PD ISO/TR 17427-4:2015

BSI Standards Publication

Intelligent transport systems — Cooperative ITS

Part 4: Minimum system requirements and behaviour for core systems

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 17427-4:2015.

The UK participation in its preparation was entrusted to Technical Committee EPL/278, Intelligent transport systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 87421 5
ICS 03.220.01; 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TR 17427-4:2015

TECHNICAL REPORT

ISO/TR 17427-4

First edition
2015-11-01

Intelligent transport systems — Cooperative ITS —

Part 4: Minimum system requirements and behaviour for core systems

Systèmes intelligents de transport — Systèmes intelligents de transport coopératifs —

Partie 4: Exigences minimales du système et comportement des systèmes principaux

Reference number
ISO/TR 17427-4:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

ISO 17427 consists of the following parts, under the general title *Intelligent transport systems — Cooperative ITS*:

— *Part 2: Framework Overview [Technical Report]*

— *Part 3: Concept of operations (ConOps) for 'core' systems [Technical Report]*

— *Part 4: Minimum system requirements and behaviour for core systems [Technical Report]*

— *Part 6: 'Core system' risk assessment methodology [Technical Report]*

— *Part 7: Privacy aspects [Technical Report]*

— *Part 8: Liability aspects [Technical Report]*

— *Part 9: Compliance and enforcement aspects [Technical Report]*

— *Part 10: Driver distraction and information display [Technical Report]*

The following parts are under preparation:

— *Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s)*

— *Part 5: Common approaches to security [Technical Report]*

— *Part 11: Compliance and enforcement aspects [Technical Report]*

— *Part 12: Release processes [Technical Report]*

— *Part 13: Use case test cases [Technical Report]*

— *Part 14: Maintenance requirements and processes [Technical Report]*

This Technical Report provides an informative 'minimum system requirements and behaviour for core systems' for Cooperative Intelligent Transport Systems (*C-ITS*). It is intended to be used alongside ISO 17427-1, ISO/TR 17465-1 and other parts of ISO 17465, and ISO 21217. Detailed specifications for the application context will be provided by other ISO, CEN and SAE deliverables, and communications specifications will be provided by ISO, IEEE and ETSI.

Introduction

*Intelligent transport system*s (*ITS*) are transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort.

A distinguishing feature of '*ITS*' is its communication with outside entities.

Some *ITS* systems operate autonomously, for example, 'adaptive cruise control' uses radar/lidar and/or video to characterize the behaviour of the vehicle in front and adjust its vehicle speed accordingly. Some *ITS* systems are informative, for example, 'variable message signs' at the roadside or transmitted into the vehicle, provide information and advice to the driver. Some *ITS* systems are semi-autonomous in that they are largely autonomous but rely on 'static' or 'broadcast' data, for example, *GNSS* (2.22) based 'SatNav' systems operate autonomously within a vehicle but are dependent on receiving data broadcast from satellites in order to calculate the location of the vehicle.

*Cooperative Intelligent transport system*s (*C-ITS*) are a group of *ITS* technologies where service provision is enabled by, or enhanced by, the use of 'live', present situation related, dynamic data/information from other entities of similar *functionality* [for example, from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure [for example, from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)]. Effectively, these systems allow vehicles to 'talk' to each other and to the infrastructure. These systems have significant potential to improve the transport network.

A distinguishing feature of '*C-ITS*' is that data is used across *application*/service boundaries.

This Technical Report is a 'living document' and as our experience with *C-ITS* develops, it is intended that it will be updated from time to time, as and when we see opportunities to improve this Technical Report.

TECHNICAL REPORT **ISO/TR 17427-4:2015(E)**

Intelligent transport systems — Cooperative ITS —

Part 4: Minimum system requirements and behaviour for core systems

1 Scope

The scope of this Technical Report is, as an informative document, to identify potential critical minimum system requirements and behaviour for core systems issues that *C-ITS* service provision may face or introduce, to consider strategies for how to identify, control, limit or mitigate such issues. The objective of this Technical Report is to raise awareness of and consideration of such issues and to give pointers, where appropriate, to subject areas and, where available, to existing standards deliverables that provide specifications for all or some of these aspects. This Technical Report does not provide specifications for solutions of these issues.

2 Terms and definitions

2.1
anonymity
lacking individuality, distinction, and recognizability within message exchanges

2.2
anonymous certificates
certificate which contains a pseudonym of the system user instead of their real identity in the subject of the certificate and thus preventing other system service recipients from identifying the certificate owner when the certificate is used to sign or encrypt a message in the connected vehicle/highway system (C-ITS, connected vehicle)

Note 1 to entry: The real identity of the anonymous certificates can be traced by authorized system operators by using the services of a registration authority and/or certification authority.

2.3
application
'app'
software application

2.4
application service
service provided, for example, by a service provider accessing data from the IVS within the vehicle in the case of C-ITS, via a wireless communications network, or provided on-board the vehicle as the result of software (and potentially also hardware and firmware) installed by a service provider or to a service provider's instruction

2.5
authenticity
property of being of undisputed origin and not a copy, authenticated, and having the origin supported by unquestionable evidence

Note 1 to entry: Something that has had its authenticity confirmed could be described as "authenticated" or "verified".

2.6
authorization
process of determining what types of activities or access are permitted on a network

Note 1 to entry: This is usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

2.7
bad actor
role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other service recipients, and/or operates outside of its authorized scope

2.8
C-ITS
Cooperative ITS
group of *ITS* technologies where service provision is enabled, or enhanced by, the use of 'live', present situation related, data/information from other entities of similar functionality [(for example, from one vehicle to other vehicle(s)], and/or between different elements of the transport network, including vehicles and infrastructure (for example from the vehicle to an infrastructure managed system or from an infrastructure managed system to vehicle(s)

2.9
catalogue
repository used by the 'Data Distribution subsystem' for maintaining data publishers information including the type of data they are transmitting, frequency of that data, address, data source, etc.

2.10
centre
entity that provides application, management, administrative, and support functions from a fixed location (the terms "back office" and "centre" are used interchangeably)

Note 1 to entry: Centre is, traditionally, a transportation-focused term, evoking management centres to support transportation needs, while back office generally refers to commercial applications; from the perspective of this Technical Report, these are considered the same.

2.11
core services
set of functions within the 'Core System' subsystems that interact with system service recipients

2.12
core system personnel
staff that operate and maintain the 'Core System'

Note 1 to entry: In addition to network managers and operations personnel, 'Core System' personnel includes the administrators, operators, maintainers, developers, deployers and testers.

2.13
coverage area
geographic jurisdiction within which a 'Core System' provides *core services* (2.11)

2.14
data provision
act of providing data to a core system

2.15
delta
updates
records
data that is new since the last block of data that was downloaded

2.16
digital certificate
electronic "identification card" that establishes user credentials when doing business or other transactions

Note 1 to entry: This is issued by a certification authority: contains name, a serial number, expiration dates, a copy of the certificate holder's *public key* (2.40) (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Note 2 to entry: From the SysAdmin, Audit, Network, Security Institute - www.sans.org

2.17
environment
circumstances, objects, and conditions that surround a system to be built

Note 1 to entry: It includes technical, political, commercial, cultural, organizational, and physical influences, as well as standards and policies that govern what a system shall do or how it will do it.

2.18
error message
message that indicates issues with cross-jurisdictional compatibility, scope coverage service or service availability

2.19
facility
building or group of buildings with access restrictions housing a 'Core System'

2.20
functionality
capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product

2.21
geo-cast
delivery of a message to a group of network destinations identified by their geographic locations

2.22
global navigation satellite system
GNSS
comprises several networks of satellites that transmit radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of its receiver anywhere around the globe

EXAMPLE GPS, GLONASS, Galileo.

2.23
integrity
internal consistency or lack of corruption in electronic data

EXAMPLE A system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible.

2.24
intelligent transport systems
ITS
transport systems in which advanced information, communication, sensor and control technologies, including the Internet, are applied to increase safety, sustainability, efficiency, and comfort

2.25
link
locus of relations among nodes

Note 1 to entry: It provides interconnections between nodes for communication and coordination; may be implemented by a wired connection or with some radio frequency (RF) or optical communications media; links implement the primary function of transporting data; links connect to nodes at a *port* (2.38).

2.26
maintainability
keep in an existing operational state preserved from failure or decline of services (with minimum repair, efficiency, or validity)

2.27
misbehaviour
act of providing false or misleading data, operating in such a fashion as to impede other service recipients, or to operate outside of their authorized scope

Note 1 to entry: This includes suspicious behaviour as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages, etc., either purposeful or unintended.

2.28
misbehaviour information
misbehaviour (2.27) reports from system service recipients, as well as other improper system user acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate system user behaviour

2.29
misbehaviour report
information from a system user identifying suspicious behaviour from another system user that can be characterized as *misbehaviour* (2.27)

2.30
mobile
vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travellers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information

2.31
mode
phase within a state (degraded mode occurs automatically due to certain conditions), such as, when in *operational state* (2.33), there is an automatic transition to degraded mode because of a detected hardware failure

Note 1 to entry: Modes are normal, degraded, restricted and degraded/restricted.

2.32
node
physical hardware engineering object that is a run-time computational resource and generally has at least memory and processing capability

Note 1 to entry: Run-time software engineering objects reside on nodes; node has some well-understood, possibly rapidly moving, location [a node may be composed of two or more (sub) nodes].

2.33
operational state
all activities during the normal conduct of operations and also needs to be able to handle support for services from other 'Cores Systems' including fail-over and/or degraded services

2.34
operator
day-to-day providers of the 'Core System' that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system

2.35
parsing
analysing (a string, text or data) into logical syntactic components

2.36
permission
authorization (2.6) granted to do something (to the 'Core System'), permissions are granted to system service recipients and *operators* (2.34) determining what actions they are allowed to take when interacting with the 'Core System'

2.37
physical security
safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, *facility* (2.19), resource, or stored information (this can include simply a locked door, badge access controls, or armed security guards)

2.38
port
physical element of a *node* (2.32) where a *link* (2.25) is connected; nodes may have one or more ports;each port may connect to one or more physical ports on (sub) nodes that are contained within the node

2.39
private network
network belonging to a person, company or organization that uses a public network (usually the Internet) to connect its remote sites or service recipients together

2.40
public key
cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key)

2.41
registry
repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.

2.42
states
distinct system setting in which the same user input will produce different results than it would in other settings

Note 1 to entry: The 'Core System' as a whole is always in one state [a state is typically commanded or placed in that state by an *operator* (2.34); states are installation, operational, maintenance, training, and standby].

3 Abbreviated terms

C-ITS cooperative intelligent transport systems, cooperative ITS

ITS intelligent transport systems (2.24)

IVS in-vehicle system (2.6)

TR technical report

ANSI	American National Standards Institute
CA	certification authority
CALM	Communications Access for Land Mobile Standards
CAMP	Crash Avoidance Metrics Partnership
ConOps	concept of operations
CRL	certification revocation lists
CVIS	Cooperative Vehicle Infrastructure System (Project)
DNS	domain name system
EC	European Commission
ESS	external support system
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GHz	gigahertz
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet protocol
LTE	long term evolution
NIST	National Institute of Standards and Technology
PKI	public key infrastructure
PKIX	public key infrastructure based on X.509 certificates
RA	registration authority
RFC	request for comments
RITA	Research and Innovative Technology Administration
RSE	roadside equipment
SAP	service access point
SyRS	system requirements specification
USDOT	US Department of Transportation
UTC	coordinated universal time
VII	vehicle infrastructure integration

4 How to use this Technical Report

4.1 Acknowledgements

Inspiration for the technical content identification and consideration of this Technical Report has been largely obtained from various documents generated and publicized by US DoT RITA, especially "'Core System' Requirements Specification (SyRS)".

Conceptual input from the EC project CVIS is also acknowledged.

Contribution from the Australian National Transport Commission, Cooperative Intelligent Transport Systems Policy Paper (A Report prepared by: National Transport Commission) ISBN: 978-1-921604-47-8) is also acknowledged.

See Bibliography for further details of contributions.

4.2 Guidance

This Technical Report is designed to provide guidance and a direction for considering the issues concerning minimum system requirements and behaviour for core systems associated with the deployment of *C-ITS* service provision. It does not purport to be a list of all potential minimum system requirements and behaviour for core systems factors, which will vary according to the scope of the core system being provided, the regime of the jurisdiction, the location of the instantiation and to the form of the instantiation, nor does it provide definitive specification. Rather, this Technical Report discusses and raises awareness of the major minimum system requirements and behaviour for core systems issues to be considered and provides guidance in the context of future and instantiation specific deployments of *C-ITS* core systems.

This document should be read in conjunction with, and in most cases, following consideration of the following:

— ISO 17427-1, *Intelligent transport systems — Cooperative ITS — Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s);*

— ISO/TR 17427-2, *Intelligent transport systems — Cooperative ITS — Part 2: Framework Overview;*

— ISO/TR 17427-3, *Intelligent transport systems — Cooperative ITS — Part 3: Concept of operations (ConOps) for 'core' systems.*

These documents, as their titles imply, identify the principal actor groups and their roles and responsibilities in *C-ITS* service provision, overview for such systems, and describe the concept of operations for core systems supporting *C-ITS* service provision. Frequent reference to these documents and their provisions will be made, but largely not re-described, so familiarity with those documents is a precursor to comprehension and understanding of this Technical Report. The objective of this Technical Report is, within the context of ISO 17427-1, ISO/TR 17427-2, and ISO/TR 17427-3, to identify the minimum system capabilities and behaviour implicitly required to provide 'Core System' service provision and support to participating actors.

4.3 Stakeholders

The term "stakeholder" may be somewhat overused but generally refers to any individual or organization that is affected by the activities of a business process or, in this case, a system being developed. They may have a direct or indirect interest in the activity and their level of participation may vary. The term here includes public agencies, private organizations or the travelling public (end service recipients) with a vested interest, or a "stake" in one or more aspect of the connected vehicle/highway system *environment* (2.17) and the 'Core System'. 'Core System' stakeholders span the breadth of the transportation *environment* including the following:

— transportation service recipients, e.g. private vehicle drivers, public safety vehicle *operators* (2.24), commercial vehicle *operators*, passengers, cyclists and pedestrians;

— transportation *operator*s, e.g. traffic managers, transit managers, fleet managers, toll *operator*s, road maintenance and construction;

— public safety organizations, e.g. incident and emergency management, including fire, police and medical support;

— information service providers, e.g. data and information providers for transportation-related data, including traffic, weather and convenience *application*s;

— *application service* (2.4) providers;

— environmental managers, including emissions and air quality monitors;

— original equipment vehicle manufacturers (OEMs);

— in-vehicle device manufacturers;

— communications providers, including cellular network *operator*s;

— jurisdiction regulatory and research agencies;

— 'Core System' owners.

For a summary of the actors associated with *C-ITS* and its core roles and responsibilities, see ISO 17427-1.

5 C-ITS and 'minimum system requirements and behaviour for core systems'

5.1 Overview

For a summary of the roles and relationships associated with *C-ITS* and its core systems, see ISO 17427-1.

ISO 17427-1 envisions the combination of *application*s, services and systems necessary to provide safety, mobility and environmental benefits through the exchange of data between *mobile* (2.30) and fixed transportation service recipients. It consists of the following:

— *application*s that provide *functionality* (2.20) to realize safety, mobility and environmental benefits;

— communications that facilitate data exchange;

— core systems, which provide the *functionality* needed to enable data exchange between and among *mobile* and fixed transportation service recipients;

— support systems, including security credentials certificate and registration authorities, that allow devices and systems to establish trust relationships.

The main mission of any 'Core System' is to enable safety, mobility and communications-based *application*s for both *mobile* and non-*mobile* service recipients.

It is not the principle role of the'Core System' to provide end user *application service*s. Such services may be provided by the same computing and communications equipment but are, and need to be, kept separate from the 'Core System'.

The scope of the 'Core System' includes those enabling technologies and services that will, in turn, provide the foundation for *application*s. The 'Core System' works in conjunction with 'External Support Systems' (ESS) like a 'Certificate Authority' (CA) for wireless communications security. The system boundary for the 'Core System' is not defined in terms of devices or agencies or vendors but by the open, standardized interface specifications that govern the behaviour of all interactions between 'Core System' service recipients.

The 'Core System' supports a distributed, diverse set of *application*s. These *application*s use both wireless and wireline communications to provide the following:

— wireless communications with and between *mobile* elements including vehicles (of all types), pedestrians, cyclists, and other transportation service recipients;

— wireless communications between *mobile* elements and field infrastructure;

— wireless and wireline communications between *mobile* elements, field infrastructure, and back office/*centre*s (2.10).

This may provide support and security management for *ITS* specific wireless communications, such as 5,9 GHz, but may also provide gateway and/or SAP access/management to public wireless communications such as 4G/LTE/3G/2G (E_UTRAN/UMTS/GSM) or *mobile* wireless broadband, WiFi and even satellite telecommunications.

The operational *environment* in which the 'Core System' exists may vary from a single jurisdiction-wide monolithic system to a heterogeneous community of systems run by multiple agencies at different levels of complexity and various locations. The potential number of scenarios involving transport-related system service recipients is unlimited but all will involve some sort of wireless communication. *Application*s may be deployed in complex configurations supporting a major metropolitan area or a minimal configuration to support a set of isolated rural road warning systems.

As 'Core Systems' are deployed, some may include just the essential functions to support a particular local area and rely on an interface to another 'Core System' to provide additional services. For instance, one 'Core System' could include the necessary hardware and software to manage a subset of the subsystems for their local area and rely on a connection to another 'Core Systems' subsystems for additional services.

The 'Core System' will not necessarily require a control *centre* with large video screens or employ a large number of *operator*s. A 'Core System' can function in an office or data *centre environment* as long as there is access to a network that enables communications between system service recipients and the 'Core System'. A 'Core System' also does not necessarily imply a system provided by a single central mainframe computer and 'Core System' *functionality* may indeed be provided by a number of networked computers. However, the core 'system' is a single cohesive 'system' and there needs to be a clear line of management and control.

See ISO/TR 17427-3 for more detailed discussion and detail of these aspects. See ISO 17427-1 for detail or 'roles and responsibilities'.

A critical factor driving the conceptual view of the 'Core System' and the entire *connected vehicle/highway system environment* is the level of trustworthiness between communicating parties. A complicating factor is the need to maintain the privacy of participants, but not necessarily exclusively through anonymous communication. A 'Core System' should normally work on the principle of 'privacy by design' wherever possible, planning *anonymity* (2.1) into most trusted exchanges of data, using the jurisdictions privacy principles guidelines, and balancing privacy against security and safety (see ISO/TR 17427-7).

While the 'Core System' is being planned for 'privacy by design', it is also providing a foundation from which to leverage alternative and multiple communications methods. Prioritization will have to be made between time critical safety *application*s, non-time critical safety *application*s, and non-safety *application*s. Most of these alternatives are typically available on the market today and the levels of *anonymity* and privacy inherent to these systems are typically governed by agreements between communication providers and consumers. So while, within the 'Core System', privacy is not compromised for an individual, what happens between that individual and their communication provider (e.g. 3G service provider) may very well compromise privacy. Some *application* providers may require personal information in order to function which would require the *application* user to opt-in to use that *application*.

A 'Core System' to support *C-ITS* service provision may be designed and implemented in some cases as a nationally deployed and managed system but in other cases, will likely be deployed locally and

regionally and it shall be able to grow organically to support the changing needs of its user base. Deployments may be managed regionally but will need to follow International Standards to ensure that the essential capabilities are compatible no matter where the deployments are established.

Within the *connected vehicle/highway system environment,* the 'Core System' concept distinguishes communications mechanisms from data exchange and from the services needed to facilitate the data exchange. The 'Core System' supports the *connected vehicle/highway system environment* by being responsible for providing the services needed to facilitate the data exchanges. The contents of the data exchange are determined by *application*s unless the data exchange is used as part of the facilitation process between the user and the 'Core System'.

The 'Core System' provides the *functionality* required to support safety, mobility, and environmental *application*s. This same *functionality* may enable commercial *application*s but that is not a driving factor, rather, a side benefit. The primary function of the 'Core System' is the facilitation of communications between service recipients, some of which shall also be secure. The 'Core System' may also provide data distribution and network support services depending on the needs of the 'Core System' deployment.

The 'Core System' exists in an *environment* where it facilitates interactions between vehicles, field infrastructure and back office service recipients, as described in ISO 17427-1.

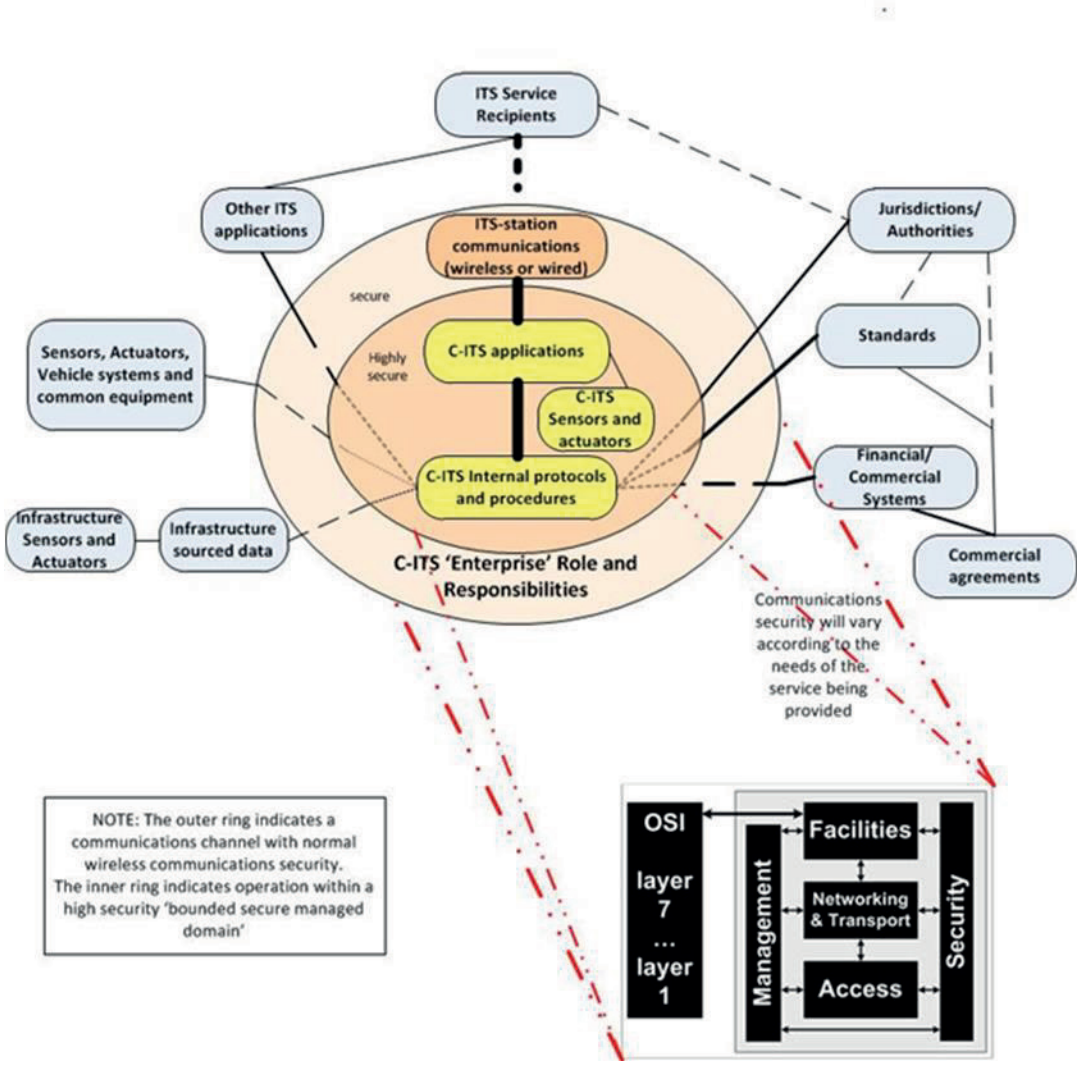

Figure 1 — 'Core system' boundary diagram (ISO 17427-1 – working draft)

In Figure 1, the service recipients, devices, and software *application*s are outside of the 'Core System' but the 'Core System' is still responsible for facilitating their security which is achieved according to

the needs of the *application*. Some *ITS* systems can utilize security from the communications network over which their wireless communication is made, which provides adequate security for the provision of their service, and others can control their data so it is only provided to a legitimate source, indeed, some data may not be sensitive to misuse. But most data in the *C-ITS* context has some sensitivity and therefore will have to be effected within layers of security and some *C-ITS* communications will have to be effected within the high levels of security that ISO 21217 calls a 'Bounded Secure Management Domain' (2.2). (See ISO 21217).

This is chiefly achieved by providing digital *certificate* (2.16)-based mechanisms to ensure trust between service recipients. The 'Core System' therefore has an intimate relationship with the 'Certification Authority' and there could be logic that the two aspects have common management to ensure consistency.

The 'Core System' also provides networking services to facilitate communications, though it does not comprise the communications network. The following are not part of the 'Core System':

— *mobile* service recipients (e.g. vehicle devices, pedestrian smartphones) – any user device;

— roadside equipment (RSE) – both public and commercial fixed devices;

— transportation management *centre*s (TMC) and other public or private back office or *centre*s.

It is also important to note that the 'Core System' is not meant to mandate or change existing transportation equipment, technology or transportation *centre*s. The 'Core System' provides mechanisms for efficiently collecting and distributing transportation data but does not necessarily replace existing systems, though it is likely that many existing data collection mechanisms will be made obsolete by its data collection and distribution function.

For further detail of these relationships and description of the subsystems, see ISO 17427-1.

While ISO 17427-1 provides the high level relationships in a *C-ITS* system and ISO/TR 17427-3 provides a *C-ITS* 'Core System' 'concept of operations', the specific role of a 'Core System' carries with it additional responsibilities, which need to be managed by defined subsystem, such as the following:

— Core2Core subsystem (see 5.2.1);

— Data distribution subsystem (see 5.2.2);

— *Misbehaviour* management subsystem (see 5.2.3);

— Network services subsystem (see 5.2.4);

— System service monitor subsystem (see 5.2.5);

— Time synchronization subsystem (see 5.2.6);

— User *permissions* subsystem (see 5.2.7);

— User trust management subsystem (see 5.2.8).

5.2 Subsystem features of the 'Core System'

5.2.1 Core2Core subsystem

In most, but not all, paradigms, the system will need to operate/co-operate with adjacent and/or parallel 'Core Systems'. See 5.1 and ISO/TR 17427-3.

This implies a requirement for a 'Core2Core subsystem'. The Core2Core subsystem needs to interface with other 'Core Systems', declaring its jurisdictional scope, offered services, and services it desires from other 'Core Systems'. The Core2Core subsystem will then need to maintain a knowledge base of data and services available among other 'Core Systems'. In this way, the 'Core System' can act as a

system user to another 'Core System', providing proxy services that it does not offer but another 'Core System' does.

Additionally, the Core2Core subsystem is responsible for compatibility between 'Core Systems', ensuring that one 'Core System' does not encroach on the scope of another 'Core System', and similarly accepting *error message*s (2.18) from *mobile* service recipients that might indicate a cross-jurisdictional compatibility or scope coverage issue. Interfaces between 'Core Systems' will be formalized in interface specifications. Conflicts and discrepancies between 'Core Systems' will have to be resolved by agreements between the organizations responsible for the respective 'Core Systems'.

For examples of typical activities, see 6.2.1.

5.2.2 Data distribution subsystem

The 'Data Distribution subsystem' needs to maintain a directory of system service recipients that want data and facilitates the delivery of that data to those service recipients. It supports multiple distribution mechanisms, including

— Source-to-Points: The data provider communicates data directly to data consumers. In this case, no data is sent to the 'Core System'; however, the 'Core System' is involved to check system user *permission*s and to provide addressing services through those subsystems, and

— Publish-Subscribe: The data provider communicates data to the 'Data Distribution subsystem', which forwards it to all service recipients that are subscribed to receive the data.

The 'Data Distribution subsystem' allows data consumers to specify (and change the specification of) data they wish to receive using criteria including

— data type,

— data quality characteristics,

— data format requirements,

— geographic area,

— sampling rate, and

— minimum and maximum frequency of data forwarding.

The 'Data Distribution subsystem' needs to maintain a *registry* (2.42) of which data consumers get what data according to the criteria defined above. Data distribution 'Publish-Subscribe' should not store or buffer data beyond that which is necessary to complete publish-subscribe actions.

NOTE This will have the consequence that if a given data consumer is unable to receive data that it has subscribed to because of a communications or other system failure, the data in question may be lost.

The degree to which data distribution buffering accommodates connectivity failures will be a function of the design of the 'Core System' deployment. Some 'Core Systems' may be designed to offer "temporary storage".

The 'Data Distribution subsystem' will need to *repackage* (2.41) data it receives from data providers, stripping away the source header information, and anonymizing the data, while maintaining the message payload. It then sends the repackaged payload data to subscribers of that data.

Acting within the limits of the privacy regulations of the jurisdiction, the 'Data Distribution subsystem' will need to securely retain a temporary archive linking the data to the data provider, in case *misbehaviour* (2.27) is reported (see 5.2.3).The duration of such data retention should be minimized as far as is practicable and subject to stringent access controls.

The 'Data Distribution subsystem' will also need to maintain source-to-points information. With this option, the data consumer will connect directly to the data provider with the address supplied by

the 'Data Distribution subsystem'. When connected, the data provider sends the data directly to each consumer, bypassing the 'Core System'. This shall be achieved within privacy regulations.

The 'Data Distribution subsystem' does not share or exchange data with other 'Core Systems'. System services recipients that require data from multiple 'Core Systems' need to subscribe to each 'Core system'.

For examples of typical activities, see 6.2.2.

5.2.3 Misbehaviour management subsystem

The '*misbehaviour* management subsystem' needs to analyse messages sent to the 'Core System' to identify service recipients operating outside of their assigned *permissions*. It will need to work with the 'user *permissions* subsystem' to identify suspicious requests and to maintain a record of specifically identifiable service recipients that

— provide false or misleading data,

— operate in such a fashion as to impede other service recipients, and

— operate outside of their authorized scope.

Because most end service recipients will rarely interface with the 'Core System', the '*misbehaviour* management subsystem' will also need to accept reports of misbehaving service recipients from other service recipients; *centre*, *mobile*, and field service recipients may send *misbehaviour reports* (2.29) that reference credentials attached to messages and note the type of *misbehaviour* in question. (Of course they will not usually be able to identify the source because it will have been anonymized).

The '*misbehaviour* management subsystem' will need to record such reports and according to a set of 'Core System' personnel-controlled rules, which will determine when to revoke credentials from such reported misbehaving service recipients (see 5.2.2). For anonymous service recipients, revocation is more complex and may result instead in a lack of credential renewal. Large numbers of failed renewals could have a significant effect on operations; system requirements and design activities will need to ensure that renewal failures do not adversely affect system performance or user experience.

For examples of typical activities, see 6.2.3.

5.2.4 Network services subsystem

The 'network services subsystem' provides information to system service recipients and 'Core System' services that enable communication between those service recipients and services. The 'network services subsystem' will provide the information necessary for service recipients to communicate with other service recipients who have given *permission* for such communication. The 'network services subsystem' will also need to provide the information necessary to enable service recipients to communicate with a group of service recipients by maintaining information regarding available communications methods, addresses, and performance characteristics for *geo-cast* (2.21) communications.

The 'network services subsystem' will also provide management for communications layer resources. It will enable decisions about which communications medium to use when more than one is available. This includes identifying available communications methods current performance characteristics and applicable user *permission* levels. *Permission* requirements will be coordinated with the 'user *permissions* subsystem' (see 5.2.7).

For examples of typical activities, see 6.2.4.

5.2.5 System service monitor subsystem

The 'system service monitor subsystem' will need to monitor the status of 'Core System' services, interfaces, and communications networks connected to the 'Core System'. It will have to inform system service recipients of the availability and status of its services.

The 'system service monitor subsystem' also needs to monitor the *integrity* (2.23) of internal 'Core System' components and supporting software, and mitigate against vulnerabilities. This will include periodic verification of the *authenticity* (2.5) of 'Core System' service software and supporting software. This will also include monitoring for vulnerabilities including but not limited to virus protection, network *port* (2.38) monitoring, and monitoring for patches to third-party components. Should a vulnerability be detected or a component of the 'Core System' be found to have lost *integrity*, the 'system service monitor subsystem' will need to take steps to mitigate against damage and performance degradation.

The 'system service monitor subsystem' will have to ensure the *physical security* (2.37) of 'Core System' services by monitoring the environmental conditions within which 'Core System' components operate (e.g. temperature and humidity), as well as the condition of its power system. The 'system service monitor subsystem' will need to take steps to mitigate against system failures in the event that environmental conditions exceed operating thresholds. Actions could include the activation of environmental or backup power systems and/or the modification of 'Core System' service operations, as well as '*core system' personnel* (2.12) ('Core System' staff) notification.

The 'system service monitor subsystem' also needs to monitor the performance of all services and interfaces and makes performance metrics available to 'core system' personnel ('Core System' staff).

For examples of typical activities, see 6.2.5.

The system service monitor subsystem monitors the status of 'Core System' services, interfaces, and communications networks connected to the 'Core System'. It informs system service recipients of the availability and status of its services.

The system service monitor also monitors the *integrity* of internal 'Core System' components and supporting software and mitigates against vulnerabilities. This includes periodic verification of the *authenticity* of core service software and supporting software. This also includes monitoring for vulnerabilities including but not limited to virus protection, network *port* monitoring, and monitoring for patches to third party components. Should a vulnerability be detected or a component of the 'Core System' found to have lost *integrity*, system service monitor takes steps to mitigate against damage and performance degradation.

5.2.6 Time synchronization subsystem

The 'time synchronization subsystem' will provide a common time base available to all system service recipients and make this time available to all 'Core System' services, which will use this time base whenever a time reference is required.

For examples of typical activities, see 6.2.6.

5.2.7 User permissions subsystem

The 'user *permission*s subsystem' will need to provide tools allowing system service recipients to verify whether a given user, identified by digital certificate-based credentials, is authorized to request or perform the action requested in the message payload. It also needs to maintain the status of service recipients, whether they have a specific account, their allowed behaviours with defined *permission*s (publish, subscribe, actions allowed to request, and administration, etc.), or if they belong to an anonymous group.

The 'user *permission*s subsystem' will need to provide the tools for 'Core System' personnel to create new service recipients and groups, modify existing service recipients and groups, and modify *permission*s associated with service recipients and groups.

For examples of typical activities, see 6.2.7.

5.2.8 User trust management subsystem

The 'user trust management subsystem' takes the task to manage access rules and credentials in an appropriate and internationally agreed form for all system service recipients and 'Core System'

components that require and are entitled to them. The 'user trust management subsystem' will create and distribute cryptographic keys to qualifying system service recipients. The 'user trust management subsystem' will need to work with the 'user *permissions* subsystem' (see 5.2.7) to determine whether a given user applying for credentials or keys is entitled to them.

The 'user trust management subsystem' also has to manage the revocation of credentials and the distribution of 'Certificate Revocation Lists' (CRLs) of disallowed credentials to interested system service recipients.

The provision, distribution, and management of appropriate digital certificates (both identity and *anonymous certificates* (2.2)) that are primarily used by *mobile* and field service recipients using wireless communications media (e.g. 5,9 GHz) will be managed by the 'user trust management subsystem' who will have to forward requests for certificate revocation for misbehaving system service recipients from '*misbehaviour* management' according to the regime it creates.

Some wireless communications media will be handled by an 'External Support System' (ESS). The user trust management subsystem will maintain a relationship with this ESS and provide information about how to contact this ESS to interested system service recipients.

The 'user trust management' subsystem will forward requests for certificate revocation for misbehaving system service recipients from the *misbehaviour* management subsystem to this ESS.

For examples of typical activities, see 6.2.8.

6 What are the key minimum system requirements and behaviour for core systems issues

6.1 Core system requirements

This section provides the high-level requirements for the 'Core System', i.e. "What the systems shall do". They are organized by the types of requirements and are related to the requirements identified in the ConOps (ISO/TR 17427-3).

Table 1 — Core system requirements

ID	Core System need	Description/Rationale	Priority	Subsystem(s)
1	Data protection	The 'Core System' needs to protect data it handles from unauthorized access. This is required to support *applications* that exchange sensitive information, such as personally identifying or financial information, which if intercepted could compromise the privacy or financial records of the user.	Essential	User trust management
2	Core trust	The 'Core System' needs to establish trust with its system service recipients. Such trust relationships are necessary so that the 'Core System' can be assured that system service recipients are who they say they are and therefore trust the source.	Essential	User trust management
3	System user trust	The 'Core System' needs to facilitate trust between system service recipients. Such trust relationships are necessary so that system service recipients can be assured that other system service recipients "are who they say they are," and therefore trust the source and data they receive from other system service recipients.	Essential	User trust management

Table 1 *(continued)*

ID	Core System need	Description/Rationale	Priority	Subsystem(s)
4	Core trust revocation	The 'Core System' needs to revoke the trust relationship it has with its system service recipients when necessary. A trusted system user may operate in a fashion that indicates it should no longer be trusted, in which case the 'Core System' shall have a way of revoking that trust.	Essential	*Misbehaviour* management, user trust management
5	System user trust revocation	The 'Core System' needs to facilitate the revocation of the trust relationships between system service recipients when necessary. A trusted system user may operate in a fashion that indicates it should no longer be trusted, in which case the 'Core System' shall have a way of facilitating revocation of trust between system service users.	Essential	*Misbehaviour* management, user trust management
6	*Authorization* Management	The 'Core System' needs to manage *authorization* mechanisms to define roles, responsibilities and *permissions* for system service recipients. This enables the 'Core System' to establish operational *environments* where different system service recipients may have different capabilities in terms of accessing *core services* and interacting with one another. For instance, some *mobile entities* may be authorized to request signal priority or some *centres* may be permitted to use the geographic broadcast service while those without those *permissions* would not.	Essential	User *permission*
7	*Authorization* Verification	The 'Core System' needs to verify that system service recipients and Core Operations Personnel are authorized to perform an attempted operation. This enables the 'Core System' to restrict operations to those service recipients who are permitted to use those operations. For example, geo-broadcast may be restricted to transportation or public safety agencies, so other service recipients may be prohibited from performing geo-broadcast.	Essential	User *permission*
8	*Misbehaviour* Management	The 'Core System' needs to identify system service recipients acting as *bad actors* (2.7). *Bad actors* are not necessarily malicious; they could be malfunctioning devices that may interfere with other system service recipients, communications layer systems or the 'Core System'. Identifying *bad actors* enables subsequent action to protect the *integrity* of all service recipients sharing the transportation *environment*.	Desirable	*Misbehaviour* Management
9	Time base	The 'Core System' needs to operate on a common time base. Coordination of time between the internal systems that operate the 'Core System' prevents internal synchronization errors and enables time-sensitive interactions with system service recipients.	Essential	Time synchronization

Table 1 *(continued)*

ID	Core System need	Description/Rationale	Priority	Subsystem(s)
10	Data request	The 'Core System' needs to provide a mechanism for data consumers to request data that is produced by data providers. This is a single request for a subscription to a certain type of dataand subsequent modification of the request to change data types or subscription parameters. Parameters include data frequency, type and location of where the data was generated. This enables the distribution of anonymously-provided data to interested data consumers, without requiring them to enter into a relationship with data providers. Request formats need to provide data consumers with the ability to differentiate and receive only the types of data they requested. For example, this includes data type, geographic range, frequency and sampling rate. This request method supports a wide variety of user needs, from planners requesting all traffic data all the time, to traveller information services requesting a subset of traffic data, to weather information services only interested in windshield wiper status for vehicles in a specific area.	Desirable	Data distribution
11	*Data provision* (2.14)	The 'Core System' needs to supply information to data providers enabling them to transmit data to interested data consumers. At a minimum, data characteristics need to include type, frequency and location where data was generated, so that service recipients that have requested data (see need data request) can differentiate between available data. This need enables data providers to direct the data they create to data consumers and serves as the provider-side corollary to the data request need. This supports a variety of *applications*, including those focused on the *centre* provision of data to service recipients. It also serves as the answer to the system user's question of "I have data, how do I provide it and to whom?"	Desirable	Data distribution
12	Data forward	The 'Core System' needs to provide a mechanism to distribute data that is produced by a system user acting as a data provider and requested by another system user. The 'Core System' needs to provide this distribution mechanism, rather than relying on individual provider-consumer relationships, because multiple consumers may want access to the same data. By having the 'Core System' distribute the data, system users are relieved of the need to transmit the data multiple times. Also, some data that could be critical to the proper functioning of mandatory *application*s, such as data supporting geo-location of service recipients (position corrections), time base data and roadway geometry data, all of which likely comes from a single source and needs to be distributed to large numbers of system service recipients. Additionally, system service recipients may interact over resource-constrained communication *link*s, so 'Core System' provided data redistribution reduces the potential load on those *link*s.	Desirable	Data distribution
13	Network connectivity	The 'Core System' needs to connect to the Internet. This allows the 'Core System' to provide services to any system user capable of connecting to the Internet.	Desirable	Network services

Table 1 *(continued)*

ID	Core System need	Description/Rationale	Priority	Subsystem(s)
14	Geographic broadcast	The 'Core System' needs to provide the information necessary for system service recipients who wish to communicate with a group of system service recipients in a specific area to do so. This capability enables system service recipients to target those in a specific area for information they wish to distribute without having to send individual messages to each recipient. Examples of *application*s that might use this include amber alerts, traffic information, and air quality alerts.	Desirable	Data distribution, network services
15	Core System service Status	The 'Core System' needs to be able to accept and maintain the status of 'Core System' services and provide accurate status information to system service recipients. Additionally, system service recipients may not be able to access a 'Core System' service (because of their location, for example) and would want to know where and when they could expect access to the service.	Desirable	System service monitor
16	System *integrity* Protection	The 'Core System' needs to protect the *integrity* of the 'Core System'. This includes defence against the loss of *integrity* from a deliberate attack, software bug, environmental or hardware failure, as well as mitigation strategies to facilitate a predictable return to normal operations. Protection and controlled restoration of normal operations ensures that system service recipients have a high confidence in the security of the information they entrust to the 'Core System'.	Essential	System service monitor
17	System availability	The 'Core System' needs to be available for system service recipients to access 'Core System' services. This ensures that system service recipients have a high confidence in the performance of the 'Core System' and can rely on its services to accomplish their objectives.	Essential	System service monitor
18	System operational Performance monitoring	The 'Core System' needs to monitor its performance. This includes the status of interfaces, services, and metrics for the number of requests and the resolution of those requests. Monitoring the performance of 'Core System' services and interfaces is necessary to understand when the system is operating properly and to gauge when the system may be nearing capacity so that action could be taken to prevent the system from failing to provide services, e.g. maximum number of transactions/second or internal communication bandwidth.	Essential	System service monitor
19	Core System Independence	The 'Core System' needs to be able to be independently deployed and operated providing 'Core System' services to all system service recipients within its jurisdictional scope. This ensures that one entity's 'Core System' deployment is not contingent on or dependent on another for basic *functionality*.	Essential	Core2Core, system service monitor, user *permission*, user trust management

Table 1 *(continued)*

ID	Core System need	Description/Rationale	Priority	Subsystem(s)
20	Core System Interoperability	The 'Core System' needs to provide services in such a way that if a *mobile* user moves into an area of another 'Core System', their interface to the 'Core System' still operates. This helps manage user expectations and helps ensure that when a *mobile* user subscribes to a service or installs an *application,* the user experience is consistent across multiple 'Core Systems'.	Essential	Core2Core, Data distribution, *misbehaviour* management,-network services, system service monitor, time synchronization, user trust management
21	Core System Interdependence	The 'Core System' needs to operate in coordination with other 'Core Systems'. This ensures that *core services* deliver information that is consistent with information delivered by other 'Core Systems', which will help avoid inconsistencies and incompatibilities between 'Core Systems' and between *mobile* service recipients interacting with multiple 'Core Systems'.	Essential	Core2Core, data distribution, *misbehaviour* management, network services, time synchronization, user trust management
22	Core System data Protection	The 'Core System' needs to protect data it maintains from unauthorized access. This ensures that information held by the 'Core System', which may include sensitive information about system service recipients, is accessed only by authorized service recipients.	Essential	System service monitor, user trust Management
23	*Anonymity* preservation	The 'Core System' needs to preserve the *anonymity* of anonymous system service recipients that use its services. This ensures that system service recipients communicating with the 'Core System' who wish to remain anonymous will not have their *anonymity* breached as a result of communicating with the 'Core System'.	Essential	User trust management
24	*Private network* Connectivity	The 'Core System' needs to be able to connect to a *private network*. This allows the 'Core System' to provide services to any system user that provides a *private network* connection to the 'Core System', which contributes to meeting deployability goals. It also allows 'Core Systems' to establish dedicated connections between them, which contributes to the 'Core Systems' collectively meeting goals of scalability, *maintainability* and reliability.	Essential	Network services
25	*Private network* routing	The 'Core System' needs to route communications between other 'Cores Systems' and system service recipients, when one or both of the parties involved in the communication is connected to the core by a *private network*. This enables system service recipients connected by *private network* to interact with *centre*-based *applications*, and also facilitates backup operations between cores.	Essential	Network services

6.2 Core System subsystem functional requirements

6.2.1 Core to Core subsystem requirements

See 5.2.1 for descriptive summary.

The following is an example of the types of requirements for the Core2Core subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.1.1 Setup

6.2.1.1.1 The Core2Core subsystem establishes persistent secure transmission connections to other 'Core Systems' when continuous exchange of messaging (e.g. 'backup data' and 'core service status' query) occurs between 'Core Systems'.

6.2.1.1.2 The Core2Core subsystem establishes session-oriented communication connections to other 'Core Systems' when message exchanges occur intermittently (e.g. 'ore status registration') between 'Core Systems'.

6.2.1.1.3 The Core2Core subsystem receives the 'Core System' distribution list from the system service monitor subsystem.

6.2.1.1.4 The Core2Core subsystem receives locally encrypted messages from the user trust subsystem.

6.2.1.2 Core configuration

6.2.1.2.1 A 'Core System' transmits its core configuration information to other 'Core Systems'.

6.2.1.2.2 A 'Core System' receives 'Core System' configuration information from other 'Core Systems'.

6.2.1.2.3 Upon receiving a core configuration from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.2.4 If a core configuration from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its core configuration records.

6.2.1.3 Registrations

6.2.1.3.1 A 'Core System' receives 'Core System' status registrations from other 'Core Systems'.

6.2.1.3.2 Upon receiving a status registration from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.3.3 If a status registration from another 'Core System' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its registration update.

6.2.1.3.4 A 'Core System' uses the contents of a 'Core System' status registration to update the contents in the service status distribution *catalogue* (2.8).

6.2.1.3.5 Upon accepting a valid 'Core System' status registration from other 'Core Systems', the Core2Core subsystem sends the Core ID, function to the 'User *permissions*' subsystem.

6.2.1.4 Service status query

6.2.1.4.1 A 'Core System' transmits its core service status query to other 'Core Systems'.

6.2.1.4.2 A 'Core System' receives a core service status query from other 'Core Systems'.

6.2.1.4.3 Upon receiving a core service status query request from another 'Core System', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.4.4 If a core service status query from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its status query request records.

6.2.1.4.5 A 'Core System' transmits its service status for 'Cores Systems' response to another 'Core System' upon request.

6.2.1.4.6 The Core2Core subsystem accepts the detailed service status from the system service monitor subsystem.

6.2.1.4.7 The Core2Core subsystem transmits the detailed service status to other 'Core Systems'.

6.2.1.4.8 The Core2Core subsystem sends its *operator* ID, function to the user *permission*s subsystem.

6.2.1.5 Misbehaviour

6.2.1.5.1 A 'Core System' transmits its C2C *misbehaviour report* to other 'Core Systems'.

6.2.1.5.2 A 'Core System' receives C2C *misbehaviour report*s from other 'Core Systems'.

6.2.1.5.3 Upon receiving a *misbehaviour report* from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.5.4 If a *misbehaviour report* from another 'Core System' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its *misbehaviour* records.

6.2.1.5.5 A 'Core System' uses the contents of a C2C *misbehaviour report* to update 'suspicious data' contents in a *misbehaviour report*s log.

6.2.1.6 Certification Revocation Lists (CRL)

6.2.1.6.1 A 'Core System' transmits its complete CRL to other 'Core Systems'.

6.2.1.6.2 A 'Core System' receives complete CRLs from other 'Core Systems'.

6.2.1.6.3 Upon receiving a CRL from another 'Core System', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.6.4 If a CRL from another 'Core System' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its CRL records.

6.2.1.6.5 A 'Core System' uses the contents of the complete CRL to update the contents in its CRL storage.

6.2.1.6.6 A 'Core System' transmits its CRL delta (2.15) updates (only the data that is new since the last block of data that was downloaded) to other 'Core Systems'.

6.2.1.6.7 A 'Core System' receives CRL delta updates from other 'Core Systems'.

6.2.1.6.8 Upon receiving a CRL delta from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.6.9 If a CRL delta from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its CRL delta records.

6.2.1.6.10 A 'Core System' uses the contents of the CRL deltas to update the contents in the CRL storage.

6.2.1.7 'Core System' conflict information

6.2.1.7.1 A 'Core System' transmits 'Core System' conflict information to other 'Core Systems'.

6.2.1.7.2 A 'Core System' receives 'Core System' conflict information from other 'Core Systems'.

6.2.1.7.3 Upon receiving 'Core System' conflict information from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.7.4 If 'Core System' conflict information from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its 'Core System' conflict information records.

6.2.1.8 Data request

6.2.1.8.1 The Core2Core subsystem transmits the data requests to other 'Core Systems'.

6.2.1.8.2 The Core2Core subsystem receives data requests from other 'Core Systems'.

6.2.1.8.3 Upon receiving a data request from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.8.4 If a data request from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its data request records.

6.2.1.9 Data backup

6.2.1.9.1 A 'Core System' transmits data backup requests to other 'Core Systems'.

6.2.1.9.2 A 'Core System' receives data backup requests from other 'Core Systems'.

6.2.1.9.3 Upon receiving a data backup request from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.9.4 If a data backup request from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its data backup records.

6.2.1.9.5 A 'Core System' uses the contents of data backup requests to update the contents in other 'Core System' data backups.

6.2.1.9.6 A 'Core System' transmits backup data to other 'Core Systems'.

6.2.1.9.7 A 'Core System' receives backup data from other 'Core Systems'.

6.2.1.9.8 Upon receiving backup data from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.9.9 If backup data from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its backup data records.

6.2.1.9.10 A 'Core System' uses the contents of backup data to update the data to be backed up contents in the backup other 'Core System' data.

6.2.1.10 Restore data

6.2.1.10.1 A 'Core System' transmits restore data to other 'Core Systems'.

6.2.1.10.2 A 'Core System' receives restore data from other 'Core Systems'.

6.2.1.10.3 Upon receiving restore data from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.10.4 If restore data from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its restore data records.

6.2.1.10.5 A 'Core System' uses the contents of restore data to update the contents of generic 'Core System' data store.

6.2.1.11 Takeover request

6.2.1.11.1 A 'Core System' transmits other 'Core System' takeover requests to other 'Core Systems'.

6.2.1.11.2 A 'Core System' receives core takeover requests from other 'Core Systems'.

6.2.1.11.3 Upon receiving a takeover request from other 'Core Systems', the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.1.11.4 If a takeover request from other 'Core Systems' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its takeover request process.

6.2.1.11.5 The accepted takeover request is processed in accordance with agreed takeover request procedures.

6.2.2 Data distribution subsystem requirements

See 5.2.2 for descriptive summary.

The following is an example of the types of requirements for the data distribution subsystem. It does not purport to be a full list, but is presented to identify important features and a direction of thinking for system analysis.

6.2.2.1 Data subscription request

6.2.2.1.1 A 'Core System' receives a data subscription request from data subscribers.

6.2.2.1.2 Upon receiving a data subscription request from a data subscriber, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.2.1.3 If a data subscription request from a data subscriber contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.2.1.4 A 'Core System' sends a data subscription confirmation information response to a data subscriber upon request.

6.2.2.1.5 A 'Core System' uses the contents of a data subscription request to update the contents in its data subscription *catalogue*.

6.2.3 Data provision request

6.2.3.1 A 'Core System' receives a *data provision* (2.14) request from a data provider.

6.2.3.2 Upon receiving a data provision request from a data provider, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.3.3 If a data provision request from a data provider contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.3.4 A 'Core System' transmits a data acceptance information response to a data provider upon request.

6.2.3.5 A 'Core System' uses the contents of a data provision request to update the contents in a data acceptance *catalogue*.

6.2.4 Geo-casts

6.2.4.1 A 'Core System' receives *geo-casts* message from system service recipients.

6.2.4.2 Upon receiving a *geo-casts* message from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.4.3 If a *geo-casts* message from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.4.4 A 'Core System' uses the contents of *geo-cast* messages to update the contents in a *geo-cast* message log.

6.2.5 Field node configuration

6.2.5.1 A 'Core System' receives a field *node* configuration information request from system service recipients.

6.2.5.2 Upon receiving a field *node* configuration information request from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.5.3 If a field *node* configuration information request from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.5.4 A 'Core System' uses the contents of field *node* configuration information to update the contents in a *geo-cast* device *catalogue*.

A 'Core System' sends the repackaged, addressed data to a data subscriber upon request.

6.2.6 Misbehaviour subsystem requirements

See 5.2.3 for descriptive summary.

The following is an example of the types of requirements for the *misbehaviour* management subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.6.1 A 'Core System' receives system user *misbehaviour report* from system service recipients.

6.2.6.2 Upon receiving a *misbehaviour report* from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.6.3 If a *misbehaviour report* from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.6.4 A 'Core System' uses the contents of system user *misbehaviour report*s to update the contents of a *misbehaviour report*s log.

6.2.6.5 A 'Core System' identifies misbehaving system service recipients.

6.2.6.6 A 'Core System' enables a privileged system *operator* to configure *misbehaviour* correlation processing.

6.2.6.7 A 'Core System' maintains *misbehaviour information* (2.28) in a *misbehaviour report*s log.

6.2.7 Networking services subsystem requirements

See 5.2.4 for descriptive summary.

The following is an example of the types of requirements for the networking services subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking and system analysis.

6.2.7.1 A 'Core System' receives the data from system service recipients (e.g. as any combination of digitally signed, secure and acknowledgement message).

6.2.7.2 Upon receiving data from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.7.3 If data from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.7.4 A 'Core System' sends data out to system service recipients (e.g. as any combination of digitally signed, secure and acknowledgement messages).

6.2.8 Network protocol

6.2.8.1 A 'Core System' supports IPv6.

6.2.8.2 A 'Core System' routes messages between networks for those system service recipients that are connected via a private *network* (2.39).

6.2.8.3 A 'Core System' installs intrusion detection software to identify suspicious network traffic.

6.2.8.4 A 'Core System' uses the contents of intrusion alerts to update the contents in a *misbehaviour report* log.

6.2.9 System service monitoring subsystem requirements

See 5.2.5 for descriptive summary.

The following is an example of the types of requirements for the system service monitoring subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.9.1 A 'Core System' manages its own system performance monitoring.

6.2.9.2 A 'Core System' manages its software configuration.

6.2.9.3 A 'Core System' manages its hardware configuration.

6.2.9.4 A 'Core System' manages its transitions between *states* (2.43).

6.2.9.5 A 'Core System's service *coverage area* (2.13) has to be configurable.

6.2.9.6 A 'Core System' provides message distribution based on its geographical location to system service recipients.

6.2.9.7 A 'Core System' receives system user status registrations from system service recipients.

6.2.9.8 Upon receiving system user status registrations from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.9.9 If a system user status registration from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.9.10 A 'Core System' uses the contents of backup data to replenish/refresh its data in the event of data file corruption.

6.2.9.11 Upon receiving service status queries from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.9.12 If a service status query from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.9.13 A 'Core System' transmits the service status response to a system user upon request.

6.2.9.14 A 'Core System' transmits the performance records to the 'Core Certification Authority' (CCA).

6.2.9.15 A 'Core System' receives requests from a privileged system *operator* to transition a 'Core System's' state.

6.2.9.16 Upon receiving a request from a privileged system *operator* to transition a 'Core System's' state, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.9.17 If a request from a privileged system *operator* to transition a 'Core System's' state contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.9.18 A 'Core System' maintains its state in an event log.

6.2.9.19 A 'Core System' receives requests from a privileged system *operator* to transition the *mode* of a 'Core System'.

6.2.9.20 Upon receiving a request from a privileged system *operator* to transition a 'Core System's' *mode*, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.9.21 If a request from a privileged system *operator* to transition the *mode* of a 'Core System' contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.9.22 A 'Core System' maintains its *mode* in an event log.

6.2.10 Time synchronization subsystem requirements

See 5.2.6 for descriptive summary.

The following is an example of the types of requirements for the time synchronization subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.10.1 A 'Core System' receives time messages from an external reference time source.

6.2.10.2 Upon receiving a time message from an external reference time source, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.10.3 If a time message from an external reference time source contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.10.4 The time synchronization subsystem sends the 'Time Local Form' to its 'Core subsystems' within an agreed time period (example: US suggested values are 10 ms. This is an example only and other countries may select different value ranges).

6.2.10.5 The 'Time Local Form' cannot be allowed to drift (lagging or leading in time) from the external time source standard time reference by more than an agreed amount of time variance (example: US suggested values are 1 second per year. This is an example only and other countries may select different value ranges).

6.2.10.6 The time synchronization subsystem may receive 'Restore Data' instruction from the Core2Core subsystem.

6.2.10.7 The time synchronization subsystem sends the *operator* ID, function to the user *permission*s subsystem.

6.2.10.8 The time synchronization subsystem receives the *permission* response from the user *permission*s subsystem.

6.2.10.9 The time synchronization subsystem receives locally encrypted message from the user trust subsystem.

6.2.10.10 The time synchronization subsystem provides 'Coordinated Universal Time' (UTC) to all 'Core System' subsystems.

6.2.11 State/Mode/Status requirements

6.2.11.1 The time synchronization subsystem accepts an operational changes message from a privilege system *operator*.

6.2.11.2 The time synchronization subsystem updates its state changes to its event log.

6.2.11.3 The time synchronization subsystem updates its actions to its event log.

6.2.11.4 The time synchronization subsystem updates its anomalies to its event log.

6.2.12 External interface requirements

6.2.12.1 The time synchronization subsystem establishes an interface to the national time reference standard (e.g. in US, Institute of Standards and Technology (NIST).

6.2.12.2 The time synchronization subsystem enables a privileged system *operator* to update the contents of the time system configuration data store.

6.2.12.3 The time synchronization subsystem enables a privileged system *operator* to update the contents of the 'Configure Time' synchronization.

6.2.13 User permission subsystem requirements

See 5.2.7 for descriptive summary.

The following is an example of the types of requirements for the user *permission* subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.13.1 A 'Core System' receives user identity and *permission* requests from system service recipients.

6.2.13.2 Upon receiving a user identity and *permission* request from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.13.3 If a user identity and *permission* request from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.13.4 A 'Core System' uses the contents of a user identity and *permission* request to update the contents in the user *permission registry*.

6.2.13.5 A 'Core System' transmits a user *permission* confirmation response to the system user.

6.2.13.6 A 'Core System' receives *application permission* requests from system service recipients.

6.2.13.7 Upon receiving an *application permission* request from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.13.8 If an *application permission* request from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.13.9 A 'Core System' transmits an *application permission* confirmation response to the system user.

6.2.13.10 A 'Core System' uses the contents of an *application permission* request to update the contents in its user *permission registry*.

6.2.14 User trust management requirements

See 5.2.8 for descriptive summary.

The following is an example of the types of requirements for the user trust subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.14.1 User permissions

6.2.14.1.1 A 'Core System' transmits user special *permission*s to an External Support System (ESS) registration authority (RA).

6.2.14.1.2 A 'Core System' receives user identifications from 'External Support System' (ESS) registration authority (RA).

7.2.14.1.3 Upon receiving a user identification from an ESS RA, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.14.1.4 If a user identifications from an ESS RA contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.14.2 Credential requests

6.2.14.2.1 A 'Core System' receives credential requests from system service recipients.

6.2.14.2.2 Upon receiving a credential request from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.14.2.3 If a credential request from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.14.2.4 A 'Core System' transmits credentials to a system user upon request.

6.2.14.2.5 A 'Core System' uses the contents of a credential request (for a certificate) to update the contents in its *application permission registry.*

6.2.14.2.6 A 'Core System' uses the contents of a credential request to update the contents in the user trust management configuration.

6.2.14.2.7 A 'Core System' transmits certificate requests to the 'External Support System' (ESS) Certificate Authority(ies)(CA).

6.2.14.3 Digital security certificates

6.2.14.3.1 A 'Core System' receives digital security certificates from an ESS CA.

6.2.14.3.2 Upon receiving the digital security certificates from an ESS CA, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.14.3.3 If the digital security certificate from an ESS CA contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.14.4 Encrypted messages

6.2.14.4.1 A 'Core System' receives remotely encrypted messages from a system service recipient.

6.2.14.4.2 Upon receiving a remotely encrypted message from a system service recipient, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.14.4.3 If a remotely encrypted message from a system service recipient contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.14.4.4 A 'Core System' transmits locally encrypted messages to system service recipients when the message is from a 'Core System'.

6.2.14.4.5 A 'Core System' receives CRLs from an 'External Support System' (ESS) Certificate Authority (CA).

6.2.14.4.6 Upon receiving CRLs from an ESS CA, the Core2Core subsystem ensures that its contents meet the acceptance criteria for all of its data objects.

6.2.14.4.7 If CRLs from an ESS CA contains a data item that the Core2Core subsystem determines as invalid, the Core2Core subsystem excludes that data item from its update of its records.

6.2.14.4.8 A 'Core System' uses the contents of CRLs to update the contents in its user trust management configuration.

6.2.14.4.9 A 'Core System' sends CRL messages to system service recipients.

6.2.14.4.10 A 'Core System' validates messages from system service recipients.

6.2.15 System performance subsystem requirements

The following is an example of the types of requirements for the system performance subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.15.1 A 'Core System' has to be available (i.e. able to provide all of its listed services while operating in normal *mode* in the *operational state* (2.33)) (example: US suggested values are 99.5 % of the time. This is an example only and other countries may select different value ranges).

6.2.16 System interface subsystem requirements

The following is an example of the types of requirements for the system interface subsystem. It does not purport to be a full list but is presented to identify important features and a direction of thinking for system analysis.

6.2.16.1 A 'Core System' communicates with other 'Core Systems'.

6.2.16.2 A 'Core System' communicates to system service recipients.

6.2.16.3 A 'Core System' communicates with its 'time' subsystem to receive time.

6.2.16.4 A 'Core System' communicates to a privileged system *operator.*

6.2.16.5 A 'Core System' connects to the Internet.

6.2.16.6 A 'Core System' connects to *private network*s.

6.2.16.7 A 'Core System' connects to the 'Core Certification Authority' (CCA).

6.3 Core system - other requirements

6.3.1 Physical security

Access control has to be provided in crucial areas such as the computer rooms, entrance rooms, electrical and mechanical areas. (Suggestion: as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers.)

6.3.2 Environmental features

6.3.2.1 The equipment hosting the 'Core System' operates when exposed to a defined relative humidity. (Example: US suggested values are from 40 % to 55 %, as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data *Centre*s. This is an example only and other countries may select different value ranges.)

6.3.2.2 The *facility* (2.19) hosting the 'Core System' *node*s operates within defined ambient temperature range. (Example: US suggested values are from 20 °C (68 °F) to 25 °C (77 °F), as specified in ANSI TIA-942. This is an example only and other countries may select different value ranges).

6.3.2.3 The *facility* hosting the 'Core System' *node*s operates up to a defined maximum dew point. (Example: US suggested values are 21 °C (69,8 °F), as specified in the ANSI TIA-942. This is an example only and other countries may select different value ranges.)

6.3.2.4 The *facility* hosting the 'Core System' *node*s maintains the temperature within a defined range. (Example: US suggested values are so that it does not vary by more than 5 °C (9 °F) per hour, as specified in ANSI TIA-942. This is an example only and other countries may select different value ranges.)

6.3.2.5 The *facility* hosting the 'Core System' *node*s needs to include heat and smoke detectors that meet or exceed all local fire code regulations.

6.3.3 Backup power

6.3.3.1 The *facility* hosting the 'Core System' *node*s needs to include supplemental power (suggested: generator or uninterruptible power supply (UPS)) as specified in IEEE Standard 446 Recommended Practice for Emergency and Standby Power System for Industrial and Commercial *Application*s).

6.3.3.4 The Core System's equipment needs to be installed in electrically grounded network equipment racks. (Example: US suggested values are as specified in the ANSI TIA-942 Telecommunications Infrastructure Standard for Data Centers. This is an example only and other countries may select different value ranges.)

6.3.4 Maintainability

A Core System's mean time to repair (MTTR) for each core service needs to be defined (example: US suggested values are not to exceed 3,0 h. This is an example only and other countries may select different value ranges).

A 'Core System' mean time between failures (MTBF) needs to be defined. (Example: US suggested values are 'should be greater than 600 h'. This is an example only and other countries may select different value ranges.)

6.3.5 Constraints

A 'Core System' shall conform to the privacy principles of the jurisdiction in which it is situated.

7 Internet-based communications standards

This section contains a listing of Internet Engineering Task Force (IETF) 'Request for Comments' (RFCs). These standards define how Internet communications systems are implemented. The 'Core System' implementations will need to be aware of the developments in this industry to ensure interoperable communications with external systems.

These tables provide the document number, title, date of the current publication, its development status and an indication of whether filing disclosures about Intellectual Property Rights (IPR).

Table 2 — IETF Network Time Protocol (NTP) standards

Document	Title	Date	Status
RFC 5905 (draft-ietf-ntp-ntpv4-proto)	Network Time Protocol Version 4: Protocol and Algorithms Specification	2010–06	RFC 5905 (proposed standard) Errata
RFC 5906 (draft-ietf-ntp-autokey)	Network Time Protocol Version 4: Autokey Specification	2010–06	RFC 5906 (informational)
RFC 5907 (draft-ietf-ntp-ntpv4-mib)	Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)	2010–06	RFC 5907 (proposed standard) Errata

Table 2 *(continued)*

Document	Title	Date	Status
RFC 5908 (draft-ietf-ntp-dhcpv6-ntp-opt)	Network Time Protocol (NTP) Server Option for DHCPv6	2010–06	RFC 5908 (proposed standard)

Source: http://datatracker.ietf.org/wg/ntp/

Table 3 — PKI X.509 standards

Document	Title	Date	Status	Ipr
Active Internet-Drafts				
draft-ietf-pkix-certimage-11	Internet X.509 *Public key* Infrastructure - Certificate Image	2011–02–15	RFC Ed Queue (for 55 days) RFC Editor State: RFC-EDITOR	
draft-ietf-pkix-eai-addresses-00	Internationalized Email Addresses in X.509 certificates	2011–03–07	I-D exists	
draft-ietf-pkix-ocspagility-10	Online Certificate Status Protocol Algorithm Agility	2011–03–11	RFC Ed Queue (for 27 days) RFC Editor State: EDIT	
draft-ietf-pkix-pubkey-caps-02	S/MIME Capabilities for *Public key* Definitions	2011–04–06 new	I-D exists	
draft-ietf-pkix-rfc2560bis-03	X.509 Internet *Public key* Infrastructure Online Certificate Status Protocol - OCSP	2011–04–05 new	I-D exists	
draft-ietf-pkix-rfc5272-bis-03	Certificate Management over CMS (CMC) Updates	2011–04–06 new	I-D exists	
draft-ietf-pkix-rfc5280- clarifications-02	Clarifications to the Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2011–03–28	I-D exists	
RFC 2459 (draft-ietf-pkix-ipki-part1)	Internet X.509 *Public key* Infrastructure Certificate and CRL Profile	1999–01	RFC 2459 (proposed standard) obsoleted by RFC 3280 Errata	
RFC 2510 (draft-ietf-pkix-ipki3cmp)	Internet X.509 *Public key* Infrastructure Certificate Management Protocols	1999–03	RFC 2510 (proposed standard) obsoleted by RFC 4210	
RFC 2511 (draft-ietf-pkix-crmf)	Internet X.509 Certificate Request Message Format	1999–03	RFC 2511 (proposed standard) obsoleted by RFC 4211	
RFC 2527 (draft-ietf-pkix-ipki-part4)	Internet X.509 *Public key* Infrastructure Certificate Policy and Certification Practices Framework	1999–03	RFC 2527 (informational) obsoleted by RFC 3647 Errata	
RFC 2528 (draft-ietf-pkix-ipki-kea)	Internet X.509 *Public key* Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 *Public key* Infrastructure Certificates	1999–03	RFC 2528 (informational)	
RFC 2559 (draft-ietf-pkix-ipki2opp)	Internet X.509 *Public key* Infrastructure Operational Protocols - LDAPv2	1999–04	RFC 2559 (historic) obsoleted by RFC 3494	

Table 3 *(continued)*

Document	Title	Date	Status	Ipr
RFC 2560 (draft-ietf-pkix-ocsp)	X.509 Internet *Public key* Infrastructure Online Certificate Status Protocol - OCSP	1999–06	RFC 2560 (proposed standard) Errata	
RFC 2585 (draft-ietf-pkix-opp-ftp-http)	Internet X.509 *Public key* Infrastructure Operational Protocols: FTP and HTTP	1999–05	RFC 2585 (proposed standard) Errata	
RFC 2587 (draft-ietf-pkix-ldapv2-schema)	Internet X.509 *Public key* Infrastructure LDAPv2 Schema	1999–06	RFC 2587 (proposed standard) obsoleted by RFC 4523	
RFC 2797 (draft-ietf-pkix-cmc)	Certificate Management Messages over CMS	2000–04	RFC 2797 (proposed standard) obsoleted by RFC 5272	
RFC 2875 (draft-ietf-pkix-dhpop)	Diffie-Hellman Proof-of-Possession Algorithms	2000–07	RFC 2875 (proposed standard)	
RFC 3029 (draft-ietf-pkix-dcs)	Internet X.509 *Public key* Infrastructure Data Validation and Certification Server Protocols	2001–02	RFC 3029 (experimental)	
RFC 3039 (draft-ietf-pkix-qc)	Internet X.509 *Public key* Infrastructure Qualified Certificates Profile	2001–01	RFC 3039 (proposed standard) obsoleted by RFC 3739	
RFC 3161 (draft-ietf-pkix-time-stamp)	Internet X.509 *Public key* Infrastructure Time-Stamp Protocol (TSP)	2001–08	RFC 3161 (proposed standard) updated by RFC 5816 Errata	
RFC 3279 (draft-ietf-pkix-ipki-pkalgs)	Algorithms and Identifiers for the Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002–04	RFC 3279 (proposed standard) updated by RFC 4055, RFC 4491, RFC 5480, RFC 5758 Errata	
RFC 3280 (draft-ietf-pkix-new-part1)	Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2002–04	RFC 3280 (proposed standard) obsoleted by RFC 5280 Updated by RFC 4325, RFC 4630 Errata	1
RFC 3281 (draft-ietf-pkix-ac509prof)	An Internet Attribute Certificate Profile for *Authorization*	2002–04	RFC 3281 (proposed standard) obsoleted by RFC 5755 Errata	
RFC 3379 (draft-ietf-pkix-dpv-dpd-req)	Delegated Path Validation and Delegated Path Discovery Protocol Requirements	2002–09	RFC 3379 (informational)	

Table 3 *(continued)*

Document	Title	Date	Status	Ipr
RFC 3628 (draft-ietf-pkix-pr-tsa)	Policy Requirements for Time- Stamping Authorities (TSAs)	2003–11	RFC 3628 (informational)	
RFC 3647 (draft-ietf-pkix-ipki-new-rfc2527)	Internet X.509 *Public key* Infrastructure Certificate Policy and Certification Practices Framework	2003–11	RFC 3647 (informational) Errata	
RFC 3709 (draft-ietf-pkix-logotypes)	Internet X.509 *Public key* Infrastructure: Logotypes in X.509 Certificates	2004–02	RFC 3709 (proposed standard) Errata	
RFC 3739 (draft-ietf-pkix-sonof3039)	Internet X.509 *Public key* Infrastructure: Qualified Certificates Profile	2004–03	RFC 3739 (proposed standard)	
RFC 3770 (draft-ietf-pkix-wlan-extns)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2004–05	RFC 3770 (proposed standard) obsoleted by RFC 4334 Errata	
RFC 3779 (draft-ietf-pkix-x509-ipad-dr-as- extn)	X.509 Extensions for IP Addresses and AS Identifiers	2004–06	RFC 3779 (proposed standard) Errata	
RFC 3820 (draft-ietf-pkix-proxy)	Internet X.509 *Public key* Infrastructure (PKI) Proxy Certificate Profile	2004–06	RFC 3820 (proposed standard)	
RFC 3874 (draft-ietf-pkix-sha224)	A 224-bit One-way Hash Function: SHA-224	2004–09	RFC 3874 (informational)	
RFC 4043 (draft-ietf-pkix-pi)	Internet X.509 *Public key* Infrastructure Permanent Identifier	2005–05	RFC 4043 (proposed standard) Errata	
RFC 4055 (draft-ietf-pkix-rsa-pkalgs)	Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2005–06	RFC 4055 (proposed standard) updated by RFC 5756 Errata	
RFC 4059 (draft-ietf-pkix-warranty-extn)	Internet X.509 *Public key* Infrastructure Warranty Certificate Extension	2005–05	RFC 4059 (informational)	
RFC 4158 (draft-ietf-pkix-certpathbuild)	Internet X.509 *Public key* Infrastructure: Certification Path Building	2005–09	RFC 4158 (informational)	
RFC 4210 (draft-ietf-pkix-rfc2510bis)	Internet X.509 *Public key* Infrastructure Certificate Management Protocol (CMP)	2005–09	RFC 4210 (proposed standard) Errata	
RFC 4211 (draft-ietf-pkix-rfc2511bis)	Internet X.509 *Public key* Infrastructure Certificate Request Message Format (CRMF)	2005–09	RFC 4211 (proposed standard) Errata	
RFC 4325 (draft-ietf-pkix-crlaia)	Internet X.509 *Public key* Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension	2005–12	RFC 4325 (proposed standard) obsoleted by RFC 5280	

Table 3 *(continued)*

Document	Title	Date	Status	Ipr
RFC 4334 (draft-ietf-pkix-rfc3770bis)	Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)	2006–02	RFC 4334 (proposed standard) Errata	
RFC 4386 (draft-ietf-pkix-pkixrep)	Internet X.509 *Public key* Infrastructure Repository Locator Service	2006–02	RFC 4386 (experimental)	
RFC 4387 (draft-ietf-pkix-certstore-http)	Internet X.509 *Public key* Infrastructure Operational Protocols: Certificate Store Access via HTTP	2006–02	RFC 4387 (proposed standard)	
RFC 4476 (draft-ietf-pkix-acpolicies-extn)	Attribute Certificate (AC) Policies Extension	2006–05	RFC 4476 (proposed standard)	
RFC 4491 (draft-ietf-pkix-gost-cppk)	Using the GOST R 34.10–94, GOST R 34.10–2001, and GOST R 34.11-94 Algorithms with the Internet X.509 *Public key* Infrastructure Certificate and CRL Profile	2006–05	RFC 4491 (proposed standard) Errata	
RFC 4630 (draft-ietf-pkix-cert-utf8)	Update to DirectoryString Processing in the Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2006–08	RFC 4630 (proposed standard) obsoleted by RFC 5280	
RFC 4683 (draft-ietf-pkix-sim)	Internet X.509 *Public key* Infrastructure Subject Identification Method (SIM)	2006–10	RFC 4683 (proposed standard) Errata	
RFC 4985 (draft-ietf-pkix-srvsan)	Internet X.509 *Public key* Infrastructure Subject Alternative Name for Expression of Service Name	2007–08	RFC 4985 (proposed standard) Errata	
RFC 5019 (draft-ietf-pkix-lightweight-ocsp-profile)	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume *Environments*	2007–09	RFC 5019 (Proposed Standard)	
RFC 5055 (draft-ietf-pkix-scvp)	Server-Based Certificate Validation Protocol (SCVP)	2007–12	RFC 5055 (proposed standard)	2
RFC 5272 (draft-ietf-pkix-2797-bis)	Certificate Management over CMS (CMC)	2008–06	RFC 5272 (proposed standard) Errata	
RFC 5273 (draft-ietf-pkix-cmc-trans)	Certificate Management over CMS (CMC): Transport Protocols	2008–06	RFC 5273 (proposed standard)	
RFC 5274 (draft-ietf-pkix-cmc-compl)	Certificate Management Messages over CMS (CMC): Compliance Requirements	2008–06	RFC 5274 (proposed standard)	
RFC 5280 (draft-ietf-pkix-rfc3280bis)	Internet X.509 *Public key* Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2008–05	RFC 5280 (proposed standard) Errata	
RFC 5480 (draft-ietf-pkix-ecc- subpub-keyinfo)	Elliptic Curve Cryptography Subject *Public key* Information	2009–03	RFC 5480 (proposed standard) Errata	

Table 3 *(continued)*

Document	Title	Date	Status	Ipr
RFC 5636 (draft-ietf-pkix-tac)	Traceable Anonymous Certificate	2009–08	RFC 5636 (experimental)	
RFC 5697 (draft-ietf-pkix-other-certs)	Other Certificates Extension	2009–11	RFC 5697 (experimental)	
RFC 5755 (draft-ietf-pkix-3281update)	An Internet Attribute Certificate Profile for *Authorization*	2010–01	RFC 5755 (proposed standard)	
RFC 5756 (draft-ietf-pkix-rfc4055-update)	Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters	2010–01	RFC 5756 (proposed standard) Errata	
RFC 5758 (draft-ietf-pkix-sha2-dsa-ecdsa)	Internet X.509 *Public key* Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA	2010–01	RFC 5758 (proposed standard) Errata	
RFC 5816 (draft-ietf-pkix-rfc3161-update)	ESSCertIDv2 Update for RFC 3161	2010–04	RFC 5816 (proposed standard)	
RFC 5877 (draft-ietf-pkix-attr-cert-mime- type)	The *application*/pkix-attr-cert Media Type for Attribute Certificates	2010–05	RFC 5877 (informational) Errata	
RFC 5912 (draft-ietf-pkix-new-asn1)	New ASN.1 Modules for the *Public key* Infrastructure Using X.509 (PKIX)	2010–06	RFC 5912 (informational) Errata	
RFC 5913 (draft-ietf-pkix- authoritycleranceconstraints)	Clearance Attribute and Authority Clearance Constraints Certificate Extension	2010–06	RFC 5913 (proposed standard)	
RFC 5914 (draft-ietf-pkix-ta-format)	Trust Anchor Format	2010–06	RFC 5914 (proposed standard) Errata	
RFC 5934 (draft-ietf-pkix-tamp)	Trust Anchor Management Protocol (TAMP)	2010–08	RFC 5934 (proposed standard) Errata	
RFC 6024 (draft-ietf-pkix-ta-mgmt-reqs)	Trust Anchor Management Requirements	2010–10	RFC 6024 (informational)	
RFC 6025 (draft-ietf-pkix-asn1-translation)	ASN.1 Translation	2010–10	RFC 6025 (informational)	
Active Internet-Drafts				
draft-chen-pkix-security-info-00	X.509 Extension with Security Information	2010–10–15 expires soon	I-D exists	
draft-moreau-pkix-aixcm-00	Auto Issued X.509 Certificate Mechanism (AIXCM)	2008–08–06	I-D exists RFC Editor State: ISR-AUTH	
draft-patterson-pkix-attribute- signing-eku-00	attributeSigning extendedKeyUsage value	2011–03–28	I-D exists	

Source: http://datatracker.ietf.org/wg/pkix/

8 Internal interfaces

The following table shows the internal interfaces between subsystems within a typical 'Core System'. The column on the left represents the subsystems that will be sending data to the subsystems represented by the columns to the right.

Table 4 — Internal subsystem to subsystem interfaces

	Receiving subsystems							
Sending subsystems	CC	DD	MM	NS	SM	TS	UP	UTM
Core2Core (CC)		y	y	y	y	y	y	y
Data Distribution (DD)	y		y	y	y		y	y
Misbehaviour Management (MM)	y				y		y	y
Network Services (NS)	y	y	y		y		y	y
System service monitor (SM)	y	y	y	y		y	y	y
Time Synchronization (TS)	y	y	y	y	y		y	y
User *Permissions* (UP)	y	y	y	y	y	y		y
User Trust Management (UTM)	y	y	y	y	y	y	y	

9 5,9 GHz security credential requirements

While only some *C-ITS* communications will use 5,9 GHz dedicated wireless communications, some of the critical *C-ITS* systems envisaged will use this wireless communications medium. This will need to be managed by the 'Certificate Authority'.

Bibliography

[1] ISO 17427-1, *Intelligent transport systems — Co-operative systems — Roles and responsibilities based on architecture(s)*

[2] ISO/TR 17427-2, *Intelligent transport systems — Cooperative ITS — Framework Overview*

[3] ISO/TR 17427-3, *Intelligent transport systems — Cooperative ITS — Concept of operations (CONOPS) for 'Core' systems*

[4] RITA: 'Core System'.System Requirements Specification (SyRS) http://www.its.dot.gov/docs/CoreSystem_SE_SyRS_RevF.pdf

[5] CVIS. 2010, www.cvisproject.org

[6] Cooperative ITS Regulatory Policy Issues. National Transport Commission, Australia

[7] C-ITS Policy Paper FINAL. National Transport Commission, Australia. Dec 2013

[8] Connected vehicle Technology. US DoT http://www.its.dot.gov/research/systems_engineering.htm

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™