framework for Intelligent Transport Systems in Australia* (Cth), p. 9.
[20] National Transport Commission. 2013. *Cooperative Intelligent Transport Systems: Final policy paper*. Melbourne, Australia.
[21] Standing Committee on Infrastructure, Transport and Cities. 2016. *Smart ICT: Report on the inquiry into the role of smart ICT in the design and planning of infrastructure*. Commonwealth of Australia, Canberra, p. 43, 97 & 127-8.

5 AUSTRALIA AND THE INTERNATIONAL COMMUNITY ARE WORKING TOGETHER ON SECURITY

Our roads and cities do not exist in isolation. They are part of a network of connected systems – interstate, inter-regional, global and cooperative – on and off the road.

5.1 International Harmonisation Task Groups

Developing the security solution for C-ITS has been one of the critical outcomes of international Harmonisation Task Groups (HTGs).

Harmonisation refers to the coordination of safety and sustainability issues, technical and policy standards, and the identification and removal of regional and international differences that potentially limit the public outcomes of C-ITS.

Harmonisation efforts aim 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.

Established in 2011 by the European Commission and the United States Department of Transportation (USDOT), the HTG initiative recognises that C-ITS is a global phenomenon which requires global cooperation, and efforts should be taken to prevent national – and indeed local – solutions to issues of international importance.[22]

HTGs bring together and draw on the expertise of vehicle and equipment manufacturers, technical standards development organisations, and government bodies.

The work is carried out by seven distinct, yet overlapping, HTGs, each of which focuses on different aspects of the C-ITS environment that could benefit from harmonisation, including safety, sustainability, security, communications, infrastructure and standards – areas that are not primarily commercial in nature, but deliver public purpose outcomes while enabling the market to develop.

5.2 Security policy through international collaboration

TCA has co-led two HTGs – HTG6 and 7 – both of which comprise policy analysts and technical experts with hands-on experience in C-ITS implementation, and security in related fields.[23]

The outcomes of these HTGs are intended to be used by policy makers and implementers, and address and anticipate the current and future challenges of privacy protection, regional differences, and the flexibility and integrity of security systems.

[22] This followed the signing of a Joint Declaration of Intent on Research Cooperation in Cooperative Systems in 2009. See European Commission. 2011. *The EU-US Cooperative Systems Standards Harmonisation Action Plan (HAP)*. Available at http://ec.europa.eu/digital-agenda/en/news/june-2011-eu-us-cooperative-systems-standards-harmonisation-action-plan-hap

[23] For TCA's report on HTG6 see Transport Certification Australia. 2015. *Cooperative Intelligent Transport Systems (C-ITS) – International Harmonisation Task Group Number 6. Findings and Recommendations*. Available at www.tca.gov.au

HTG6's objective was to develop an end-to-end security policy framework for C-ITS that identifies the key areas for harmonisation across jurisdictional boundaries. The principal outcome was the development of the CCMS, currently being adopted by both America and the European Union, and described in more detail below.[24]

Since commencing with HTG6 in 2014, international cooperation has achieved a number of significant technical and policy benefits.[25] The combined efforts of HTG6 has led to a consistent set of recommendations on security for vehicles employing C-ITS that has been achieved with a far lower investment by participating countries than would have otherwise been required. Harmonisation of security has also ensured greater consistency for those developing in-vehicle technologies, and simultaneously reduced development costs, which would have been greater without coordinated harmonisation efforts.

Currently underway, the broad objectives of HTG7 are to consolidate and expand the security-related work of HTG6, perform gap analysis and standards selection, create a national solution to the management of services related to C-ITS applications, and bring the HTG work to bear on automated vehicles and Smart Cities initiatives.

6 NECESSITY OF HARMONISATION FOR AUSTRALIA

Australia has its own unique interests in the global harmonisation of C-ITS. It has a relatively small new vehicle market that sources new vehicles from around the globe. With major vehicle manufacturers expected to launch vehicles equipped with C-ITS over the next 12 months, it is crucial that Australia is prepared to respond to – and benefit from – what will be a major shift in the automotive world. This includes identifying and removing barriers that risk compromising an efficient, effective and secure C-ITS environment.

Australia has the opportunity both to learn from and influence international advancements in and implementations of C-ITS. Advancements in the United States and Europe have been achieved through collaboration and strategic partnerships across government and industry. Coordinated research and action supports and accelerates the deployment and adoption of C-ITS, mitigates against needless overlaps and the adoption of redundant standards, and identifies security outcomes that are national advantageous, yet international in scope.

Involvement in international C-ITS activities is important due to Australia's limited market influence on vehicle manufacturing. It is critical that Australia take steps to align itself with, and strategically contribute to, the development of the global C-ITS agenda. Australia's demonstrated track record in transport system innovation – from enabling third generation heavy vehicle access, to alcohol interlocks and taxi and hire car systems – increases the potential for Australian transport system stakeholders to play a strong role in the international C-ITS environment as it develops, and to work with companies working on C-ITS and autonomous and automated vehicles.

[24] HTG6 drew on the work of previous HTGs, including work on security and communication standards performed by HTG1 and HTG3 respectively; the work of HTG2, which focussed on cooperative and safety messages harmonisation; and the work of HTGs 4 and 5, which focused on infrastructure messaging standards.

[25] European Commission. 2015. Harmonized security policies for cooperative Intelligent Transport Systems create international benefits. https://ec.europa.eu/digital-agenda/en/news/harmonized-security-policies-cooperative-intelligent-transport-systems-create-international.

7 THE C-ITS SECURITY SOLUTION: COOPERATIVE CREDENTIAL MANAGEMENT SYSTEM (CCMS)

7.1 What is a CCMS?

The security solution being adopted by the EU and the US for C-ITS is generically referred to as a Cooperative Credential Management System (CCMS). The CCMS provides security for the C-ITS environment and for C-ITS devices.

A CCMS is both an institutional framework and a piece of infrastructure, encompassing human/management, electronic and physical elements –it is 'cyberphysical.' 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.

A CCMS is a distributed system – that is, it comprises multiple roles and functions, both computational and organisational/institutional.

When C-ITS share information – be it vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) or vehicle-to-elsewhere (V2X) – it appears as though one C-ITS device is transmitting and receiving information from another C-ITS device; in fact, there are a number of addition entities and processes involved, and those communications are part of a digital certificate, and are encrypted and decrypted to guarantee privacy and authenticity via Public Key Infrastructure (PKI) (see below).

A CCMS is based on PKI, which consists of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of sensitive data.

The CCMS provides C-ITS with security, interoperability and privacy across different communications mediums and different devices. Its implementation is communications agnostic, and can therefore support a wide variety of communications technologies.

7.2 Establishing an entity responsible for providing security: CCMS Manager

While a CCMS is composed of a variety of roles, responsibilities and functions, there needs to be an entity responsible for providing a high level of ongoing security for the C-ITS environment. The generic term for this entity is the CCMS Manager, who provides security services that underpin and protect the operation of C-ITS devices and the C-ITS environment.

The CCMS Manager is responsible for the development of processes, procedures, standards and certification for the CCMS. Some functions of the CCMS are intrinsically the responsibility of the CCMS Manager while other functions are the responsibility of the operator of the C-ITS device.

The CCMS Manager provides administration and system management, including certification and audit (Misbehaviour management), of the CCMS. The CCMS periodically issues new digital certificates to the various devices operating in the C-ITS environment as a safeguard to ensure that the rules that underpin its integrity are maintained. Devices that are identified as misbehaving, or as posing a safety and security threat to the C-ITS environment, are not supplied with new digital certificates, and are unable to participate in certain applications, or in the environment altogether, depending on the risk they pose.

Assurance of compliance with technical standards and policies by entities wishing to operate functions within the CCMS will be administered by the CCMS Manager.

Given its importance, it is expected the CCMS Manager will play an active role in the maintenance and ongoing development of security for the CCMS and, by extension, the C-ITS environment. The C-ITS environment, which is made possible by the issuing (and, where necessary, revocation) of digital certificates, is one that requires the utmost levels of integrity and confidentiality.

The consequences of mishandling digital certificates and breaches in security are potentially very dangerous, and the CCMS Manager will need to monitor and actively engage on complex technical and policy issues. Recent publically reported examples illustrate the importance of this role: both Microsoft and Google have experienced security breaches relating to the improper issuing of digital certificates, which could have been used by attackers to impersonate trusted parties.[26]

Eventually, the CCMS Manager will need to coordinate with other CCMS Managers particularly where interoperability and trust is required. Without a relationship between CCMS Managers, a C-ITS device has the potential to misbehave when it is “away from home” and this can be difficult to manage without visibility of its full area of operation.

7.3 Three pillars of security: Confidentiality, Integrity and Availability[27]

A CCMS has two distinct, yet overlapping high-level requirements. First, it will need to authenticate thousands of data exchanges simultaneously and in real time, ensuring that exchanges, such as alerts and warnings, received by one C-ITS device can be trusted by another, even when these C-ITS device have no previous relationship.

This is especially important for key, safety-critical applications – a warning about an impending crash hazard that does not work in real-time is useless; a ‘fake’ warning is potentially just as dangerous as receiving no warning at all.

Second, in addition to providing trusted data exchanges, a CCMS will need to provide protection for the overall C-ITS environment, inclusive of devices and its structure.

A CCMS is a cyberphysical system that establishes and maintains trust amongst users in a communications network by providing the three pillars of ICT security, tailored for the connected, C-ITS environment: Confidentiality, Integrity (including non-repudiation) and Availability.

These terms are commonly used to describe cybersecurity objectives relating to information, but they can be understood in more familiar scenarios.

[26] Broersma, M. 2015. Google Warns Of Unauthorised Security Certificates in Latest Breach. Available at http://www.techweekeurope.co.uk/security/google-certificates-breach-164993

[27] Cybersecurity in general refers to ‘methods of using people, process, and technology to prevent, detect, and recover from damage to confidentiality, integrity and availability of information in cyberspace’. Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J, & Weiss, J. 2012. *Cyber Security Policy Guidebook*. Hokoken: Wiley, p. 3. Although there are other ways of presenting the objectives of cybersecurity, Confidentiality, Integrity (including non-repudiated) and Availability is the widely accepted triad and industry/government standard. See, for example, National Institute of Standards and Technology (NISTA). 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

To return to the example used earlier in this paper, an office is accessible by a swipe card. The swipe card works like the key to a house, but unlike a house key, it may not work afterhours and on weekends. In this scenario:

- ***Confidentiality* relates to limiting use of a service to authorised parties** – at all times, the swipe card to your office will not grant you access to my office, and vice versa. I may or may not be allowed to access my office on Saturday.

- ***Integrity* (encompassing non-repudiation) refers to the ability to preserve authenticity and accuracy** – my swipe card is unique and assigned to me alone. If I am allowed to use my swipe card to access the office on weekends, a record will be created by the system whenever I use this access. If valuables go missing from the office over the weekend, and no one else accessed the office, I may have some explaining to do – I cannot deny (repudiate) that my swipe card was used on that day and at that time.

- ***Availability* refers to the timely use and capability of a service –** when I use my swipe card, it works immediately, not an hour later, and the correct door opens. If I report that my swipe card has been lost or stolen, the card will be cancelled, and will no longer grant me (or the person who found or stole it) access the office at all.

THREE PILLARS OF SECURITY

Confidentiality– ensuring only those authorised can access and disclose information, ensuring privacy.

Integrity (encompassing authentication and non-repudiation) – ensuring only messages from authorised, reputable sources are acted on, that they arrive in-tact; and participants cannot deny originating or signing these messages.

Availability– ensuring information – and the system that underpins the information – is available and accessible in a timely fashion, avoiding disruptions and delays.

7.4 Why we need to start talking about cryptography

What does it mean when we are informed that, for the connected vehicle environment, we need to get 'used to setting up secure networks and sending encrypted messages as the default'?[28]

In short, it means that we need to implement the same – and in some cases greater – levels of privacy, security and assurance that are taken for granted in other facets of our digital lives. Lapses in digital security may be technical, organisational, or the result of human error, but they invariably affect people.

Cryptography is not traditionally associated with the automotive world. This has changed, as it is converging with the digital sphere. Cryptography is now the norm.

[28] National ITS Architecture Team. 2015. A Primer on the Connected Vehicle Environment. *Connected Vehicle Reference Implementation Architecture*, p. 6. Available at http://www.iteris.com/cvria/docs/primerconnectedvehicleenvironment.pdf

7.5 Public Key Infrastructure (PKI)

A CCMS is based on PKI, and this section provides an introduction to the basic concept and benefits of leveraging PKI for C-ITS security.

PKI consists of cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of sensitive data. PKI is used to confirm the identity 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.

KEY TERMS

Cryptography – 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'.

Confidentiality, Integrity, Availability – the three pillars of security.

Interoperability – the ability of one system to work with another.

Harmonisation – the common adoption or compatibility of elements (technical, operational, policy commercial, organisational) that enable interoperation of, and trust between, different systems and devices.

Public Key Infrastructure – cryptographic technologies, standards, organisational and policy controls and procedures to provide security for exchanges of sensitive data.

Digital certificate – an electronic 'passport' that contains the cryptographic keys used to encrypt and decrypt messages, ensuring users can trust messages from other users.

A CCMS based on PKI has been identified as the security infrastructure for C-ITS for a number of reasons, chiefly:

- It is a well-established method of providing cryptographic security
- It can support a very large environment
- It can be extended and adapted, and therefore has longevity
- It offers legacy support for the detection and usability of older devices and software, and
- It is cryptographically versatile enough to accommodate needs as they differ across different regions.

While a CCMS will adopt the fundamental principles of PKI, it will be specific to C-ITS. Some aspects of PKI will need to be refined because, for example, the C-ITS environment will require very low latency communications i.e. the time taken between one C-ITS device encrypting and sending a message, and another C-ITS device receiving and decrypting the message.

A PKI scheme underpins the CCMS to achieve the security goals related to establishing trust among users – a critical requirement to enable vehicles and infrastructure to trust information

being exchanged in an environment where there is no previous relationship between the C-ITS devices.

7.5.1 How PKI works

The use of PKI involves the creation and management of digital certificates that certify the source of messages, which enables users to trust one another and the system as a whole.

PKI uses cryptography to provide authentication, integrity and confidentiality when sending messages between different users. In symmetric cryptography, two users have identical keys. One user uses their copy of the key to encrypt a message; the other uses their copy of the key to decrypt the message. As long as there are only two keys and they are kept private, the users can communicate securely.

PKI, however, uses asymmetric cryptography, and there are two types of keys – public keys and private keys. Public keys are more widely available to other users, while private keys are unique to a single user. The keys are different, but if a public key can be used to decrypt a message, then it is confirmation that the private key was used to encrypt it (and vice versa).

This is known as a key pair: the two keys are mathematically linked in such a way that what is encrypted by one key can be decrypted by the other. Although the keys are mathematically linked, it is extremely difficult to derive one key based on knowledge of the other. When asymmetric cryptography is used, PKI provides the assurance that the public key is valid by putting the public key in a digital certificate signed by the private key.

7.5.2 Why the CCMS will use PKI

By leveraging PKI in this way, a sender and a receiver (i.e. two C-ITS devices) do not need to have any prior interaction to securely send and receive messages and trust that the messages are authentic.

The rational for this is quite simple when one considers all the vehicles that have never shared a road before, or travelling to a new destination with unfamiliar infrastructure – all of these would involve C-ITS devices needing to exchange secure messages; they have no prior relationship, but they are able to trust each other because of PKI.

The ability to trust other C-ITS devices, while simultaneously enabling privacy through anonymity, is the unique security feature of the way PKI has been designed for use in a C-ITS environment.

This is a simple explanation and, in fact, describes the minimum functionality of PKI. Greater privacy can be enabled through the additional cryptographic processes, and PKI is able to support this, as and when required by the C-ITS application.

7.6 How does a CCMS provide security?

Cryptographic key pairs are indispensible, but the real common currency of the connected, C-ITS environment is digital certificates, into which public and private keys are placed and then circulated.

It will not be apparent to the majority of users, but the CCMS enables and performs tasks that users will expect to occur for C-ITS to work from day one. It is the CCMS that ensures that user information is kept private, and that the information being used in C-ITS has integrity.

7.6.1 The CCMS manages digital certificates and misbehaviour

The roles and functions of a CCMS essentially revolve around the generation, installation, revocation and management of digital certificates. A C-ITS device will have different types of certificates for different purposes, some of them valid for long periods of time, others are highly disposable and in frequent need of renewal.

Digital certificates, which are originally installed in or requested by devices, need to be issued by a trusted party. A C-ITS device that poses a threat to other users and the connected environment needs to be able to be identified and, possibly, have their certificates revoked. This is called Misbehaviour Management.

7.6.2 The CCMS provides lifecycle management

The ability of the CCMS to provide security, from when a C-ITS device enters (or 'enrols' in) the environment (as a new vehicle, for instance), to when it leaves (and can no longer interact with any other C-ITS devices) is called 'lifecycle' management.

The ability of the CCMS to do this must take into account that the environment will include both old and new devices; and that C-ITS devices will travel between security domains i.e. between CCMSs. Harmonisation and interoperability between CCMSs is therefore essential.

This capability also means that the CCMS has a key role in managing cybersecurity, and deterring and preventing hackers and other malicious behaviour.

7.6.3 The CCMS provides assurance and access

The CCMS is a means to ensure that only those vehicles, infrastructure and devices that are authorised and meet the required standards can participate in the C-ITS environment.

Importantly, the CCMS manages the applications in which a vehicle or C-ITS enabled piece of infrastructure can participate. Much like how a company allows its staff to access certain systems and applications in its IT environment (a manager may have full access to a server, whereas an officer may only be able to access certain folders) the CCMS manages authorisation to use a C-ITS application.

This functionality is important, for example, when determining whether an emergency vehicle such as a fire truck can interact with traffic lights to receive prioritisation.

7.6.4 Conclusion

The CCMS is a secure, trustworthy and reliable piece of cyberphysical infrastructure that 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.

8 CRITICAL LINKAGES TO OTHER DEVELOPMENTS IN THE CONNECTED AND COOPERATIVE SPACE

The linkages to other developments, and the centrality of the establishment of security for C-ITS, were identified in Section 5 of this discussion paper. This section will briefly expand on some of the more prominent developments in the connected and cooperative space.

8.1 Internet of Things (IoT)

C-ITS and the connected and cooperative vehicle and transport network will come to be seen as some of the boldest steps towards the Internet of Things (IoT) – the incalculably vast network of uniquely identifiable objects that can communicate with one another, at home, at work, while commuting, and facilitating seamless transitions in-between.

The challenges that will arise along the way to the IoT are those that are currently being addressed in the C-ITS space – those of harmonisation, interoperability, inter-regional cooperation and, linking all of these together, security.

The Internet provides a useful comparison for these security concerns, because it is a powerful example of a system in which trust between users and devices can be compromised. Furthermore, it illustrates the costs and challenges of building security measures into a system once it is established.

The Internet is a diverse ecosystem that has grown over time, supports an almost infinite number of applications, and is spread across the globe. Many of the Internet's core elements however, were never intended to support such an environment. Internet Protocol (IP) addressing is one example: when IPv4 could no longer support the number of connected devices, IPv6 was introduced.

Furthermore, as the USDOT have noted of the IoT: 'Given the number of potentially vulnerable connected devices, the most significant risks are expected to emerge around issues of security, privacy, and governance [...] The view appears to be widely held that the approach used to develop the Internet thus far will not provide the level of security and resilience needed in a world of billions of connected machines and sensors.'[29]

The extent to which the Internet has had to accommodate changes like this is an important lesson that should inform the development of extensible, agnostic security for C-TIS and the connected and cooperative environment, because applications will arise that were not and, indeed, cannot be anticipated.

8.2 Automated vehicles

Eventually, there will be *convergence*, and connected and automated vehicles, pedestrians, motor bikes and bicycles will interact and interconnect to achieve greater safety, and after-market products will reach the market quickly once the opportunity is known to and understood by the private sector.

[29] United States Department of Transportation. 2015. *2015 OST-R Transportation Technology Scan: A Look Ahead.* Available at http://www.rita.dot.gov/sites/default/files/technology_scan.pdf

An automated vehicle can perform safety-critical (such as braking and steering) functions without driver input, and C-ITS standards, infrastructure and connectivity will realise their full potential.[30] It has been widely recognised that automated vehicles will require C-ITS to enhance situational awareness where localised vehicle sensors cannot "see" such as around blind corners.

The standards selection and identification of gaps for C-ITS occurring nationally and internationally will support emerging connected automated vehicle deployments.

Connectivity – and the standards that enable it – will be especially important for communication between vehicles and infrastructure when the former are operating in automated mode, and need to be receptive to messages from road infrastructure.

To receive these messages, the automated vehicle would need to have connectivity enabled – be it via Dedicated Short Range Communications (DSRC) on the 5.9GHz band, 3G and 4G, Wi-Fi and Bluetooth – used by C-ITS devices when they communicate with one another and with infrastructure.

While automated and autonomous vehicles can operate in a limited manner on some current road infrastructure, connectivity and C-IT is considered an important element needed for their success and ability to operate across the wider road network under more varied operational conditions.

While automation can see with direct line of sight, connectivity provides the means to communicate between vehicles that are beyond its visibility. Somewhat like telepathy, connectivity provides the ability for vehicles to proactively interact together rather than simply trying to anticipate what the other vehicle might be about to do which passive sensors currently achieve.

C-ITS connectivity provides infrastructure communications which ensures infrastructure changes – both temporary and permanent – can be communicated to vehicles. The benefit of being able to communicate between vehicles that are not visible to one another is considered critical in achieving reliable automation and autonomy.

In March 2016, it was widely reported that one of Google's autonomous vehicles had experienced its first accident not caused by a human driver, when it crashed into a bus. This event highlights the importance of C-ITS for automated vehicles is now being reported in mainstream media, including *Forbes*.[31]It is probable that C-ITS communications would have avoided the incident. The Google car crashed at a low speed, but as automation reaches new milestones, speed will become a growing safety issue that could be addressed by C-ITS standards.

8.3 Smart Cities

Similar to automated vehicles, C-ITS have immediate and future relevance and use for "Smart Cities" initiatives, which are already underway in Europe and the USA – especially C-ITS applications that interact between the transport network and city infrastructure.

The USA has established a number of "Smart Cities" initiatives with a significant one being the New York project that will connect up to 10,000 vehicles with the New York City road

[30] There are five different levels of vehicle automation, ranging from partial to full automation. See National Transport Commission. 2016. *Regulatory options for automated vehicles.* Available at http://www.ntc.gov.au/Media/Reports/(80E9EBF1-53F0-44F7-96CF-07D60A324122).pdf

[31]Abuelsamid, S. 2016. "The First Google Self-Driving Car Accident Makes The Case for V2V Communications. *Forbes*, 7 March 2016. Available at http://www.forbes.com/sites/samabuelsamid/2016/03/07/the-first-google-self-driving-car-accident-makes-the-case-for-v2v-communications/#3a15bde569ce

management system. Europe is also undertaking a large number of diverse Smart Cities initiatives.

The currency of existing ITS and C-ITS applications, and TCA's involvement, was signalled in the Commonwealth's *Smart ICT: Report on the inquiry into the role of smart ICT in the design and planning of infrastructure.* The report cites role and importance of C-ITS in these initiatives, and draws attention to TCA's administration of the IAP and OBM, the importance of data security, and the work being performed by TCA as an HTG co-leader.

Many of the systems and cyberphysical infrastructure that will enable C-ITS, and will either be part of, or interact with the CCMS, will be common to, or can be leveraged by, Smart Cities.

Looking ahead, the ability to consolidate these systems and infrastructures into 'one stop shops' will be especially useful for application developers, supporting the global market.

Incorporating the Australian ITS Architecture into international C-ITS architectures to identify interface and associated standards includes many of the systems and interfaces that enable interaction with city infrastructure.

The ongoing work in C-ITS standards includes many of the systems and interfaces – such as traveller information, public transport and traffic management and emergency services – that will enable communications between users, devices, infrastructure and back offices envision by Smart Cities initiatives.

As the Smart Cities initiatives continue to be defined, those in the national and international security and harmonisation space will be engaging with Standards Development Organisations common both to C-ITS and Smart Cities, a great many of which overlap.

9 AUSTRALIAN FOUNDATIONALREQUIREMENTS FOR A NATIONAL CCMS

9.1 General

Each region will have their own regional adaptation, in the form of requirements for a CCMS. Importantly, a region's adaptation and implementation of a CCMS need not be exactly the same as that of another region. Rather, it needs to be harmonised to the extent that it provides interregional security, and is interoperable with other CCMSs.

Critically, to be harmonised does not require identical security solutions. Instead, systems can use common technical or even slightly incompatible approaches as long as there is coordination on a policy level regarding exactly what criteria are used to determine that a system is trustworthy.

TCA has, as part of its international harmonisation role, taken the HTG6 work and HTG7 input, and synthesised them with other relevant sources, including material from the National Transport Commission, Austroads, Commonwealth Department of Finance and the US National Highway Traffic Safety Administration.

This has resulted in the development of a tailored set of Foundational Requirements for a National CCMS for Australia.

These Foundational Requirements envision a nation-wide security solution for C-ITS, in the form of a national CCMS, to support deployments from day one, through to a mature, interconnected environment which interfaces with those around the globe.

These Foundational Requirements satisfy the immediate and future needs of a national C-ITS deployment. A requirement may be required for deployment from 'day 1' or can undergo a 'phased approach' – that is, it can implemented over time, providing that consideration is given to it from the outset.

9.2 Categorisations for CCMS Requirements

For the benefit of policy and decision makers, TCA has categorised the 52 Foundational Requirements for a National CCMS into five categorisations, laid out in Table 2.

Table 2: Principle Categorisations for CCMS Requirements

	Principle Categorisation	Foundational Explanation
1.	Confidentiality, Integrity and Availability	The CCMS shall provide Confidentiality, Integrity (encompassing authentication and non-repudiation) and Availability on an ongoing basis, as demanded by the C-ITS and connected environment.
2.	Future Thinking	The CCMS shall be the initial and ongoing security product and enabler of national and international alignment and harmonisation for C-ITS.
3.	Flexibility and Interoperability	The CCMS shall ensure interoperability, and be communications agnostic, supporting the lifecycle of devices, and maximising safety and productivity afforded

		by critical messages.
4.	Smart Cities Scalability	The CCMS shall be highly scalable and flexible, supporting Australia's C-ITS needs for transport systems, across all levels of participation, that support devices in operation for at least 10 years.
5.	Management and Accountability	The CCMS Manager shall be accountable for the implementation, operation and maintenance of the CCMS.

9.3 How to use these Foundational Requirements

The Foundational Requirements are intended to be a national resource for those responsible for decision making and planning in this space, and to enable informed discussion and cooperation amongst Australian stakeholders.

The 'Level of Maturity' attribute expresses TCA's view on the state of the global market on each particular requirement. This view is based on TCA's long-term involvement in and co-leadership of the international harmonisation efforts associated with C-ITS.

A Foundational Requirement may be required for deployment from 'day 1' or can undergo a 'phased approach' – that is, it can implemented over time, providing that consideration is given to it from the outset.

Each foundational requirement is further supported by a high level, 'plain language' description intended for policy and decision makers.

*Note: These requirements have been developed for a **national** CCMS, and a **holistic** approach to security. Although they can be tailored and subsequently adapted for the purpose of C-ITS pilots, there are security, technical and operational consequences associated with their selective adoption.*

Note: These requirements are draft insomuch as finalisations of the CCMS requirements internationally are still progressing, including further consideration in Australia.

9.4 Australian Foundational Requirements for a National Cooperative Credential Management System (CCMS)

9.4.1 Confidentiality, Integrity and Availability

The CCMS shall provide Confidentiality, Integrity (encompassing authentication and non-repudiation) and Availability on an ongoing basis, as demanded by the C-ITS and connected environment.

Requirement	Required for Day 1?	Explanation	Level of Maturity
1. The CCMS shall have the capability to detect and respond to imminent and perceived threats and attacks in the on-road environment	Phased approach	Pilots internationally have recently commenced examining the detection and response mechanisms for imminent and perceived threats. This work remains immature and will be informed by the pilots and initial stages of deployment. It is considered a vital area for the establishment of appropriate practise in the early stages of operation.	Low
2. The CCMS shall support Misbehaviour Management[32]	Phased approach	Misbehaviour Management is a developing area. It shall be supported by building proactive security monitoring into the foundations of the CCMS. It is expected that the misbehaviour functions will evolve rapidly from operational learnings.	Low
3. A Privacy Impact Assessment (PIA) shall be conducted on the CCMS to ensure it is implemented in accordance with privacy requirements	Yes	A PIA for the CAM/DENM[33] is being undertaken by Austroads. Consideration should be given to a PIA of the CCMS and to the institutional arrangements for its operation.	High
4. The CCMS shall enable the highest possible level of anonymity of drivers	Yes	Privacy shall be achieved through anonymous broadcast of vehicle travel information. The CCMS shall support the privacy of users through the use of Pseudonym Certificates.[34] Anonymity will also be dependent on decisions regarding how frequently the ITS Station "swaps" pseudonym certificates during its operation.	Low

[32] Misbehaviour Management – the ability to detect and, where appropriate, remove from the operational environment devices that pose a security or safety threat.
[33] Cooperative Awareness Message (CAM) and Decentralised Environmental Notification Message (DENM) – messages that are being constantly broadcast by C-ITS devices.
[34] When an ITS Station wishes to communicate with another ITS Station it will use, as required, authorisation (including pseudonym) certificates so that the other ITS Station can establish whether it will trust the information. The use of pseudonym certificates provides anonymity.

Requirement	Required for Day 1?	Explanation	Level of Maturity
5. The design of the CCMS 'back office' shall provide the highest possible level of anonymity for drivers	Phased approach	Back office anonymity is dependent on a combination of technical architecture and organisation structure for CCMS management. The technical architecture of the CCMS is untested in full operation, however testing is underway in other regions. The organisation structure required to achieve anonymity within the CCMS is proven with other regulatory telematics programs and within the ISO 15638 TARV standards.	Medium
6. The CCMS shall support the reporting of Misbehaviour Management and certificate revocation activities with other CCMS where there is cross-certification[35] and appropriate arrangements exist	Yes	These functions and formal arrangements ensure that the CCMS is interoperable with deployments in Europe and North America. As manual cross-certification with other CCMS is recommended for day 1, some reporting to other CCMS should be enabled. An analysis and PIA should be undertaken when appropriate on the exchange of information between CCMSs given this will result in data exchange across borders.	Low
7. The CCMS shall detect and respond to imminent and perceived threats and attacks within the CCMS	Phased approach	Misbehaviour Management is a developing field, but the CCMS can be monitored for a number of threats and attacks known to exist on the Internet. Monitoring for these threats will help inform future deployments and the risks and issues associated with operating a complex and distributed security system.	Low
8. The CCMS shall provide privacy protection required and expected in Australia	Yes	CCMS in the US and EU markets provide on-road privacy. However the EU architecture does not address privacy within the CCMS back-office environment. Considering this matter thoroughly would require further analysis. Australia has institutional arrangements that are not present in US and EU markets and provide capability to manage the security requirements of the back-office environment.	Medium
9. The foundation security within the CCMS shall be Public Key Infrastructure (PKI)	Yes	Existing PKI security technology and procedures provide all the necessary privacy and anonymity elements to support the unique needs of C-ITS.PKI has been identified globally as the security infrastructure to support communications agnostic C-ITS.	Medium

[35] Cross-certification is the ability of one CCMS to trust the certificates issued to a C-ITS device by another CCMS – it is part of developing a trusted and interoperable environment.

Requirement	Required for Day 1?	Explanation	Level of Maturity
10. The CCMS shall have a Threat, Vulnerability and Risk Assessment (TVRA) completed during its implementation; ideally after the development of its architecture, and certainly before deployment	Yes	The CCMS is subject to a high degree of security risk. It may be the target of a variety of malicious attacks (or inadvertent lapses in security) on a number of fronts. To enable a risk-based operational approach, a TVRA shall be undertaken to verify the architecture and design for operational readiness.	Medium
11. The CCMS shall support receiving requests, generating and issuing, and revoking enrolment certificates	Yes	These are core functions of the CCMS and may be supported with manual processes however this could be resource intensive for a national deployment depending on the take-up.	Medium
12. The CCMS shall support receiving, generating and issuing, and revoking authorisation and pseudonym certificates	Yes	These are core functions of the CCMS and may be supported with manual processes. This could be resource intensive for a national deployment depending on the take-up. Where an ITS Station is unable to request new pseudonym certificates automatically, the manual processes can ensure the provider can still participate. This may be necessary in the early stages of a national deployment if there are limited numbers of vehicles.	Medium
13. The CCMS shall adopt privacy by design principles	Yes	Policy makers will need to 'measure up' CCMS functions and future CCMS Manager processes and practices against 'best practice' privacy design. References to ICT and telecommunications can provide valuable insights.	High
14. The architecture of the CCMS informs any specific policy requirements for the protection of the identification of individuals and management of personal information	Yes	The CCMS architecture and its objectives will inform policy makers on the need for the protection of privacy. Policy requirements and capabilities of the CCMS will inform policy makers in order to achieve a result that is practical and implementable.	High

Requirement	Required for Day 1?	Explanation	Level of Maturity
15. Compliance assurance shall be determined based on risk and appropriate certification approaches	Yes	Certification processes of organisations, applications and ITS Stations (as applicable) shall address the security risks. This involves managing risks associated with the issuing of enrolment and pseudonym certificates, identifying minimum compliance requirements, and a process for compliance assurance (note this could be a combination of self-assessment, certification and testing). It is anticipated this compliance assurance activity will be largely contained with the pre-operational phase. Internationally activities are progressing in identifying appropriate approaches with the US and EU both exploring how this will be achieved.	Medium
16. Data interfaces within and to the CCMS shall operate reliability and securely	Yes	The CCMS will support secured communications between functions. This will use symmetric keys where appropriate. Full audit trail will be enabled to support reviews and operational learnings. Given the complexity of the C-ITS environment, the audit of activities of the CCMS will be an important aspect.	High

Discussion Questions

- What privacy provisions should be considered for opt-in C-ITS applications?
- How should C-ITS users (end users, public and private sector organisations) be informed of breaches of, or threats to, confidentiality, integrity and availability?
- Where privacy in back office systems is not supported (as may be the case in some jurisdictions):
  - what can be done to alert users to the risks associated within the security domain?
  - what steps can be put into place to ensure that adequate levels of security are ensured?

9.4.2 Future Thinking

The CCMS shall be the initial and ongoing security product and enabler of national and international alignment and harmonisation for C-ITS.

Requirement	Required for Day 1?	Explanation	Level of Maturity
17. Government should lead the design, establishment and operation of the CCMS	Yes	To align with US and EU CCMS scoping, the CCMS development and operation should be led by the public sector. This does not preclude the private sector from providing the systems. With the potential for significant privacy issues, in addition to public policy considerations, this approach will ensure adherence to strict privacy requirements in a highly complex information environment. For example, the European Commission has established the C-ITS Platform, an initiative led by the European Commission that engages all areas of interest to establish all aspects of C-ITS.	Low
18. The CCMS shall align with the standards necessary to support a national decision on regional alignment	Yes	The CCMS will adopt European standards and hence, the European CCMS architecture. Particularly standards from ETSI and ISO/CEN are applicable. While some key standards, in particular those for the CCMS directly are yet to be developed for Europe (and they are available as specifications in the United States for the current deployments) consideration will be given to United States Standards where they provide value and do not affect the deployment (such as SAE 2735). It should be noted that while this is a simple statement, following the European standards, and hence supporting Europe's' global footprint, will require close and continuous engagement and monitoring with European CCMS counterparts – in particular ETSI and ISO/CEO.	Medium
19. The CCMS shall adopt the Cooperative-ITS Security Policy Framework developed by HTG6 and appropriate standards	Yes	The Cooperative-ITS Security Policy Framework developed by HTG6 identified priorities for security harmonisation in the C-ITS domain. Aligning as much as possible with these priorities will maximise the chances of re-using systems and processes across deployments which in turn minimise future costs.	High

Requirement	Required for Day 1?	Explanation	Level of Maturity
20. The CCMS shall, through the CCMS Manager, support bootstrapping of ITS Stations in Australia and overseas	Yes	It is anticipated that most C-ITS equipped vehicles will be bootstrapped overseas and should be supported.	Medium
21. The CCMS shall support cross-certification with another CCMS	Phased approach	A future national CCMS will need to support cross-certification with another (overseas) CCMS. The CCMS should be able to support cross-certification as it is expected by vehicle manufacturers and in the future, mobile (or smartphone) ITS Stations.	Low
22. The CCMS shall comply with Australian Government security standards	Yes	The alignment of C-ITS standards and international harmonisation priorities with the Australian Government Security standards (specifically the Australian Government Information Security Manual (ISM)) has not been tested. This should be undertaken.	High

Discussion Questions

- What are the public policy considerations involved in Government leading the design, establishment and operation of the CCMS?
- What are the primary challenges associated with initiating and sustaining meaningful stakeholder cooperation and coordination on a national level in Australia?
- What assurances are required for users surrounding the C-ITS readiness (bootstrapping) of new vehicles?

9.4.3 Flexibility and Interoperability

The CCMS shall ensure interoperability, and be communications agnostic, supporting the lifecycle of devices, and maximising safety and productivity afforded by critical messages.

Requirement	Required for Day 1?	Explanation	Level of Maturity
23. The CCMS shall support the deployment of any ITS Station[36] that meets the requirements that govern its operation in Australia	Yes	The CCMS will need to support the needs of the ITS Stations from day 1. This is mitigated by aligning the CCMS with the use of internationally developed/developing standards.	Low
24. The CCMS shall support four levels of participation (full participation, collection only, beacon only and no participation)	Phased approach	Digital certificates may be required to identify ITS Station capabilities with respect to how they interact with other ITS Stations. This will be supported where the standards allow it.	Low
25. The CCMS shall meet the needs of ITS Stations and applications (i.e. enrolment and pseudonym certificates)	Yes	The CCMS should accommodate any distinct features of ITS Stations and applications requiring certificates for signing. For the CCMS to provide long-term security and support, review and reporting needs to highlight departures from anticipated futures standards and/or norms as a guidance for future CCMS enhancement and C-ITS implementation.	Medium

[36]ITS Station – the collective ITS functions implemented in cars, mobile phones, roadside infrastructure, etc.). This is the more specific term to designate what is elsewhere referred to as a C-ITS device.

Requirement	Required for Day 1?	Explanation	Level of Maturity
26. The CCMS shall be communications agnostic	Yes	The CCMS shall support any communication medium requiring it – this is similar to PKI such as that used to secure websites, which is agnostic of the communication medium (i.e. it is the same whether the website is visited over ADSL/Fibre, mobile or dial-up connection). The CCMS shall also support applications running on ITS Stations agnostic of the communications medium the ITS Station uses for its application – this will mean applications can leverage the CCMS for security independent of the method of communication with other ITS Stations. This does not mean an application must use security provided by the CCMS (although safety applications should use it) but the CCMS should not be designed limiting the communications mechanisms in use to cater to innovation and evolution in communications.	High

Discussion Questions

- Beyond safety applications, are there applications for which use of the CCMS should be mandatory; if so, should the communications medium, to ensure interoperability, be specified for these applications?

9.4.4 Smart Cities Scalability

The CCMS shall be highly scalable and flexible, supporting Australia's C-ITS needs for transport systems, across all levels of participation, that support devices in operation for at least 10 years.

	Requirement	Required for Day 1?	Explanation	Level of Maturity
27.	The CCMS shall be highly scalable and extensible	Yes	It is unclear how many ITS Stations, services and applications will need to be supported and over what timeframe the adoption of C-ITS will occur. It is recommended that analysis should be undertaken to identify the scalability and its timeframe.	Low
28.	The CCMS shall support the automated distribution of Certificate Revocation Lists (CRL)	Yes	Certificate Revocation Lists (CRLs) are made available to identify ITS Stations which can no longer be trusted in the C-ITS environment. Commonly referred to as blacklisting, the CRL can be used by other ITS Stations and systems to identify CAM/DENM and application messages from specific ITS Stations that should be ignored due to any reason – common reasons include malfunctions, security breaches, incorrect performance, bugs and other issues. Current EU CCMS deployments do not support the automated CRL distribution (though this may be supported in the future), instead relying the CCMS rejecting requests for pseudonym certificate updates for 'blacklisted' ITS Stations. The planned and unified US CCMS deployment, on the other hand, will support automated CRL distribution. Timely use of CRLs goes to the core of the long-term integrity of a CCMS.	Medium
29.	Where possible, a performance-based approach to specifying security needs should be used	Yes	With many elements to security, there is no "one size fits all" approach. The performance of the CCMS and its manager will enable the ongoing viability and robustness of this approach as operational learnings are captured.	High
30.	The CMMS shall be extensible across ITS Stations, applications and geography	Yes	The CCMS needs capability to support a changing, multi-channel and geographically diverse environment.	High

Requirement	Required for Day 1?	Explanation	Level of Maturity
31. The CCMS shall support the very long term deployment of ITS Stations (i.e. ITS Stations with a lifespan of greater than 10 years)	Phased approach	It is expected the CCMS and ITS Stations will require upgrades within five years to support future developments. While vehicles may be in the market longer than 10 years, for the purposes of a CCMS, it is expected it will need to support the security functions as they evolve for at least 10 years.	Medium
32. The CCMS shall support C-ITS core functions[37] across the full lifecycle of the ITS Station	Yes	All C-ITS core functions across the lifecycle of the ITS Station shall be supported.	Medium
33. The CCMS architecture and implementation strategy shall enable and accommodate organic growth	Yes	The system side of the CCMS can follow appropriate IT standards based processes. These should be identified as best suited to the CCMS IT implementation and its operation. The process side of the CCMS should 'touch' the full ITS Station lifecycle. Information Technology Infrastructure Library (ITIL) represents a well-regarded framework for IT service delivery that could be relevant in this instance.	High

[37] The C-ITS core functions developed by Austroads are based on an assessment of the Australian and New Zealand situation, and take into account those developed by the United States Federal Highway Administration, and the combined definitions from standards organisations ISO, CEN and ETSI. The core functions are:

1. Secure exchange of data between users and applications
2. Trust and integrity of data
3. Assurance of privacy between users and from third parties
4. Facilitation of a platform for sharing of data and efficient use of resources
5. Assurance of national interoperability and nationally consistence service areas.

See Austroads. 2015. *Concept of Operations for C-ITS Core Functions*, p. 9-10. Available at https://www.onlinepublications.austroads.com.au/items/AP-R479-15

Discussion Questions

- How can end-of-life (the the time at which the operation of a service or product will cease to be supported by the manufacturer, developer, or other service provider) be managed, and conveyed to users?
- How should users:
  - be notified that they have been ‘blacklisted’ (ie. added to a Certificate Revocation List)?
  - be notified of the reason why they have been blacklisted?
  - resolve issues surrounding being removed from a blacklist?
- Should/how might users have the ability to report the misbehaviour of their own C-ITS devices, or the misbehaviour of others?

9.4.5 Management and Accountability

The CCMS Manager shall be accountable for the implementation, operation and maintenance of the CCMS.

Requirement	Required for Day 1?	Explanation	Level of Maturity
34. The CCMS Manager shall ensure the core functions needed by its various stakeholders are supported and available	Yes	Establishment of the service levels should be driven by the needs of ITS Stations and their business owners. There will be varying service levels depending on the ITS Station – road managers and operators may require different service levels to mobile ITS Stations for example. These should be investigated and developed to inform the CCMS development and implementation.	Medium
35. The CCMS Manager shall provide a coordination function with other CCMS Managers nationally (if required) and internationally	Yes	A single CCMS should be implemented for Australia given its cost and complexity. To avoid the risk of a proliferation of CCMS implementations, the CCMS Manager should undertake a coordination function to maximise national benefits, and more facilitate international harmonisation.	Medium
36. The CCMS Manager shall be responsible for the establishment of processes, standards and 'certification' for the CCMS and ITS Stations wishing to receive enrolment and pseudonym certificates (i.e. to participate)	Yes	International Harmonisation Task Groups (specifically, HTGs 6 and 7) identified a need for certification of security of ITS Stations to be undertaken to the level needed to issue an enrolment certificate[38] to an ITS Station. The issuing of an enrolment certificate enables the ITS Station to commence operating in the C-ITS environment and without appropriate controls it could result in a plethora of ITS Stations operating incorrectly and without oversight. The CCMS Manager is logically placed to undertake the necessary certification to enable security and hence participation. Once allowed in, given the volume and breadth of ITS Stations expected, it will be difficult to operationally manage the C-ITS environment if these matters are not settled from the outset.	Medium
37. The CCMS Manager shall be responsible for the maintenance of processes, procedures, standards and certification for the CCMS	Phased approach	A recommendation from the Cooperative ITS Security Policy Framework developed by HTG6, these activities should be undertaken by the CCMS Manager. It is not clear the extent of effort and resources required to establish and maintain this requirement. Pilots are informing this task and a phased approach may enable prioritisation of critical processes, procedures and certification.	Low

[38] Enrolment certificates are in effect the ITS Station's birth certificate. The enrolment certificate is installed into the ITS Station using an approved, secure, and trusted process that is typically certified by a certification body. The enrolment certificate is the master certificate of the ITS Station and so not typically used for everyday transactions but kept safe and secure within the ITS Station.

Requirement	Required for Day 1?	Explanation	Level of Maturity
38. The CCMS Manager shall be responsible for the compliance with processes, procedures, standards and certification for the CCMS	Phased approach	These activities shall be undertaken by the CCMS Manager. It is not clear the extent of effort and resources required to establish and maintain this requirement. Pilots are informing this task and a phased approach may enable prioritisation of critical processes, procedures and certification.	Low
39. The CCMS Manager shall have appropriate funding arrangements	Yes	The structure of funding regimes (e.g. user-pays verse causer-pays) shall be determined.	High
40. The CCMS Manager shall have long term viability	Yes	The long-term viability of a national CCMS is critical and should be informed by continued pilots, international developments and cooperation.	High
41. CCMS shall be implemented locally	Yes	There are significant privacy issues and there are few private sector providers of the CCMS. To ensure the appropriate privacy environment and avoid conflicts, the CCMS shall be implemented within Australia. The technical and operational benefits to doing so are also significant in that it enables evolution through operational learnings and more efficient re-configuration to support an evolving environment.	Low
42. The CCMS Manager shall manage the CCMS and its full lifecycle	Yes	Management of the CCMS should address both the implementation and ongoing 'fit for purpose' capability of the CCMS. Recognising that the life of a C-ITS device will be consistent with the life of vehicles in the market (nominally at least 10 years) there will need to be active and ongoing management and maintenance of the CCMS throughout its lifecycle. Having an entity 'on point' to manage the issue would both support the ongoing viability and provide insight into the long-term need for and intensity of this kind of activity.	Low
43. A central approach to the administration of the CCMS should be taken	Yes	On day 1 a centralised approach should be taken to the CCMS as far as is possible. While it may de-centralise over time, by centralising the CCMS it will enable closer management of security and operational risks and issues that can be addressed more effectively and in a timelier manner that will be important to the early stages of operation.	Low
44. Certification and accreditation processes shall be, as far as practicable, based on national and international standards	Yes	Harmonisation with international practices shall be an ongoing process, which should be undertaken by the CCMS Manager.	Low

Requirement	Required for Day 1?	Explanation	Level of Maturity
45. Each entity participating in the CCMS shall ensure their compliance with the security requirements established in relation to the CCMS	Yes	The CCMS is not an isolated security system – it is dependent on stakeholders that use it to ensure they operate in a secure manner in accordance with agreed policies and procedures. If an ITS Station is not appropriately secured, it can lead to vulnerabilities both to the vehicle as well as to the C-ITS environment. Much like providing users with incorrect access to a server, certificates must be managed appropriately once issued to avoid spoofing of vehicles and other threats. Many activities are related to adhering to appropriate policies and procedures rather than simply technology.	Medium
46. The CCMS Manager shall be responsible for the CCMS Architecture	Yes	The CCMS architecture may need to evolve or be refined in response to issues uncovered. Having an entity 'on point' to manage the issue would both support the ongoing viability of the trial and provide insight into the long-term need for and intensity of this kind of activity.	Medium
47. The CCMS Manager shall make policies and requirements available to those that legitimately require it	Yes	Making available the CCMS related policies and requirements to stakeholders would serve as both an educational and verification process – strengthening the national implementation.	Medium
48. The CCMS shall support the reporting of Misbehaviour Management and certificate revocation activities with other stakeholders as required by operations	Yes	Linked to Misbehaviour Management, the CCMS Manager's engagement with stakeholders to manage operational issues that will occur with ITS Stations and the CCMS (Misbehaviour Management) is important and should be seen as an area that will evolve in the operational environment.	High
49. The CCMS Manager shall be transparent in its management of the CCMS	Yes	Institutional arrangements will need to be put in place that enable appropriate reporting and communications with a large and diverse stakeholder group. This will require strict governance to ensure the exchange of information necessary to operate the CCMS in a manner to ensure the overall success of a C-ITS deployment, and the overall C-ITS environment.	High

Requirement	Required for Day 1?	Explanation	Level of Maturity
50. The CCMS Manager shall undertake stakeholder management of all stakeholders that interface with the CCMS	Yes	These activities can, in principle, be performed outside an CCMS Manager role. However, stakeholder management – at least from a reporting perspective – should inform future decision making.	High
51. The CCMS Manager shall ensure the establishment and maintenance of trust between organisations participating in C-ITS	Yes	An organisational function, establishing the necessary mechanisms to verify and trust participating organisations is critical to establishing the certification, accreditation or approval requirements to ensure participating organisations meet the required standards. It is expected the CCMS Manager would undertake this activity.	High
52. The CCMS Manager shall have technical, operational and commercial capability	Yes	The capability the CCMS Manager is critical to the operation of a PKI security environment, and to be able to monitor and maintain a complex, geographically diverse environment which is based upon a culture of the highest integrity and confidentiality.	High

Discussion Questions

- Should/how might the CCMS Manager alert users and other stakeholders to security threats both on and off the road?
- How can the CCMS Manager better facilitate the ability of entities to take steps to ensure their compliance?
- What systems and processes could be enabled to manage end-of-life cycles between service providers/developers and the CCMS Manager?

10 FURTHER DISCUSSION QUESTIONS

Issues in scope

- Are there issues that this discussion paper has not touched on that should be included?

Non-traditional stakeholders

- How can Governments and industry better engage with non-traditional stakeholders in the security, automotive and connected space?

Disruptive technology

- Has your organisation developed, or considered developing, a disruption/transformation strategy?
- If so, what were the main challenges associated?

Public engagement

- What strategies should governments and industry be considering, to engage the public on matters concerning the connected and cooperative environment, leading to Smart Cities and the Internet of Things?