October 2013

SDOs and Private Organizations

Contents

1 Smart grid standards 3

2 Smart standards on energy 4

3 Smart cards standards 5

4 WC3 standards 10

5 Wireless networking standards 12

6 Intelligent transport systems 16

1 Smart grid standards

IEEE

- **Overview**
  The IEEE's approach to the smart grid is to view it as a large 'System of Systems' wherein individual smart grid domains based on the NIST Smart Grid Conceptual Model are expanded into three layers:

1. Power and Energy
2. Communications
3. IT/Computer

The IEEE considers the Communications and IT/Computer layers to be enabling infrastructure for the Power and Energy layer

- **Standards**
  The IEEE works closely with NIST on its standards roadmap and conformance testing/certification framework for the smart grid. The organization also collaborates with other global standards bodies to effectively facilitate standards coordination and to ensure the intensifying smart grid movement's success.
  There are more than 100 standards that have been approved or in development relating to the smart grid. Among the broad number of systems and technologies addressed by these standards are broadband over power line, cyber security, distributed energy resources, Distributed Network Protocol (DNP3), and Greenhouse gas emissions credits, among others.

  *****Please see Annex A for an extensive list of IEEE standards on relating to smart grids*****

2 Smart standards on energy

EnergySMART

- **OpenADR** (Open Automated Demand Response) - Transforming the Smart Grid Through Standards
  Please see the following article for more information
  http://energysmart.enernoc.com/bid/334732/OpenADR-Transforming-the-Smart-Grid-Through-Standards

- **Energy Intelligence Software (EIS) –** energy intelligence dashboard
  Please see the following article for more information
  http://energysmart.enernoc.com/bid/322815/energy-intelligence-software-enables-better-energy-management

3 Smart cards standards

- ## Federal Information Processing Standard 201 – FIPS 201

  As a result of Homeland Security Presidential Directive 12 (HSPD-12), issued by former President George W. Bush on August 27, 2004, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, on February 25, 2005.

  FIPS 201 provides the specifications for a standard Federal smart ID card, called the PIV card, that must be used for both physical and logical access and can be used for other applications as determined by individual agencies. The PIV card is a smart card with both contact and contactless interfaces. Government agencies are currently implementing FIPS 201-compliant systems.

  NIST has also issued a number of special publications with additional specifications for PIV card implementations.

- ## Other Federal Information Processing Standards (FIPS)

  FIPS standards are developed by the Computer Security Division within NIST. FIPS standards are designed to protect federal computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.

  Digital Signatures

  - **FIPS 186-2** specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm.
  - **ANSI X9.31-1998** contains specifications for the RSA signature algorithm. The standard specifically covers both the manual and automated management of keying material using both asymmetric and symmetric key cryptography for the wholesale financial services industry.
  - **ANSI X9.62-1998** contains specifications for the ECDSA signature algorithm.

  Advanced Encryption Standards

  - **FIPS 197**: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.

  Security Requirements for Cryptographic Modules

  - **FIPS 140**: The security requirements contained in FIPS 140 (currently version 2) pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic

interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

- **GlobalPlatform**
  GlobalPlatform (GP) is an international, non-profit association. Its mission is to establish, maintain and drive the adoption of standards to enable an ***open and interoperable infrastructure*** for ***smart cards, devices and systems*** that simplifies and accelerates development, deployment and management of applications across industries.
  According to GlobalPlatform, as of 2009, an estimated 305.7 million GlobalPlatform-based smart cards had been deployed across the world, with an additional two billion ***GSM cards*** using GlobalPlatform technology for over-the-air (OTA) application download.

- **Common Criteria**
  Common Criteria (CC) is an internationally approved security evaluation framework providing a clear and reliable evaluation of the security capabilities of IT products, including secure ***ICs, smart card operating systems, and application software***.
  CC provides an independent assessment of a product's ability to meet security standards, with the goal of giving customers confidence in the security of IT products and leading to better decisions about security.
  Security-conscious customers, such as national governments, are increasingly requiring CC certification in making purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. CC has been adopted and is recognized by 14 countries.

- **International Civil Aviation Organization**
  The International Civil Aviation Organization (ICAO) is responsible for issuing guidance on the standardization and specifications for Machine Readable Travel Documents (MRTD) – i.e. passports, visas, and travel documents.
  ICAO published the specification for electronic passports that uses a ***contactless smart chip*** in the ***passport to securely store information*** on the passport holder's data page.

- **International Airline and Transportation Association (IATA)**
  The IATA develops standards for recommendation to the airline and transportation industry. IATA has formed a task force to develop interoperability standards for smart card-based ***ticketless travel***. Its mission is to ensure easy and convenient negotiation of electronic airline tickets.

- **G8 Health Standards**
  The G8 countries have come together to develop a standard format for populating data on a health card.
  This standard attempts to create interoperability across health cards from the G8 countries. It addresses ***file formats***, ***data placement*** on the card, and use of ***digital certificates in health care***.

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)**

This law states that the ***Secretary of Health and Human Services (HHS)*** is to adopt national standards for implementing a secure electronic health transaction system.
Examples of these transactions include: ***claims, enrolment, eligibility, payment, and coordination of benefits***.
The goal of HIPAA is to create a secure, cost-effective means for individuals to efficiently accomplish electronic health care transactions. HHS has designated the Centres for Medicare and Medicaid Services the responsible entity for enforcing HIPAA.

- ## Global System for Mobile Communication (GSM) Standards

The mobile phone industry has several telecommunications standards, but the predominant one globally is GSM.
The GSM standard uses smart cards called Subscriber Identity Modules (SIMs) that are configured with information essential to authenticating a GSM-compliant mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.
The GSM standard is managed by the ***European Telecommunication Standards Institute.***

*****See Annex B to Private and SDO Standards - GSM Standards*****

- ## EMV 2000

EMV is an open-standard set of specifications for smart card payments and acceptance devices. EMVCo, owned by American Express, JCB, MasterCard, and Visa, manages, maintains and enhances the EMV specifications, to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs.
The EMV standard initially started out as a terminal specification but has evolved to contain four books:

- ***Book 1, Application-Independent Integrated Circuit Card (ICC) to Terminal Interface Requirements***, describes the minimum functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability independent of the application to be used.
- ***Book 2, Security and Key Management***, describes the minimum security functionality required for integrated circuit cards and terminals to ensure correct operation and interoperability. Additional requirements and recommendations are provided on online communication between ICC and issuer and the management of cryptographic keys at terminal, issuer and payment system level.
- ***Book 3, Application Specification***, defines the terminal and integrated circuit card procedures necessary to effect a payment system transaction in an international interchange environment.
- ***Book 4, Cardholder, Attendant, and Acquirer Interface Requirements***, defines the mandatory, recommended, and optional terminal requirements necessary to support the acceptance of integrated circuit cards in accordance with Books 1, 2 and 310.

EMVCo is also active in developing specifications, requirements and approval processes for supporting contactless and mobile payments.

- ## Personal Computer/Smart Card (PC/SC) Workgroup

The PC/SC Workgroup, formed in 1996, included ***Schlumberger Electronic Transactions, Bull CP8, Hewlett-Packard, Microsoft***

This group has developed open specifications for integrating ***smart cards*** with personal computers. The specifications are platform-independent and based on existing industry standards. They are designed to enable application developers to create smart card-based secure network applications for ***banking, health care, corporate security, and electronic commerce.***
The specifications include cryptographic functionality and secure storage, programming interfaces for smart card readers and PCs, and a high-level application interface for application development. The specifications are based on the ***ISO/IEC 7816 standard*** and support ***EMV and GSM application standards***.

- ## OpenCard™ Framework

The OpenCard Framework is a set of guidelines announced by ***IBM, Netscape, NCI, and Sun Microsystems*** for integrating smart cards with network computers.
The guidelines are based on open standards and provide an architecture and a set of application program interfaces (APIs) that enable application developers and service providers to build and deploy smart card solutions on any OpenCard-compliant network computer. Through the use of a smart card, an OpenCard-compliant system will enable access to personalized data and services from any network computer and dynamically download from the Internet all device drivers that are necessary to communicate with the smart card.
By providing a high-level interface which can support multiple smart card types, the OpenCard Framework is intended to enable vendor-independent card interoperability.
The system incorporates Public Key Cryptography Standard (PKCS) - 11 and is expandable to include other public key mechanisms.

- ## APTA - American Public Transportation Association

The American Public Transportation Association (APTA) has published the ***Contactless Fare Media System (CFMS)*** **Standard** that provides a manual of standards and recommended practices for ***universal transit fare cards***.

- ## Java Card

Java Card provides a ***smart card*** operating system for running ***multiple applications***. The applicable Java Card specification is: Java Card 3.0.1 Platform Specification.

- ## ANSI-INCITS Biometric Standards

Many new secure ID system implementations are using both biometrics and smart cards to improve the security and privacy of the ID system.

- ***ANSI-INCITS 358-2002, BioAPI Specification*** - (ISO/IEC 19784-1). BioAPI is intended to provide a high-level generic biometric authentication model–one suited for any form of biometric technology. It covers the basic functions of enrolment, verification, and identification, and includes a database interface to allow a biometric service provider (BSP) to manage the technology device and identification population for optimum performance. It also provides primitives that allow the application to separately manage the capture of samples on a client workstation, and the enrolment, verification, and identification functions on a server. The BioAPI framework has been ported to Win32, Linux, UNIX, and WinCE. Note that BioAPI is not optimum for a microcontroller environment such as might be embedded within a door access control

reader unit or within a smart card processor. BioAPI is more suitable when there is a general-purpose computer available.

- *ANSI-INCITS 398, Common Biometric Exchange Formats Framework (CBEFF)* - (ISO/IEC 19785-1). The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies and exchange data in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. This specification is a revised (and augmented) version of the original CBEFF, the Common Biometric Exchange File Format, originally published as NISTIR 6529.

- *ANSI-INCITS Biometric Data Format Interchange Standards*. ANSI-INCITS has created a series of standards specifying the interchange format for the exchange of biometric data. These standards specify a data record interchange format for storing, recording, and transmitting the information from a biometric sample within a CBEFF data structure. The ANSI-INCITS published data interchange standards are shown below. The ISO equivalent standards for each are in process but not yet finalized.
  - **ANSI-INCITS 377-2004 - Finger Pattern Based Interchange Format**
  - **ANSI-INCITS 378-2004 - Finger Minutiae Format for Data Interchange**
  - **ANSI-INCITS 379-2004 - Iris Interchange Format**
  - **ANSI-INCITS 381-2004 - Finger Image Based Interchange Format**
  - **ANSI-INCITS 385-2004 - Face Recognition Format for Data Interchange**
  - **ANSI-INCITS 395-2005 - Signature/Sign Image Based Interchange Format**
  - **ANSI-INCITS 396-2004 - Hand Geometry Interchange Format**
  - **ISO/IEC 19794 series on biometric data interchange formats**:
    - Part 1 is the framework
    - Part 2 defines the finger minutiae data
    - Part 3 defines the finger pattern spectral data
    - Part 4 defines the finger image data
    - Part 5 defines the face image data
    - Part 6 defines the iris image data, and still in development
    - Part 7 will define the signature/sign time series data
    - Part 8 will define the finger pattern skeletal data and Part 8 will define the vascular image data.

4 WC3 standards

• Government Linked Data

Completed Work

2013-08-01	Asset Description Metadata Schema (ADMS)
2013-08-01	Registered Organization Vocabulary
2013-06-27	Linked Data Glossary

Drafts

2013-09-24	Internationalization Tag Set (ITS) Version 2.0
2013-08-01	Data Catalog Vocabulary (DCAT)
2013-06-25	The RDF Data Cube Vocabulary
2013-06-25	The Organization Ontology
2012-04-05	Terms for describing people

• e-Government

Completed Work

2013-06-27	Linked Data Glossary
2009-05-12	Improving Access to Government through Better Use of the Web

Drafts

2013-09-24	Internationalization Tag Set (ITS) Version 2.0
2013-08-01	Data Catalog Vocabulary (DCAT)
2013-06-25	The RDF Data Cube Vocabulary
2013-06-25	The Organization Ontology
2012-04-05	Terms for describing people
2009-09-08	Publishing Open Government Data

• Health Care and Life Sciences (Semantic Web)

Completed Work

2013-06-27	Linked Data Glossary
2011-10-20	Ontology of Rhetorical Blocks (ORB)
2009-10-20	SIOC, SIOC Types and Health Care and Life Sciences
2009-10-20	Semantic Web Applications in Neuromedicine (SWAN) Ontology
2009-10-20	SWAN/SIOC: Alignment Between the SWAN and SIOC Ontologies
2008-06-04	A Prototype Knowledge Base for the Life Sciences
2008-06-04	Experiences with the conversion of SenseLab databases to RDF/OWL

- ## Web Real Time Communication

Drafts

2013-09-10	WebRTC 1.0: Real-time Communication Between Browsers
2013-09-03	Media Capture and Streams
2013-07-09	Mediastream Image Capture
2013-02-05	MediaStream Recording
2012-03-06	MediaStream Capture Scenarios

5 Wireless networking standards

The following wireless networking standards chart give a quick overview of which main standards there are available.

Standard	Data Rate	Modulation Scheme	Security	Info
IEEE 802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered 'Wi-Fi Certified.' Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered 'Wi-Fi Certified.' Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered 'Wi-Fi Certified.' May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11

				of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.16 (WiMAX)	Specifies WiMAX in the 10 to 66 GHz range	OFDM	DES3 and AES	Commonly referred to as WiMAX or less commonly as WirelessMAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)
IEEE 802.16a (WiMAX)	Added support for the 2 to 11 GHz range.	OFDM	DES3 and AES	Commonly referred to as WiMAX or less commonly as WirelessMAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)
Bluetooth	Up to 2Mbps in the 2.45GHz band	FHSS	PPTP, SSL or VPN	No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals.
HomeRF	Up to 10Mbps in the 2.4GHZ band	FHSS	Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm.	Note: HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 150 feet from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation.
HiperLAN/1 (Europe)	Up to 20Mbps in the 5GHz band	CSMA/CA	Per-session encryption and individual authentication.	Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth.

HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band	OFDM	Strong security features with support for individual authentication and per-session encryption keys.	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.
OpenAir	Pre-802.11 protocol, using Frequency Hopping and 0.8 and 1.6 Mb/s bit rate	CSMA/CA with MAC retransmissions	OpenAir doesn't implement any encryption at the MAC layer, but generates Network ID based on a password (Security ID)	OpenAir is the proprietary protocol from Proxim. All OpenAir products are based on Proxim's module.

- ## ZigBee Network Standards

ZigBee is a specification for a suite of high-level communication protocols used to create personal area ***networks*** built from small, low-power ***digital radios***. ZigBee is based on an ***IEEE 802.15 standard.*** Though low-powered, ZigBee devices often transmit data over longer distances by passing data through intermediate devices to reach more distant ones, creating a mesh network; i.e. a network with no centralized control or high-power transmitter/receiver able to reach all of the networked devices. The decentralized nature of such ***wireless*** ad hoc ***networks*** make them suitable for applications where a central node can't be relied upon.

ZigBee is used in applications that require a low data rate, long battery life, and secure networking. ZigBee has a defined rate of 250 kbit/s, best suited for periodic or intermittent data or a single signal transmission from a sensor or input device. Applications include wireless light switches, electrical meters with in-home-displays, traffic management systems, and other consumer and industrial equipment that requires short-range wireless transfer of data at relatively low rates. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other ***WPANs***, such as ***Bluetooth*** or ***Wi-Fi.***

ZigBee networks are secured by 128 bit symmetric encryption keys. In home automation applications, transmission distances range from 10 to 100 meters line-of-sight, depending on power output and environmental characteristics.

ZigBee was conceived in 1998, standardized in 2003 and revised in 2006.

Areas covered:

- **Building Automation** (Efficient commercial spaces)
- **Remote Control** (Advanced remote controls)
- **Smart Energy** (Home energy savings)
- **Smart Energy Profile 2** (IP-based home energy management)

- **Health Care** (Health and fitness monitoring)
- **Home Automation** (Smart homes)
- **Input Device** (Easy-to-use touchpads, mice, keyboards, wands)
- **Light Link** (LED lighting control)
- **Retail Services** (Smarter shopping)
- **Telecom Services** (Value-added services)

6 Intelligent transport systems

Intelligent Transport Systems (ITS) include telematics and all types of communications in vehicles, between vehicles (e.g. car-to-car), and between vehicles and fixed locations (e.g. car-to-infrastructure). However, ITS are not restricted to Road Transport - they also include the use of information and communication technologies (ICT) for rail, water and air transport, including navigation systems.

In general, the various types of ITS rely on radio services for communication and use specialized technologies.

- **Automotive systems**

  Currently, there are currently the following projects related to automotive ITS:

  - ***Dedicated Short-Range Communications (DSRC)*** provide communications between the vehicle and the roadside in specific locations (for example toll plazas). Applications such as Electronic Fee Collection (EFC) will operate over DSRC.
  - ***Wireless Communications Systems dedicated to Intelligent Transport Systems and Road Transport and Traffic Telematics*** will provide network connectivity to vehicles and interconnect them. Using radio bands requires adequate Harmonized Standards which are under development for the bands 5 GHz and 63 GHz.
  - ***Continuous Air interface Long and Medium range (CALM)*** provides continuous communications between a vehicle and the roadside using a variety of communication media, including cellular, 5 GHz, 63 GHz and infra-red links. CALM will provide a range of applications, including vehicle safety and information, as well as entertainment for driver and passengers.

  These technological projects form part of wider initiatives on matters such as road safety (for example the European Commission's eSafety initiative) and road tolling.

- **Railway systems**

  The railways industries have agreed to use ***GSM*** for the signalling on high speed railways, as well as for conventional railways when interoperating across national borders. Within Europe, interoperability of high-speed railways is a regulatory requirement, addressed by the European Commission's Directive 96/48/EC.

- **Aeronautical and maritime systems**

  Aeronautical applications extend from professional services, such as air traffic control systems, to services for passengers, such as onboard telephony, and ETSI is responsible for specifying many of them.

Maritime applications support routine maritime operations, including navigation, as well as safety purposes. ETSI is responsible for producing a range of technical standards and reports concerning radio equipment and system for maritime and inland waterways use.

Dowload the ITS Technology Leaflet
Download the Cooperative ITS Technology Leaflet

- **ETSI Standards** (Harmonized European Standards)

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

They are officially recognized by the European Union as a European Standards Organization. The high quality of their work and their open approach to standardization has helped them evolve into a European roots.

ETSI is a not-for-profit organization with more than 700 ETSI member organizations drawn from 62 countries across 5 continents worldwide.

Please see below a list of ETSI standards on Intelligent Transport Systems:

Standard No.	Standard title.
EN 302 571	Intelligent Transport Systems (ITS); Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
TS 101 539-1	Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification
TS 102 869-1	Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
TS 102 869-2	Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 2: Test Suite Structure and Test Purposes (TSS&TP)

TS 102 869-3	Intelligent Transport Systems (ITS); Testing; Conformance test specification for Decentralized Environmental Notification Messages (DENM); Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
TS 102 894-1	Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications
TS 102 894-2	Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary
TS 103 096-1	Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 1: Protocol Implementation Conformance Statement (PICS)
TS 103 096-2	Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 2: Test Suite Structure and Test Purposes (TSS&TP)
TS 103 096-3	Intelligent Transport Systems (ITS); Testing; Conformance test specification for TS 102 867 and TS 102 941; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)
EN 302 663	Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band
ES 200 674-1	Intelligent Transport Systems (ITS); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communications (DSRC); Part 1: Technical characteristics and test methods for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band
TR 101 607	Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1
TS 103 097	Intelligent Transport Systems (ITS); Security; Security header and certificate formats

TS 102 708-2-1	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification
TS 102 708-2-2	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-Part 2: Test Suite Structure and Test Purposes (TSS&TP)
TS 102 708-2-3	Intelligent Transport Systems (ITS); RTTT; Test specifications for High Data Rate (HDR) data transmission equipment operating in the 5,8 GHz ISM band; Part 2: Application Layer; Sub-part 3: Abstract Test Suite (ATS) and partial PIXIT proforma
TR 102 965	Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list
TS 102 917-1	Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 1: Protocol Implementation Conformance Statement (PICS)
TS 102 917-2	Intelligent Transport Systems (ITS); Test specifications for the channel congestion control algorithms operating in the 5,9 GHz range; Part 2: Test Suite Structure and Test Purposes (TSS & TP)