# Template for collection of Data related to the Internet of Things

This template is used to collect data for an all-encompassing spreadsheet on standards related to the Internet of Things. The goal is to include all standards from all Standards Development Organizations that can possibly relate to the IoT. The top of the spreadsheet is locked and contains the column titles, some possible entries for several of the columns and some examples of data entered into the spreadsheet. You are NOT restricted to the suggested entries. If you feel that there is an ambiguity in your entry please feel free to provide extra information.

| **Title of Deliverable** | **Scope of deliverable** | **SDO** | **Current Status** | **Target Date** | **Type of Deliverable** | **Technology Domain** | **Specific Technology** | **Application Domain** | **Issues** | |
|---|---|---|---|---|---|---|---|---|---|---|
| *Possible Entries for this column* | *From the document* | *Possible Entries for this column* | *Possible Entries for this column* | | *Possible Entries for this column* | *Possible Entries for this column* | *Possible Entries for this column* | *Possible Entries for this column* | | |
| Standard | | ANSI | Published | | Technology | Localization and Tracking | RFID | Water monitoring | | |
| Technical report | | ISO | CD | | Conformance Testing | Communications and Networking | QR Code | Power grid conditioning | | |
| Recommendation | | IEC | Recommendation | | Interoperability Testing | Applications | 6LoWPAN | Retail goods tracking | | |
| RFC | | AIM | | | Performance | Processing/Computing | CDMA | Building facilities monitoring | | |
| | | ITU-T | | | | Security, Privacy, and Authentication | GSM | Accessibility | | |
| | | | | | | Data Structure/Formats | | | | |
| | | | | | | Data Carrier | | | | |
| | | | | | | etc. | etc. | etc. | | |

## Enter Real Data Below

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Release 10 features for Machine Type Communication | Section 4.2 of Release 10 document in the following link:<br>http://www.3gpp.org/ftp/Information/WORK_PLAN/<br>Description_Releases/ | 3GPP | Completed | | | M2M | | | | 1. |
| Release 11 features for Machine Type Communication | Section 4.2 of Release 11 document in the following link:<br>http://www.3gpp.org/ftp/Information/WORK_PLAN/<br>Description_Releases/ | 3GPP | Completed | | | M2M | | | | 2. |
| Release 12 features for Machine Type Communication | Work currently in Progress | 3GPP | In progress | | | M2M | | | | 3. |
| EN 12323:2005 - AIDC technologies - Symbology specifications - Code 16K | This document:<br>- specifies the requirements for the multi row bar code symbology known as "Code 16K";<br>- specifies "Code 16K" symbology characteristics, data character encodation, dimensions, tolerances, decoding algorithms and user-defined application parameters;<br>- describes a subset of "Code 16K" assigned to EAN International. | CEN TC | Published | | | AIDC | | | | 4. |
| EN 1556:1998 - Bar coding - Terminology | This European Standard defines a number of technical and other terms applicable to bar code technology, which are used in the standards produced by CEN TC225 and may be encountered elsewhere in bar coding standards produced by other organisations. Definitions given are in the context of bar coding and the terms so defined may customarily have a wider meaning than that shown in this Standard. Translations of the terms defined into the t w o other official languages of CEN are also shown to facilitate cross-reference. | CEN TC | Published | | | AIDC | | | | 5. |
| EN 1573:1996 - Bar coding - Multi-industry transport label | This European Standard<br>- specifies the general requirements for the design of bar coded transport labels for use by a wide range of industries;<br>- provides for traceability of transported units by automatic access via a 'license plate' printed in bar code and supplemented where necessary by other identified data presented both in bar code and human readable form. | CEN TC | Published | Revision started 11-2011 | | AIDC | | | | 6. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | - provides a choice of bar code symbologies;<br>- specifies quality requirements, classes of bar code density;<br>- gives recommendations as to label material, size and the inclusion of free text and any appropriate graphics. | | | | | | | | | |
| EN 1649:2004 - AIDC technologies - Operational aspects affecting the reading of bar code symbols | This document specifies the operational aspects affecting the reading of bar code symbols which must be considered in the preparation of application standards. It defines the subjects which must be addressed by application standards if they are to provide practical guidance to the user industries for whose use they are developed. | CEN TC | Published | | | AIDC | | | | 7. |
| EN 606:2004 - Bar coding - Transport and handling labels for steel products | This document specifies the requirements for labels containing human readable and bar coded information for fixing to steel products for the purpose of despatch, transport, and reception in accordance with the requirements of ISO 15394. Data elements are specified together with their status, location on the label, the appropriate data identifier and choice of bar code symbology. | CEN TC | Published | | | AIDC | | | | 8. |
| EN 841:1995 - Bar coding - Symbology specifications - Format Description | This standard<br>- specifies the format for bar code symbology specifications.<br>- specifies the characteristics of the symbology which need to be defined.<br>The standard is applicable as the basis for European Standards for bar code symbologies. | CEN TC | Published | | | AIDC | | | | 9. |
| Application Levels Events (ALE) | This standard specifies an interface through which clients may obtain filtered, consolidated Electronic Product Code™ (EPC) data from a variety of sources | GS1 | Version 1.1,1, March 2009 | | Technology | Reader | RFID | | | 10. |
| Core Business Vocabulary (CBV) | The Core Business Vocabulary Standard is to specifies various vocabulary elements and their values for use in conjunction with the EPCIS standard, which defines mechanisms to exchange information both within and across company boundaries. The vocabulary identifiers and definitions in this standard will ensure that all parties who exchange EPCIS data using the Core Business Vocabulary will have a common understanding of the semantic meaning of that data. | GS1 | Version 1.0, October 2010 | | Application Standard | Communications and Networking | | | | 11. |
| Discovery, Configuration, and Initialization (DCI) for Reader Operations | This GS1 EPCglobal standard specifies an interface between RFID Readers and Access Controllers and the network on which they operate. The purpose of this document is to specify the necessary and optional operations of a Reader and Client that allow them to utilize the network to which they are connected to communicate with other devices, exchange configuration information, and initialize the operation of each Reader, so that the Reader Operations Protocols can be used to control the operation of the Readers to provide tag and other information to the Client | GS1 | Version 1.0, June 2009 | | Technology | Reader | RFID | | | 12. |
| EPC Infomation Services (EPCIS) | The goal of EPCIS is to enable disparate applications to leverage Electronic Product Code (EPC) data via EPC-related data sharing, both within and across enterprises. Ultimately, this sharing is aimed at enabling participants in the EPCglobal Network to gain a shared view of the disposition of EPC-bearing objects within a relevant business context. | GS1 | Version 1.0.1, September 2007 | | Technology | Communications and Networking | | | | 13. |
| GS1 EPC Tag Data Standard | The Tag Data Standard covers two broad areas:<br>- The specification of the Electronic Product Code, including its representation at various levels of the EPCglobal Architecture and its correspondence to GS1 keys and other existing codes<br>- The specification of data that is carried on Gen 2 RFID tags, including the EPC, "user memory" data, control information, and tag manufacture information | GS1 | Version 1.7, May 2013 | | Technology | Data Structure/Formats | Data exchange, RFID | Visibility | | 14. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| GS1 EPC Tag Data Translation | Provides in machine-readable form all of the rules that define how to translate between EPC encodings defined by the EPC Tag Data Standard. | GS1 | Version 1.6, October 2011 | | Technology | Data Structure/Formats | Data exchange, RFID | Visibility | | 15. |
| GS1 General Specifications | Core GS1 standard reference for:<br>- GS1 identifications keys definitions<br>- Application Identifers<br>- Linear and 2D bar codes: EAN/UPC, ITF-14, GS1-128, GS1 DataBar, DGS1 DataMatrix, Composite bar codes, GS1 QR Code<br>- Application standards using GS1 standard data and bar code technologies | GS1 | Version 13.1, July 2013 | | Technology and applications | Applications | Identification, Linear and 2D bar codes | Supply chain | | 16. |
| GS1 HF Class 1 | The HF Class 1 Air Interface specifies the air interface for passive RFID Tags operating in the 13.56MHz radio frequency band, with functionality comparable to UHF Class 1 Gen 2 tags | GS1 | Version 2.0.3, September 2011 | | Technology | Data Carrier | RFID | | | 17. |
| GS1 System Landscape | This document provides a comprehensive inventory of the GS1 standards and catalogues and classifies them into topic areas. | GS1 | Published | February 2011 | | Supply chain | | | | 18. |
| GS1 UHF Class 1 Gen 2 | The UHF Class 1 Gen 2 Air Interface (often referred to simply as "Gen 2") specifies the air interface for passive RFID Tags operating in the 860 MHz – 960 MHz radio frequency band, with functionality as specified for "Class 1" tags in Section 4.2.1, above. This standard is maintained in synchrony with ISO/IEC 18000-63 | GS1 | Version 1.2.0, October 2008 | | Technology | Data Carrier | RFID | | | 19. |
| Low level reader protocol (LLRP) | This document specifies an interface between RFID Readers and Clients. The interface protocol is called low-level because it provides control of RFID air protocol operation timing and access to air protocol command parameters. The design of this interface recognizes that in some RFID systems, there is a requirement for explicit knowledge of RFID air protocols and the ability to control Readers that implement RFID air protocol communications. It also recognizes that coupling control to the physical layers of an RFID infrastructure may be useful for the purpose of mitigating RFID interference. | GS1 | Version 1.1, October 2010 | | Technology | Reader | RFID | | | 20. |
| Object Name Service (ONS) | ONS specifies how the Domain Name System is used to locate authoritative metadata and services associated with a given Electronic Product Code™ (EPC). | GS1 | Version 2.0.1, January 2013 | | Technology | Communications and Networking | | | | 21. |
| Reader Management (RM) | Protocol used by management software to monitor the operating status and health of EPCglobal compliant RFID Readers | GS1 | Version 1.0.1, May 2007 | | Technology | Reader | RFID | | | 22. |
| Analysis of an Equal-Cost Multi-Path Algorithm | Equal-cost multi-path (ECMP) is a routing technique for routing packets along multiple paths of equal cost.The forwarding engine identifies paths by next-hop. When forwarding a packet the router must decide which next-hop (path) to use. This document gives an analysis of one method for making that decision. | IETF | RFC 2992 (Informational) | 2000-11 | Informational | network level | Routing | | | 23. |
| Babel Hashed Message Authentication Code (HMAC) Cryptographic Authentication | This document describes a cryptographic authentication mechanism for the Babel routing protocol. This document updates RFC 6126. The mechanism allocates two new TLV types for the authentication data, uses Hashed Message Authentication Code (HMAC), and is both optional and backward compatible. | IETF | RFC 7298 (Experimental) | 2014-07 | Experimental | network level | Internetwork | | | 24. |
| Cisco Hot Standby Router Protocol (HSRP) | The memo specifies the Hot Standby Router Protocol (HSRP).The protocol insures that one and only one of the routers is forwarding packets on behalf of the virtual router. End hosts forward their packets to the virtual router. | IETF | RFC 2281 (Informational) | 1998-03 | Informational | network level | Routing | | | 25. |
| Distance Vector Multicast Routing Protocol | This RFC describes a distance-vector-style routing protocol for routing multicast datagrams through an internet. It is derived from the Routing Information Protocol (RIP) , and implements multicasting as described in RFC-1054. | IETF | RFC 1075 (Experimental) | 1998-11 | Experimental | network level | Routing | | | 26. |
| EXTERIOR GATEWAY PROTOCOL (EGP) | EGP is enable one or more autonomous systems to be used as transport media for traffic originating in some other autonomous system a | IETF | RFC 827 | 1982-10 | Unknown | network level | Internetwork | | | 27. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | destined for yet another. It was proposed in RFC 827 which was updated by RFC904. | | (Unknown) | | | | | | | |
| Exterior Gateway Protocol formal specification | This document updates RFCs 827 and 888. This RFC specifies a standard for the DARPA community. Interactions between gateways of different autonomous systems in the ARPA-Internet must follow this protocol. | IETF | RFC 904 (Historic) | 1984-04 | Historic | network level | Internetwork | | | 28. |
| IPv4 Address Behaviour Today | The main purpose of this note RFC2101 is to clarify the current interpretation of the 32-bit IP version 4 address space | IETF | RFC 2101 (Informational) | 1997-02 | Informational | network level | Addressing | | | 29. |
| Reserved IPv6 Interface Identifier for Proxy Mobile IPv6 | This document attempts to simplify this operational requirement by making a reservation for special addresses that can be used for this purpose. This document also updates RFC 5213. | IETF | RFC 6543 (Proposed Standard) | 2012-03 | Proposed Standard | network level | Mobility | | | 30. |
| Special-Purpose IP Address Registries | This memo reiterates the assignment of an IPv4 address block (192.0.0.0/24) to IANA, The RFC 6890 obsoletes RFC 4773, RFC 5156, RFC 5735, RFC 5736 | IETF | RFC 6890 (Best Current Practice) | 2013-04 | Best Current Practice | network level | Addressing | | | 31. |
| Special-Use Domain Names | This document describes what it means to say that a Domain Name (DNS name) is reserved for special use, when reserving such a name is appropriate, and the procedure for doing so. It establishes an IANA registry for such domain names, and seeds it with entries for some of the already established special domain names. | IETF | RFC 6761 (Proposed Standard) | 2013-02 | Proposed Standard | network level | Addressing | | | 32. |
| 6LoWPAN-GHC: Generic Header Compression for IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs) | RFC 6282 defines header compression in 6LoWPAN packets (where"6LoWPAN" refers to "IPv6 over Low-Power Wireless Personal Area Network"). The present document specifies a simple addition that enables the compression of generic headers and header-like payloads, without a need to define a new header compression scheme for each such new header or header-like payload. | IETF 6lo | RFC 7400 (Proposed Standard) | 2014-11-14 | Proposed Standard | network level | 6LoWPAN | | | 33. |
| Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) | This document defines a portion of the Management Information Base(MIB) for use with network management protocols in the Internet community. In particular, it defines objects for managing IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) | IETF 6lo | RFC 7388 (Proposed Standard) | 2014-10-30 | Proposed Standard | network level | 6LoWPAN | | | 34. |
| Transmission of IPv6 over MS/TP Networks | Master-Slave/Token-Passing (MS/TP) is a contention-free access method for the RS-485 physical layer, which is used extensively in building automation networks. This specification defines the frame format for transmission of IPv6 packets and the method of forming link-local and statelessly autoconfigured IPv6 addresses on MS/TP networks. | IETF 6lo | draft-ietf-6lo-6lobac-01 I-D Exists | 2015-09-10 | Internet draft | network level | 6LoWPAN | | | 35. |
| Transmission of IPv6 Packets over ITU-T G.9959 Networks | This document describes the frame format for transmission of IPv6 packets as well as a method of forming IPv6 link-local addresses and statelessly autoconfigured IPv6 addresses on ITU-T G.9959 networks. | IETF 6lo | RFC 7428 (Proposed Standard) | 2015-02-02 | Proposed Standard | network level | 6LoWPAN | | | 36. |
| Transmission of IPv6 Packets over BLUETOOTH(R) Low Energy | This document describes how IPv6 is transported over Bluetooth low energy using 6LoWPAN techniques | IETF 6lo | draft-ietf-6lo-btle-10 AD Evaluation | 2015-03-02 | Proposed Standard | network level | 6LoWPAN | | | 37. |
| Transmission of IPv6 Packets over DECT Ultra Low Energy | This document describes how IPv6 is transported over DECT ULE using 6LoWPAN techniques. | IETF 6lo | draft-ietf-6lo-dect-ule-01 I-D Exists | 2015-01-27 | Internet draft | network level | 6LoWPAN | | | 38. |
| Transmission of IPv6 Packets over Near Field Communication | This document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques. | IETF 6lo | draft-ietf-6lo-nfc-00 I-D Exists | 2015-03-03 | Proposed Standard | network level | 6LoWPAN | | | 39. |
| IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals | This document describes the assumptions, problem statement, and goals for transmitting IP over IEEE 802.15.4 networks. The set of goals enumerated in this document form an initial set only. | IETF 6lowpanWG | RFC 4919 (Informational) | 2007-08 | Informational | network level | 6LoWPAN | | | 40. |
| Transmission of IPv6 Packets over IEEE 802.15.4 Networks | This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. Additional specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes. | IETF 6lowpanWG | RFC 4944 (Proposed Standard) | 2007-09 | Proposed Standard | network level | 6LoWPAN | | | 41. |
| A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) | This document specifies a method for generating IPv6 Interface Identifiers to be used with IPv6 Stateless Address Autoconfiguration (SLAAC), such that an IPv6 address configured using this method is stable within each subnet, but the corresponding Interface Identifier changes when the host moves from one network to another | IETF 6man | RFC 7217 (Proposed Standard) | 2014-04 | Proposed Standard | network level | IPv6 | | | 42. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A Uniform Format for IPv6 Extension Headers | In IPv6, optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the transport-layer header. There are a small number of such extension headers currently defined. This document describes the issues that can arise when defining new extension headers and discusses the alternate extension mechanisms in IPv6. It also provides a common format for defining any new IPv6 extension headers, if they are needed. | IETF 6man | RFC 6564 (Proposed Standard) | 2012-04 | Proposed Standard | network level | IPv6 | | | 43. |
| An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL) | In Low-Power and Lossy Networks (LLNs), memory constraints on routers may limit them to maintaining, at most, a few routes. In some configurations, it is necessary to use these memory-constrained routers to deliver datagrams to nodes within the LLN. The Routing Protocol for Low-Power and Lossy Networks (RPL) can be used in some deployments to store most, if not all, routes on one (e.g., the Directed Acyclic Graph (DAG) root) or a few routers and forward the IPv6 datagram using a source routing technique to avoid large routing tables on memory-constrained routers. This document specifies a new IPv6 Routing header type for delivering datagrams within a RPL routing domain. | IETF 6man | RFC 6554 (Proposed Standard) | 2012-03 | Proposed Standard | network level | Routing | | | 44. |
| Analysis of the 64-bit Boundary in IPv6 Addressing | The IPv6 unicast addressing format includes a separation between the prefix used to route packets to a subnet and the interface identifier used to specify a given interface connected to that subnet. Currently, the interface identifier is defined as 64 bits long for almost every case, leaving 64 bits for the subnet prefix. This document describes the advantages of this fixed boundary and analyzes the issues that would be involved in treating it as a variable boundary. | IETF 6man | RFC 7421 (Informational) | 2015-01 | Informational | network level | Addressing | | | 45. |
| Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums | This document provides an applicability statement for the use of UDP transport checksums with IPv6.It defines recommendations and requirements for the use of IPv6 UDP datagrams with a zero UDP checksum. It describes the issues and design principles that need to be considered when UDP is used with IPv6 to support tunnel encapsulations, and it examines the role of the IPv6 UDP transport checksum. The document also identifies issues and constraints for deployment on network paths that include middleboxes | IETF 6man | RFC 6936 (Proposed Standard) | 2013-04 | Proposed Standard | network level | IPv6 | | | 46. |
| Default Address Selection for Internet Protocol Version 6 (IPv6) | This document describes two algorithms, one for source address selection and one for destination address selection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. They do not override choices made by applications or upper-layer protocols, nor do they preclude the development of more advanced mechanisms for address selection | IETF 6man | RFC 6724 (Proposed Standard) | 2012-09 | Proposed Standard | network level | IPv6 | | | 47. |
| Distributing Address Selection Policy Using DHCPv6 | This document defines a new DHCPv6 option for such configuration, allowing a site administrator to distribute address selection policy overriding the default address selection parameters and policy table, and thus allowing the administrator to control the address selection behavior of nodes in their site | IETF 6man | RFC 7078 (Proposed Standard) | 2014-01 | Proposed Standard | network level | IPv6 | | | 48. |
| Duplicate Address Detection Proxy | The document describes a proxy-based mechanism allowing the use of Duplicate Address Detection (DAD) by IPv6 nodes in a point-to-multipoint architecture with a "split-horizon" forwarding scheme, primarily deployed for Digital Subscriber Line (DSL) and Fiber access architectures | IETF 6man | RFC 6957 (Proposed Standard) | 2013-06 | Proposed Standard | network level | IPv6 | | | 49. |
| Handling of Overlapping IPv6 Fragments | The fragmentation and reassembly algorithm specified in the base IPv6 specification allows fragments to overlap. This document demonstrates the security issues associated with allowing overlapping fragments and updates the IPv6 specification to explicitly forbid overlapping fragments | IETF 6man | RFC 5722 (Proposed Standard) | 2009-12 | Proposed Standard | network level | IPv6 | | | 50. |
| IANA Allocation Guidelines for the IPv6 Routing Header | This document specifies the IANA guidelines for allocating new values for the Routing Type field in the IPv6 Routing Header. | IETF 6man | RFC 5871 (Proposed Standard) | 2010-05 | Proposed Standard | network level | Routing | | | 51. |
| IPv6 and UDP Checksums for Tunneled Packets | This document updates the IPv6 specification (RFC 2460) to improve Performance when a tunnel protocol uses UDP with IPv6 to tunnel packets. This specification describes how the IPv6 UDP checksum requirement can be relaxed when the encapsulated packet itself contains a checksum. It also describes the limitations and risks of this approach and discusses the restrictions on the use of this method. | IETF 6man | RFC 6935 (Proposed Standard) | 2013-04 | Proposed Standard | network level | IPv6 | | | 52. |
| IPv6 Flow Label Specification | This document specifies the IPv6 Flow Label field and the minimum requirements for IPv6 nodes labeling flows, IPv6 nodes forwarding | IETF 6man | RFC 6437 (Proposed | 2011-11 | Proposed Standard | network level | IPv6 | | | 53. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | labeled packets, and flow state establishment methods | | Standard) | | | | | | | |
| IPv6 Multicast Address Scopes | This document updates the definitions of IPv6 multicast scopes and therefore updates RFCs 4007 and 4291 | IETF 6man | RFC 7346 (Proposed Standard) | 2014-08 | Proposed Standard | network level | Addressing | | | 54. |
| IPv6 Node Requirements | This document defines requirements for IPv6 nodes. It is expected that IPv6 will be deployed in a wide range of devices and situations. Specifying the requirements for IPv6 nodes allows IPv6 to function well and interoperate in a large number of situations and deployments. | IETF 6man | RFC 6434 (Informational) | 2011-12 | Informational | network level | IPv6 | | | 55. |
| IPv6 Router Advertisement Options for DNS Configuration | This document specifies IPv6 Router Advertisement options to allow IPv6 routers to advertise a list of DNS recursive server addresses and a DNS Search List to IPv6 hosts. | IETF 6man | RFC 6106 (Proposed Standard) | 2010-11 | Proposed Standard | network level | Routing | | | 56. |
| IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes | IPv6 specifies a model of a subnet that is different than the IPv4 subnet model. The subtlety of the differences has resulted in incorrect implementations that do not interoperate. This document spells out the most important difference: that an IPv6 address isn't automatically associated with an IPv6 on-link prefix | IETF 6man | RFC 5942 (Proposed Standard) | 2010-07 | Proposed Standard | network level | IPv6 | | | 57. |
| Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol | This document defines the IPv6 datagram compression option that can be negotiated by a node on the link through the IPV6CP. | IETF 6man | RFC 5172 (Proposed Standard) | 2008-02 | Proposed Standard | network level | IPv6 | | | 58. |
| Neighbor Unreachability Detection Is Too Impatient | IPv6 Neighbor Discovery includes Neighbor Unreachability Detection. That function is very useful when a host has an alternative neighbor-- for instance, when there are multiple default routers -- since it allows the host to switch to the alternative neighbor in a short time. | IETF 6man | RFC 7048 (Proposed Standard) | 2014-01 | Proposed Standard | network level | IPv6 | | | 59. |
| Processing of IPv6 "Atomic" Fragments | This document discusses the generation of the aforementioned atomic fragments and the corresponding security implications. Additionally, this document formally updates RFC 2460 and RFC 5722, such that IPv6 atomic fragments are processed independently of any other fragments, thus completely eliminating the aforementioned attack vector. | IETF 6man | RFC 6946 (Proposed Standard) | 2013-05 | Proposed Standard | network level | IPv6 | | | 60. |
| Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers | This document describes how the zone identifier of an IPv6 scoped address, defined as in the IPv6 Scoped Address Architecture(RFC 4007), can be represented in a literal IPv6 address and in a Uniform Resource Identifier that includes such a literal address. It updates the URI Generic Syntax specification (RFC 3986) accordingly | IETF 6man | RFC 6874 (Proposed Standard) | 2013-02 | Proposed Standard | network level | IPv6 | | | 61. |
| Reserved IPv6 Interface Identifiers | An IPv6 node autoconfiguring an interface identifier in these ranges will encounter unexpected consequences. Since there is no centralized repository for such reserved identifiers, this document aims to create one. | IETF 6man | RFC 5453 (Proposed Standard) | 2009-02 | Proposed Standard | network level | IPv6 | | | 62. |
| Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery | This document analyzes the security implications of employing IPv6 Fragmentation with Neighbor Discovery (ND) messages. It updates RFC4861 such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages, thus allowing for simple and effective countermeasures for Neighbor Discovery attacks. Finally, it discusses the security implications of using IPv6 fragmentation with Secure Neighbor Discovery (SEND) and formally updates RFC 3971 to provide advice regarding how the aforementioned security implications can be mitigated | IETF 6man | RFC 6980 (Proposed Standard) | 2013-08 | Proposed Standard | network level | IPv6 | | | 63. |
| Significance of IPv6 Interface Identifiers | This document clarifies that the bits in an interface identifier have no meaning and that the entire identifier should be treated as an opaque value. In particular, RFC 4291 defines a method by which the Universal and Group bits of an IEEE link-layer address are mapped into an IPv6 unicast interface identifier. This document clarifies that those two bits are significant only in the process of deriving interface identifiers from an IEEE link-layer address, and it updates RFC 4291 accordingly. | IETF 6man | RFC 7136 (Proposed Standard) | 2014-02 | Proposed Standard | network level | IPv6 | | | 64. |
| The Line-Identification Option | In Ethernet-based aggregation networks, several subscriber premises may be logically connected to the same interface of an Edge Router. This document proposes a method for the Edge Router to identify the subscriber premises using the contents of the received Router Solicitation messages. The applicability is limited to broadband network deployment scenarios in which multiple user ports are mapped to the same virtual interface on the Edge Router. | IETF 6man | RFC 6788 (Proposed Standard) | 2012-11 | Proposed Standard | network level | | | | 65. |
| The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying | The Routing Protocol for Low-Power and Lossy Networks (RPL) includes routing information in data-plane datagrams to quickly identify | IETF 6man | RFC 6553 (Proposed | 2012-03 | Proposed Standard | network level | Routing | | | 66. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| RPL Information in Data-Plane Datagrams | inconsistencies in the routing topology. This document describes the RPL Option for use among RPL routers to include such routing information. | | Standard) | | | | | | | |
| Transmission and Processing of IPv6 Extension Headers | Various IPv6 extension headers have been standardised since the IPv6 standard was first published. This document updates RFC 2460 to clarify how intermediate nodes should deal with such extension headers and with any that are defined in the future. It also specifies how extension headers should be registered by IANA, with a corresponding minor update to RFC 2780. | IETF 6man | RFC 7045 (Proposed Standard) | 2013-12 | Proposed Standard | network level | IPv6 | | | 67. |
| Updates to the IPv6 Multicast Addressing Architecture | This document updates the IPv6 multicast addressing architecture by redefining the reserved bits as generic flag bits. The document also provides some clarifications related to the use of these flag bits | IETF 6man | RFC 7371 (Proposed Standard) | 2014-09 | Proposed Standard | network level | Addressing | | | 68. |
| Using 127-Bit IPv6 Prefixes on Inter-Router Links | On inter-router point-to-point links, it is useful, for security and other reasons, to use 127-bit IPv6 prefixes. Such a practice parallels the use of 31-bit prefixes in IPv4. This document specifies the motivation for, and usages of, 127-bit IPv6 prefixlengths on inter-router point-to-point links. | IETF 6man | RFC 6164 (Proposed Standard) | 2011-04 | Proposed Standard | network level | Routing | | | 69. |
| Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels | The IPv6 flow label has certain restrictions on its use. This document describes how those restrictions apply when using the flow label for load balancing by equal cost multipath routing and for link aggregation, particularly for IP-in-IPv6 tunneled traffic | IETF 6man | RFC 6438 (Proposed Standard) | 2011-11 | Proposed Standard | network level | IPv6 | | | 70. |
| Border Gateway Multicast Protocol (BGMP): Protocol Specification | This document describes the Border Gateway Multicast Protocol (BGMP),a protocol for inter-domain multicast routing. | IETF bgmp WG | RFC 3913 (Historic) | 2004-09 | Historic | network level | Internetwork | | | 71. |
| Framework for Content Distribution Network Interconnection (CDNI) | The intent of this document is to outline what each interface needs to accomplish and to describe how these interfaces and mechanisms fit together, while leaving their detailed specification to other documents. This document, in combination with RFC 6707, obsoletes RFC 3466. | IETF cdni WG | RFC 7336 (Informational) | 2014-08 | Informational | network level | Internetwork | | | 72. |
| Issues with Private IP Addressing in the Internet | The discussion of RFC6752 focuses on link addresses and, to a small extent, loopback addresses. | IETF grow WG | RFC 6752 (Informational) | 2012-09 | Informational | network level | Addressing | | | 73. |
| A Border Gateway Protocol 4 (BGP-4) | This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. | IETF idr WG | RFC 4271 (Draft Standard) | 2006-01 | Draft Standard | network level | Internetwork | | | 74. |
| Autonomous-System-Wide Unique BGP Identifier for BGP-4 | This document updates RFC 4271.To accommodate situations where the current requirements for the BGP Identifier are not met, this document relaxes the definition of the BGP Identifier to be a 4-octet, unsigned, non-zero integer and relaxes the "uniqueness" requirement so that only Autonomous-System-<br>wide (AS-wide) uniqueness of the BGP Identifiers is required. | IETF idr WG | RFC 6286 (Proposed Standard) | 2011-06 | Proposed Standard | network level | Internetwork | | | 75. |
| BGP Support for Four-Octet Autonomous System (AS) Number Space | The Autonomous System number is encoded as a two-octet entity in the base BGP specification. This document describes extensions to BGP to carry the Autonomous System numbers as four-octet entities. This document obsoletes RFC 4893 and updates RFC 4271. | IETF idr WG | RFC 6793 (Proposed Standard) | 2012-12 | Proposed Standard | network level | Internetwork | | | 76. |
| Subcodes for BGP Finite State Machine Error | This document defines several subcodes for the BGP Finite State Machine (FSM) Error that could provide more information to help network operators in diagnosing BGP FSM issues and correlating network events. This document updates RFC 4271. | IETF idr WG | RFC 6608 (Proposed Standard) | 2012-03 | Proposed Standard | network level | Internetwork | | | 77. |
| Issues with IP Address Sharing | The RFC6269 gives the solutions about the Issues with IP Address Sharing to solve the problem that IPv4 addresses are not sufficient. | IETF intarea WG | RFC 6269 (Informational) | 2011-06 | Informational | network level | Addressing | | | 78. |
| An Architecture for IPv6 Unicast Address Allocation | This document RFC1887 provides an architecture for allocating IPv6 unicast addresses in the Internet. | IETF ipngwg WG | RFC 1887 (Informational) | 1995-12 | Informational | network level | Addressing | | | 79. |
| IPv6 Multicast Address Assignments | This document RFC2375 defines the initial assignment of IPv6 multicast addresses. | IETF ipngwg WG | RFC 2375 (Informational) | 1998-07 | Informational | network level | Addressing | | | 80. |
| Internet Key Exchange Protocol Version 2 (IKEv2) | This document describes version 2 of the Internet Key Exchange (IKE)protocol. IKE is a component of IPsec used for performing mutualauthentication and establishing and maintaining Security Associations(SAs). This document obsoletes RFC 5996, and includes all of the errata for it. It advances IKEv2 to be an Internet Standard. This document obsoletes RFC 5996,RFC5996 obsoletes RFC 4306, RFC4306 Obsoletes RFC 2407, RFC 2408, RFC 2409. | IETF ipsec WG | RFC 7296 (Internet Standard) | 2014-10 | Internet Standard | network level | Security | | | 81. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| IP Authentication Header | This document describes an updated version of the IP Authentication Header (AH), which is designed to provide authentication services in IPv4 and IPv6. This document obsoletes RFC 2402 (November 1998). | IETF ipsec WG | RFC 4302 (Proposed Standard) | 2005-12 | Proposed Standard | network level | Security | | | 82. |
| IP Encapsulating Security Payload (ESP) | This document describes an updated version of the Encapsulating Security Payload (ESP) protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. This document obsoletes RFC 2406 (November 1998). | IETF ipsec WG | RFC 4303 (Proposed Standard) | 2005-12 | Proposed Standard | network level | Security | | | 83. |
| IPsec Anti-Replay Algorithm without Bit Shifting | This document presents an alternate method to do the anti-replay checks and updates for IP Authentication Header (AH) and Encapsulating Security Protocol (ESP). The method defined in this document obviates the need for bit shifting and it reduces the number of times an anti-replay window is adjusted. | IETF ipsec WG | RFC 6479 (Informational) | 2012-01 | Informational | network level | Security | | | 84. |
| Security Architecture for the Internet Protocol | This document describes an updated version of the "Security Architecture for IP", which is designed to provide security services for traffic at the IP layer. This document obsoletes RFC 2401 (November 1998). | IETF ipsec WG | RFC 4301 (Proposed Standard) | 2005-12 | Proposed Standard | network level | Security | | | 85. |
| Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) | This document describes the use of Advanced Encryption Standard (AES) in Counter with CBC-MAC (CCM) Mode, with an explicit initializationvector (IV), as an IPsec Encapsulating Security Payload (ESP) mechanism to provide confidentiality, data origin authentication, and connectionless integrity. | IETF ipsec WG | RFC 4309 (Proposed Standard) | 2005-12 | Proposed Standard | network level | Security | | | 86. |
| Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification | RFC2463 IS Obsoleted by RFC 4443,This document describes the format of a set of control messages used in ICMPv6 (Internet Control Message Protocol). ICMPv6 is the Internet Control Message Protocol for Internet Protocol version 6(IPv6). | IETF IPV6WG | RFC 4443 (Draft Standard) | 2006-03 | Draft Standard | network level | | | | 87. |
| IP Version 6 Addressing Architecture | RFC2373 IS Obsoleted by RFC 3513,This document obsoletes RFC 3513, "IP Version 6 Addressing Architecture". This specification defines the addressing architecture of the IP Version 6 (IPv6) protocol. The document includes the IPv6 addressing model, text representations of IPv6 addresses, definition of IPv6 unicast addresses, anycast addresses, and multicast addresses, and anIPv6 node's required addresses. | IETF IPV6WG | RFC 4291 (Draft Standard) | 2006-02 | Draft Standard | network level | Addressing | | | 88. |
| IPv6 Stateless Address Autoconfiguration | RFC2462 IS Obsoleted by RFC 4862.This document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6. The autoconfiguration process includes generating a link-local address, generating global addresses via stateless address autoconfiguration, and the Duplicate Address Detection procedure to verify the uniqueness of the addresses on a link. | IETF IPV6WG | RFC 4862 (Draft Standard) | 2007-09 | Draft Standard | network level | Addressing | | | 89. |
| Multicast Addresses for Documentation | This document discusses which multicast addresses should be used for documentation purposes and reserves multicast addresses for such use. | IETF mboned WG | RFC 6676 (Informational) | 2012-08 | Informational | network level | Addressing | | | 90. |
| Multicast Source Discovery Protocol (MSDP) Deployment Scenarios | This document describes best current practices for intra-domain and inter-domain deployment of the Multicast Source Discovery Protocol (MSDP) in conjunction with Protocol Independent Multicast Sparse Mode(PIM-SM). | IETF mboned WG | RFC 4611 (Best Current Practice) | 2006-08 | Best Current Practice | network level | Internetwork | | | 91. |
| Mobility Support in IPv6 | IETF RFC6275-This document specifies Mobile IPv6, a protocol that allows nodes to remain reachable while moving around in the IPv6 Internet. | IETF mext WG | RFC 6275 (Proposed Standard) | 2011-07 | Proposed Standard | network level | Mobility | | | 92. |
| Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4 | This document specifies extensions to Mobile IP registration messages that can be used to create Mobility Security Associations between the mobile node and its home agent, and/or between the mobile node and a foreign agent. | IETF mip4 | RFC 3957 (Proposed Standard) | 2005-03 | Proposed Standard | network level | Mobility | | | 93. |
| Darpa internet program<br>protocol specification | This document specifies the DoD Standard Internet Protocol. The document is based on six earlier editions of the ARPA Internet Protocol Specification, and this edition revises aspects of addressing, error handling, option codes, and the security, precedence, compartments, and handling restriction features of the internet protocol. | IETF mip4 | RFC791(Internet Standard) | 1981-09 | Internet Standard | network level | Adressing＆Error Handing | | | 94. |
| Dual-Stack Mobile IPv4 | This specification provides IPv6 extensions to the Mobile IPv4 protocol. The extensions allow a dual-stack node to use IPv4 and IPv6 home addresses as well as to move between IPv4 and dual stack network | IETF mip4 | RFC 5454 (Proposed | 2009-03 | Proposed Standard | network level | Mobility | | | 95. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | infrastructures |  | Standard) |  |  |  |  |  |  |  |
| Dynamic Prefix Allocation for Network Mobility for Mobile IPv4 (NEMOv4) | The base Network Mobility for Mobile IPv4 (NEMOv4) specification defines extensions to Mobile IPv4 for mobile networks. This specification defines a dynamic prefix allocation mechanism for NEMOv4. | IETF mip4 | RFC6626(Proposed Standard) | 2012-05 | Proposed Standard | network level | Mobility |  |  | 96. |
| Experimental Message, Extensions, and Error Codes for Mobile IPv4 | Mobile IPv4 message types range from 0 to 255. This document reserves a message type for use by an IETF, company, or organization for experimental purposes, to evaluate enhancements to Mobile IPv4 messages before a formal standards proposal is issued. | IETF mip4 | RFC 4064 (Proposed Standard) | 2005-05 | Proposed Standard | network level | Mobility |  |  | 97. |
| Foreign Agent Error Extension for Mobile IPv4 | This document specifies a new extension for use by Foreign Agents operating Mobile IP for IPv4. Currently, a foreign agent cannot supply status information without destroying the ability for a mobile node to verify authentication data supplied by the home agent. The new extension solves this problem by making a better place for the foreign agent to provide its status information to the mobile node. | IETF mip4 | RFC 4636 (Proposed Standard) | 2006-10 | Proposed Standard | network level | Mobility |  |  | 98. |
| Generic Notification Message for Mobile IPv4 | This document specifies protocol enhancements that allow Mobile IPv4 entities to send and receive explicit notification messages using a Mobile IPv4 message type designed for this purpose. | IETF mip4 | RFC6098(Proposed Standard) | 2012-04 | Proposed Standard | network level | Mobility |  |  | 99. |
| Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4 | The Generic Routing Encapsulation (GRE) specification contains a Key field, which MAY contain a value that is used to identify a particular GRE data stream. This specification defines a new Mobile IP extension that is used to exchange the value to be used in the GRE Key field. This extension further allows the Mobility Agents to set up the necessary protocol interfaces prior to receiving the mobile node traffic. The new extension allows a Foreign Agent to request GRE tunneling without disturbing the Home Agent behavior specified for Mobile IPv4 | IETF mip4 | RFC6245(Proposed Standard) | 2011-05 | Proposed Standard | network level | Mobility |  |  | 100. |
| Home Agent-Assisted Route Optimization between Mobile IPv4 Networks | This document describes a home agent-assisted route optimization functionality for the IPv4 Network Mobility Protocol. The function is designed to facilitate optimal routing in cases where all nodes are connected to a single home agent; thus, the use case is route optimization within a single organization or similar entity. The functionality enables the discovery of eligible peer nodes (based on information received from the home agent) and their network prefixes ,and the establishment of a direct tunnel between such nodes. | IETF mip4 | RFC 6521 (Experimental) | 2012-03 | Experimental | network level | Mobility |  |  | 101. |
| IP Mobility Support for IPv4, Revised | This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet.The protocol provides for registering the care-of address with a home agent.This document Obsoletes RFC 3344. | IETF mip4 | RFC 5944 (Proposed Standard) | 2010-11 | Proposed Standard | network level | Mobility |  |  | 102. |
| Low-Latency Handoffs in Mobile IPv4 | The aim of this document is to present two methods to achieve low-latency Mobile IPv4 handoffs. In addition, a combination of these two methods is described. The described techniques allow greater support for real-time services on a Mobile IPv4 network by minimizing the period of time when a Mobile Node is unable to send or receive IPv4 packets due to the delay in the Mobile IPv4 Registration process | IETF mip4 | RFC 4881 (Experimental) | 2007-06 | Experimental | network level | Mobility |  |  | 103. |
| Mobile IPv4 Challenge/Response Extensions (Revised) | In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow a foreign agent to use a challenge/response mechanism to authenticate the mobile node. Furthermore, this document updates RFC 3344 by including a new authentication extension called the Mobile-Authentication, Authorization, and Accounting (AAA) Authentication extension. | IETF mip4 | RFC 4721 (Proposed Standard) | 2007-01 | Proposed Standard | network level | Mobility |  |  | 104. |
| Mobile IPv4 Dynamic Home Agent (HA) Assignment | Mobile IPv4 (RFC 3344) uses the home agent (HA) to anchor sessions of a roaming mobile node (MN). This document proposes a messaging mechanism for dynamic home agent assignment and HA redirection. The goal is to provide a mechanism to assign an optimal HA for a Mobile IP session while allowing any suitable method for HA selection. | IETF mip4 | RFC 4433 (Proposed Standard) | 2006-03 | Proposed Standard | network level | Mobility |  |  | 105. |
| Mobile IPv4 Extension for Carrying Network Access Identifiers | This document defines a Mobile IP extension that carries identities for the Home AAA and HA servers in the form of Network Access Identifiers (NAIs). The extension allows a Home Agent to pass its identity (and that of the Home AAA server) to the mobile node, which can then pass it on to the local AAA server when changing its point of attachment. This extension may also be used in other situations requiring communication | IETF mip4 | RFC 3846 (Proposed Standard) | 2004-06 | Proposed Standard | network level | Mobility |  |  | 106. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | of a NAI between Mobile IP nodes. | | | | | | | | | |
| Mobile IPv4 Fast Handovers | This document adapts the Mobile IPv6 Fast Handovers to improve delay and packet loss resulting from Mobile IPv4 handover operations. Specifically, this document addresses movement detection, IP address configuration, and location update latencies during a handover. For reducing the IP address configuration latency, the document proposes that the new Care-of Address is always made to be the new access router's IP address. | IETF mip4 | RFC 4988 (Experimental) | 2007-10 | Experimental | network level | Mobility | | | 107. |
| Mobile IPv4 RADIUS Requirements | This document provides an applicability statement as well as a scope definition for specifying Remote Authentication Dial-In User Service (RADIUS) extensions to support Mobile IPv4. The goal is to allow specification of RADIUS attributes to assist the Mobile IPv4 signaling procedures proposes that the new Care-of Address is always made to be the new access router's IP address. | IETF mip4 | RFC 5030 (Informational) | 2007-10 | Informational | network level | Mobility | | | 108. |
| Mobile IPv4 Regional Registration | This document describes a new kind of "regional registrations", i.e., registrations local to the visited domain. The regional registrations are performed via a new network entity called a Gateway Foreign Agent (GFA) and introduce a layer of hierarchy in the visited domain. Regional registrations reduce the number of signaling messages to the home network, and reduce the signaling delay when a mobile node moves from one foreign agent to another within the same visited domain. This document is an optional extension to the Mobile IPv4 protocol. | IETF mip4 | RFC 4857 (Experimental) | 2007-06 | Experimental | network level | Mobility | | | 109. |
| Mobile IPv4 Traversal across IPSec-Based VPN Gateways | This document outlines a solution for the Mobile IPv4 (MIPv4) and IPSec coexistence problem for enterprise users. The solution consists of an applicability statement for using Mobile IPv4 and IPSec for session mobility in corporate remote access scenarios, and a required mechanism for detecting the trusted internal network securely. | IETF mip4 | RFC 5265 (Proposed Standard) | 2008-06 | Proposed Standard | network level | Mobility | | | 110. |
| Network Mobility (NEMO) Extensions for Mobile IPv4 | This document describes a protocol for supporting Mobile Networks between a Mobile Router and a Home Agent by extending the Mobile IPv4 protocol. A Mobile Router is responsible for the mobility of one or more network segments or subnets moving together. The Mobile Router hides its mobility from the nodes on the Mobile Network. The nodes on the Mobile Network may be fixed in relationship to the Mobile Router and may not have any mobility function | IETF mip4 | RFC 5177 (Proposed Standard) | 2008-04 | Proposed Standard | network level | Mobility | | | 111. |
| Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways | Deploying Mobile-IP v4 in networks that are connected to the Internet through a Virtual Private Network (VPN) gateway presents some problems that do not currently have well-described solutions. This document aims to describe and illustrate these problems, and to propose some guidelines for possible solutions. | IETF mip4 | RFC 4093 (Informational) | 2005-08 | Informational | network level | Mobility | | | 112. |
| Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE) | Enterprise users require mobility and secure connectivity when they roam and connect to the services offered in the enterprise. Secure connectivity is required when the user connects to the enterprise from an untrusted network. Mobility is beneficial when the user moves, either inside or outside the enterprise network, and acquires a new IP address. This document describes a solution using Mobile IPv4 (MIPv4) and mobility extensions to IKEv2 (MOBIKE) to provide secure connectivity and mobility | IETF mip4 | RFC 5266 (Best Current Practice) | 2008-06 | Best Current Practice | network level | Mobility | | | 113. |
| Hierarchical Mobile IPv6 (HMIPv6) Mobility Management | This document introduces extensions to Mobile IPv6 and IPv6 Neighbour Discovery to allow for local mobility handling. Hierarchical mobility management for Mobile IPv6 is designed to reduce the amount of signalling between the mobile node, its correspondent nodes, and its home agent.This document Obsoletes RFC 4140. | IETF mipshop WG | RFC 5380 (Proposed Standard) | 2008-10 | Proposed Standard | network level | Mobility | | | 114. |
| Mobile IPv6 Fast Handovers | This document specifies a protocol to improve handover latency due to Mobile IPv6 procedures. This document does not address improving the link-switching latency. | IETF mipshop WG | RFC 5568 (Proposed Standard) | 2009-07 | Proposed Standard | network level | Mobility | | | 115. |
| Multicast Extensions to OSPF | RFC 1584 documents enhancements to the OSPF protocol enabling the routing of IP multicast datagrams. | IETF mospf WG | RFC 1584 (Historic) | 1994-03 | Historic | network level | Routing | | | 116. |
| Applicability Statement for CR-LDP | This document discusses the applicability of Constraint-Based LSP Setup using LDP. It discusses possible network applications, extensions to Label Distribution Protocol (LDP) required to implement constraint-based routing, guidelines for deployment and known limitations of the protocol. This document is a prerequisite to advancing CR-LDP on the | IETF mpls | RFC 3213 (Informational) | 2002-01 | Informational | network level | Internetwork | | | 117. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | standards track. | | | | | | | | | |
| Applicability Statement for Extensions to RSVP for LSP-Tunnels | This memo discusses the applicability of "Extensions to RSVP (Resource Reservation Protocol) for LSP Tunnels". It highlights the protocol's principles of operation and describes the network context for which it was designed. Guidelines for deployment are offered and known protocol limitations are indicated.This document is intended to accompany the submission of "Extensions to RSVP for LSP Tunnels" onto the Internet standards track. | IETF mpls | RFC 3210 (Informational) | 2001-12 | Informational | network level | Internetwork | | | 118. |
| Graceful Restart Mechanism for Label Distribution Protocol | This document describes a mechanism that helps to minimize the negative effects on MPLS traffic caused by Label Switching Router's (LSR's) control plane restart, specifically by the restart of its Label Distribution Protocol (LDP) component, on LSRs that are capable of preserving the MPLS forwarding component across the restart. The mechanism described in this document is applicable to all LSRs, both those with the ability to preserve forwarding state during LDP restart and those without (although the latter needs to implement only a subset of the mechanism described in this document). | IETF mpls | RFC 3478 (Proposed Standard) | 2003-02 | Proposed Standard | network level | Internetwork | | | 119. |
| LDP Applicability | A fundamental concept in MPLS is that two Label Switching Routers (LSRs) must agree on the meaning of the labels used to forward traffic between and through them. This common understanding is achieved by using a set of procedures, called a label distribution protocol, by which one LSR informs another of label bindings it has made. This document describes the applicability of a set of such procedures called LDP (for Label Distribution Protocol) by which LSRs distribute labels to support MPLS forwarding along normally routed paths. | IETF mpls | RFC 3037 (Informational) | 2001-01 | Informational | network level | Internetwork | | | 120. |
| LDP State Machine | This document provides state machine tables for ATM (Asynchronous Transfer Mode) switch LSRs. In the current LDP specification, there is no state machine specified for processing LDP messages. We think that defining a common state machine is very important for interoperability between different LDP and CR-LDP implementations. | IETF mpls | RFC 3215 (Informational) | 2002-01 | Informational | network level | Internetwork | | | 121. |
| LSP Modification Using CR-LDP | This document presents an approach to modify the bandwidth and possibly other parameters of an established CR-LSP (Constraint-based Routed Label Switched Paths) using CR-LDP (Constraint-based Routed Label Distribution Protocol) without service interruption. After a CR-LSP is set up, its bandwidth reservation may need to be changed by the network operator, due to the new requirements for the traffic carried on that CR-LSP. | IETF mpls | RFC 3214 (Proposed Standard) | 2002-01 | Proposed Standard | network level | Internetwork | | | 122. |
| MPLS Loop Prevention Mechanism | This paper presents a simple mechanism, based on "threads", which can be used to prevent Multiprotocol Label Switching (MPLS) from setting up label switched path (LSPs) which have loops. The mechanism is compatible with, but does not require, VC merge. The mechanism can be used with either the ordered downstream-on-demand allocation or ordered downstream allocation. The amount of information that must be passed in a protocol message is tightly bounded (i.e., no path-vector is used). | IETF mpls | RFC 3063 (Experimental) | 2001-02 | Experimental | network level | Internetwork | | | 123. |
| Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) Environment | This document offers a framework for IP multicast deployment in an MPLS environment. Issues arising when MPLS techniques are applied to IP multicast are overviewed. The pros and cons of existing IP multicast routing protocols in the context of MPLS are described and the relation to the different trigger methods and label distribution modes are discussed. | IETF mpls | RFC 3353 (Informational) | 2002-08 | Informational | network level | Internetwork | | | 124. |
| The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols | This document documents the consensus reached by the Multiprotocol Label Switching (MPLS) Working Group within the IETF to focus its efforts on "Resource Reservation Protocol (RSVP)-TE: Extensions to RSVP for Label-Switched Paths (LSP) Tunnels" (RFC 3209) as the MPLS signaling protocol for traffic engineering applications and to undertake no new efforts relating to "Constraint-Based LSP Setup using Label Distribution Protocol (LDP)" (RFC 3212).The recommendations of section 6 have been accepted by the IESG. | IETF mpls | RFC 3468 (Informational) | 2003-02 | Informational | network level | Internetwork | | | 125. |
| Use of Label Switching on Frame Relay Networks Specification | This document defines the model and generic mechanisms for Multiprotocol Label Switching on Frame Relay networks. Furthermore, it extends and clarifies portions of the Multiprotocol Label Switching Architecture described in [ARCH] and the Label Distribution Protocol (LDP) described in [LDP] relative to Frame Relay Networks. MPLS enables the use of Frame Relay Switches as Label Switching Routers | IETF mpls | RFC 3034 (Proposed Standard) | 2001-01 | Proposed Standard | network level | Internetwork | | | 126. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | (LSRs). |  |  |  |  |  |  |  |  |  |
| Multicast Source Discovery Protocol (MSDP) | The Multicast Source Discovery Protocol (MSDP) describes a mechanism to connect multiple IP Version 4 Protocol Independent Multicast Sparse-Mode (PIM-SM) domains together. Each PIM-SM domain uses its own independent Rendezvous Point (RP) and does not have to depend on RPs in other domains. This document reflects existing MSDP implementations. | IETF msdp WG | RFC 3618 (Experimental) | 2003-10 | Experimental | network level | Internetwork |  |  | 127. |
| ICMP Router Discovery Messages | This document specifies an extension of the Internet Control Message Protocol (ICMP) to enable hosts attached to multicast or broadcast networks to discover the IP addresses of their neighboring routers. | IETF rdisc WG | RFC 1256 (Proposed Standard) | 1991-09 | Proposed Standard | network level | Routing |  |  | 128. |
| NACK-Oriented Reliable Multicast (NORM) Transport Protocol | This document describes the messages and procedures of the Negative-ACKnowledgment (NACK) Oriented Reliable Multicast (NORM) protocol.This protocol can provide end-to-end reliable transport of bulk data objects or streams over generic IP multicast routing and forwarding services.This document obsoletes RFC 3940. | IETF rmt WG | RFC 5740 (Proposed Standard) | 2009-11 | Proposed Standard | network level | Internetwork |  |  | 129. |
| A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network | This document specifies a mechanism that enables a Routing Protocol for Low-power and Lossy Networks (RPL) router to measure the aggregated values of given routing metrics along an existing route towards another RPL router, thereby allowing the router to decide if it wants to initiate the discovery of a better route. | IETF roll | RFC 6998 (Experimental) | 2013-08 | Experimental | network level | Routing |  |  | 130. |
| A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs) | This document presents a security threat analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). The development builds upon previous work on routing security and adapts the assessments to the issues and constraints specific to low-power and lossy networks. A systematic approach is used in defining and evaluating the security threats. Applicable countermeasures are application specific and are addressed in relevant applicability statements. | IETF roll | RFC 7416 (Informational) | 2015-01 | Informational | network level | Routing |  |  | 131. |
| Building Automation Routing Requirements in Low-Power and Lossy Networks | The Routing Over Low-Power and Lossy (ROLL) networks Working Group has been chartered to work on routing solutions for Low-Power and Lossy Networks (LLNs) in various markets: industrial, commercial (building), home, and urban networks. Pursuant to this effort, this document defines the IPv6 routing requirements for building automation. | IETF roll | RFC 5867 (Informational) | 2010-06 | Informational | network level | Routing |  |  | 132. |
| Industrial Routing Requirements in Low-Power and Lossy Networks | The wide deployment of lower-cost wireless devices will significantly improve the productivity and safety of industrial plants while increasing the efficiency of plant workers by extending the information set available about the plant operations. The aim of this document is to analyze the functional requirements for a routing protocol used in industrial Low-power and Lossy Networks (LLNs) of field devices. | IETF roll | RFC5673 (Informational) | 2009-10 | Informational | network level | Routing |  |  | 133. |
| Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL) | The Routing Protocol for Low-Power and Lossy Networks (RPL) specification defines a generic Distance Vector protocol that is adapted to a variety of network types by the application of specific Objective Functions (OFs). An OF states the outcome of the process used by a RPL node to select and optimize routes within a RPL Instance based on the Information Objects available; an OF is not an algorithm. This document specifies a basic Objective Function that relies only on the objects that are defined in the RPL and does not use any protocol extensions. | IETF roll | RFC6552(Proposed Standard) | 2012-03 | Proposed Standard | network level | Routing |  |  | 134. |
| Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks | This document specifies a point-to-point route discovery mechanism, Complementary to the Routing Protocol for Low-power and Lossy Networks (RPL) core functionality. This mechanism allows an IPv6 router to discover "on demand" routes to one or more IPv6 routers in a Low-power and Lossy Network (LLN) such that the discovered routes meet specified metrics constraints. | IETF roll | RFC 6997 (Experimental) | 2013-08 | Experimental | network level | Routing |  |  | 135. |
| Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks | Low-Power and Lossy Networks (LLNs) have unique characteristics compared with traditional wired and ad hoc networks that require the specification of new routing metrics and constraints. By contrast, with typical Interior Gateway Protocol (IGP) routing metrics using hop counts or link metrics, this document specifies a set of link and node routing metrics and constraints suitable to LLNs to be used by the Routing Protocol for Low-Power and Lossy Networks(RPL). | IETF roll | RFC6551(Proposed Standard) | 2012-03 | Proposed Standard | network level | Routing |  |  | 136. |
| Routing Requirements for Urban Low- | This document details application-specific IPv6 routing requirements for Urban Low-Power and Lossy Networks (U-LLNs). Note that this | IETF roll | RFC 5548 | 2009-05 | Informational | network level | Routing |  |  | 137. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Power and Lossy Networks | document details the set of IPv6 routing requirements for U-LLNs in strict compliance with the layered IP architecture | | (Informational) | | | | | | | |
| RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks | This document specifies the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), which provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point as well as point-to-multipoint traffic from the central control point to the devices inside the LLN are supported. Support for point-to-point traffic is also available. | IETF roll | RFC 6550 (Proposed Standard) | 2012-03 | Proposed Standard | network level | Routing | | | 138. |
| Terms Used in Routing for Low-Power and Lossy Networks | This document provides a glossary of terminology used in routing requirements and solutions for networks referred to as Low-Power and Lossy Networks (LLNs). An LLN is typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links. There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (e.g., heating, ventilation, air conditioning, lighting access control, fire), connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration. | IETF roll | RFC 7102 (Informational) | 2014-01 | Informational | network level | Routing | | | 139. |
| The Minimum Rank with Hysteresis Objective Function | The Routing Protocol for Low-Power and Lossy Networks (RPL)constructs routes by using Objective Functions that optimize or constrain the routes it selects and uses. This specification describes the Minimum Rank with Hysteresis Objective Function (MRHOF), an Objective Function that selects routes that minimize a metric, while using hysteresis to reduce churn in response to small metric changes. MRHOF works with additive metrics along a route, and the metrics it uses are determined by the metrics that the RPL Destination Information Object (DIO) messages advertise. | IETF roll | RFC6719(Proposed Standard) | 2012-09 | Proposed Standard | network level | Routing | | | 140. |
| IPv6 Address Assignment to End Sites | This document RFC6177 obsoletes the RFC 3177 recommendations on the assignment of IPv6 address space to end sites. | IETF v6ops WG | RFC 6177 (Best Current Practice) | 2011-03 | Best Current Practice | network level | Addressing | | | 141. |
| Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 | TheVirtual Router Redundancy Protocol(VRRP) is a computer networking protocol that provides for automatic assignment of available Internet Protocol(IP) routers to participating hosts. | IETF vrrp WG | RFC 5798 (Proposed Standard) | 2010-03 | Proposed Standard | network level | Routing | | | 142. |
| ISO 10374, Freight containers – Automatic identification | Specifies all necessary user requirements. Includes: a container identification system, data coding systems, description of data, performance criteria and security features. | ISO TC 104/SC 4 | International Standard | 2007-02-24 | | RFID | | | | 143. |
| ISO 18185-1, Freight containers – Electronic seals – Part 1: Communication protocol | SO 18185-1:2007 provides a system for the identification and presentation of information about freight container electronic seals. The identification system provides an unambiguous and unique identification of the container seal, its status and related information.<br>The presentation of this information is provided through a radio-communications interface providing seal identification and a method for determining whether a freight container's seal has been opened.<br>ISO 18185-1:2007 specifies a read-only, non-reusable freight container seal identification system, with an associated system for verifying the accuracy of use, having<br>- a seal status identification system,<br>- a battery status indicator,<br>- a unique seal identifier including the identification of the manufacturer,<br>- seal (tag) type.<br>ISO 18185-1:2007 is used in conjunction with the other parts of ISO 18185.<br>It applies to all electronic seals used on freight containers covered by ISO 668, ISO 1496-1 to ISO 1496-5, and ISO 8323. Wherever appropriate and practicable, it also applies to freight containers other than those covered by these International Standards. | ISO TC 104/SC 4 | International Standard | 2011-05-13 | | RFID | | | | 144. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO 18185-2, Freight containers – Electronic seals – Part 2: Application requirements | ISO 18185-2:2007 specifies a freight container seal identification system, with an associated system for verifying the accuracy of use, having:<br>- a seal status identification system;<br>- a battery status indicator;<br>- a unique seal identifier including the identification of the manufacturer;<br>- a seal (tag) type.<br>ISO 18185-2:2007 is used in conjunction with the other parts of ISO 18185. | ISO TC 104/SC 4 | International Standard | 2011-01-20 | | RFID | | | | 145. |
| ISO 18185-3, Freight containers – Electronic seals – Part 3: Environmental characteristics | ISO 18185-3:2006 specifies the minimum environmental characteristics for electronic seals.<br>ISO 18185-3:2006 describes the environmental requirements for the ISO 18185 series, for ISO 10374 (Freight containers -- RF automatic identification) and for ISO 17363 (Supply chain applications of RFID -- Freight containers), since it is expected that the implementation of these International Standards will face the same environmental conditions. However, each of these International Standards has its own unique requirements other than environmental conditions. | ISO TC 104/SC 4 | International Standard | 2009-09-18 | | RFID | | | | 146. |
| ISO 18185-4, Freight containers – Electronic seals – Part 4: Data protection | ISO 18185-4:2007 specifies requirements for the data protection, device authentication and conformance capabilities of electronic seals for communication to and from a seal and its associated reader. These capabilities include the accessibility, confidentiality, data integrity, authentication and non-repudiation of stored data. | ISO TC 104/SC 4 | International Standard | 2011-05-13 | | RFID | | | | 147. |
| ISO 18185-5, Freight containers – Electronic seals – Part 5: Physical layer | ISO 18185-5:2007 specifies the air interface between electronic container seals and Reader/Interrogators of those seals.<br>It is to be used in conjunction with the other parts of ISO 18185.<br>ISO 18185-5:2007 describes the physical layer for supply chain applications of RFID for freight containers in accordance with the ISO 18185 series and ISO 17363, since it is expected that the implementation of these standards will face the same international conditions. However, each of these standards has its own unique requirements other than the physical layer. It is expected that RFID Freight Container Identification (as specified in ISO 10374 and ISO 17363), and electronic seals (as specified in the ISO 18185 series) will be able to use the same infrastructure, while recognizing that that there may be requirements for different frequencies for passive devices as opposed to the active devices identified in ISO 18185-5:2007. | ISO TC 104/SC 4 | International Standard | 2011-05-13 | | RFID | | | | 148. |
| ISO 6346, Freight containers – Coding, identification and marking | Provides a system for general application for the identification and presentation of information about freight containers. Specifies an identification system with mandatory marks for visual interpretation and optional features for automatic identification and electronic data interchange and a coding system for data on container size and type. Replaces the second edition, which has been technically revised. | ISO TC 104/SC 4 | International Standard | 1998-01-22 | | AIDC | | | | 149. |
| ISO/TS 10891, Freight containers – Radio frequency identification (RFID) – Licence plate tag | ISO/TS 10891:2009 establishes:<br>- a set of requirements for container tags, which allow the transfer of information from a container to automatic processing systems by electronic means;<br>- a data coding system for container identification and permanent related information which resides within a container tag;<br>- a data coding system for the electronic transfer of both container identification and permanent related information from container tags to automatic data processing systems;<br>- the description of data to be included in container tags for | ISO TC 104/SC 4 | International Standard | 2009-01-30 | | RFID | | | | 150. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | transmission to automatic data processing systems;<br>- performance criteria necessary to ensure consistent and reliable operation of container tags within the international transportation community;<br>- the physical location of container tags on containers;<br>- features to inhibit malicious or unintentional alteration and/or deletion of the information content of container tags when installed on a freight container.<br>It is intended to be applicable to freight containers as defined in ISO 668 as well as to other containers not defined in ISO 668 and container ancillary equipment such as road and terminal chassis, generator sets and power packs .<br>The use of container tags and the equipping of containers for automatic identification are optional. The purpose of ISO/TS 10891:2009 is to optimise the efficiency of equipment control systems and to assist in container security initiatives and programs, including the optional usage of electronic seals in accordance with ISO 18185, and any subsequent International Standard. For this reason, any container tag system used for identifying containers shall be non-proprietary and conform to and be compatible with ISO/TS 10891:2009. | | | | | | | | | |
| ISO 17363, Supply chain applications of RFID – Freight containers | ISO 17363:2013 defines the usage of read/write radio-frequency identification technology (RFID) cargo shipment-specific tags associated with containerized freight for supply chain management purposes (“manifest tags”). This International Standard, through reference to other standards within ISO TC 122, ISO TC 104, and ISO/IEC JTC 1/SC 31, defines the air interface communications, a common set of required data structures, and a commonly organized, through common syntax and semantics, set of optional data requirements.<br>This International Standard<br>- Makes recommendations about a second generation supply chain tag intended to monitor the condition and security of the freight resident within a freight container.<br>- Specifies the implementation of sensors for freight resident in a freight container.<br>- Makes specific recommendations about mandatory non-reprogrammable information on the shipment tag.<br>- Makes specific recommendations about optional, re-programmable information on the shipment tag.<br>- Makes specific recommends about the data link interface for GPS or GLS services.<br>- Specifies the reuse and recyclability of the RF tag.<br>- Specifies the means by which the data in a compliant RF tag is “backed-up” by bar codes and two-dimensional symbols, as well as human-readable information. | ISO TC 122 | 2nd Ed Approved 2012-12-07, awaiting publication | | | RFID | | | | 151. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO 15394, Packaging — Bar code and two-dimensional symbols for shipping, transport and receiving labels | This International Standard:<br>– specifies the minimum requirements for the design of labels containing linear bar code and two dimensional symbols on transport units to convey data between trading partners;<br>– provides for traceability of transported units via a unique transport unit identifier (licence plate);<br>– provides guidance on the formatting on the label of data presented in linear bar code, two-dimensional symbol or human readable form; – provides specific recommendations regarding the choice of bar code symbologies, and specifies quality requirements;<br>– makes recommendations as to label placement, size and the inclusion of free text and any appropriate graphics;<br>– provides guidance on the selection of label material. This International Standard is not applicable to the direct printing on to kraft coloured corrugated surfaces. | ISO TC 122/WG 12 | International standard | 12-Jun-2006 | Application Standard | Application Standard | Bar code & 2D symbols | Supply chain | Expected revision to begin in 2013 | 152. |
| ISO 17364, Supply chain applications of RFID – Returnable transport items (RTIs) | ISO 17364:2013 defines the basic features of RFID for the use in the supply chain when applied to returnable transport items. In particular it<br>• provides specifications for the identification of the RTI and RPI,<br>• makes recommendations about additional information on the RF tag,<br>• specifies the semantics and data syntax to be used,<br>• specifies the data protocol to be used to interface with business applications and the RFID system,<br>• specifies the minimum performance requirements,<br>• specifies the air interface standards between the RF interrogator and RF tag, an<br>• specifies the reuse and recyclability of the RF tag. | ISO TC 122/WG 12 | International standard | 22-Feb-2013 | Application Standard | Application Standard | RFID | Supply chain | | 153. |
| ISO 17365, Supply chain applications of RFID – Transport units | ISO 17365:2013 defines the basic features of RFID for the use in the supply chain when applied to transport units. In particular it<br>provides specifications for the identification of the transport unit,<br>makes recommendations about additional information on the RF tag,<br>• specifies the semantics and data syntax to be used,<br>• specifies the data protocol to be used to interface with business applications and the RFID system,<br>• specifies the minimum performance requirements,<br>• specifies the air interface standards between the RF interrogator and RF tag, and<br>• specifies the reuse and recyclability of the RF tag | ISO TC 122/WG 12 | International standard | 22-Feb-2013 | Application Standard | Application Standard | RFID | Supply chain | | 154. |
| ISO 17366, Supply chain applications of RFID – Product packaging | • ISO 17366:2013 defines the usage of RFID technology for product packaging i defines the basic features of RFID for the use in the supply chain when applied to product packaging. In particular it<br>• provides specifications for the identification of the product packaging,<br>• makes recommendations about additional information on the RF tag,<br>• specifies the semantics and data syntax to be used,<br>• specifies the data protocol to be used to interface with business applications and the RFID system,<br>• specifies the minimum performance requirements,<br>• specifies the air interface standards between the RF interrogator and RF tag, and<br>• specifies the reuse and recyclability of the RF tag. | ISO TC 122/WG 12 | International standard | 22-Feb-2013 | Application Standard | Application Standard | RFID | Supply chain | | 155. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO 17367, Supply chain applications of RFID – Returnable transport items (RTIs) | • ISO 17367:2013 defines the basic features of RFID for the use in the supply chain when applied to product tagging. In particular it<br>• provides specific recommendations about the encoded identification of the product,<br>• makes recommendations about additional information about the product on the RF tag,<br>• makes recommendations about the semantics and data syntax to be used,<br>• makes recommendations about the data protocol to be used to interface with business applications and the RFID system, and<br>• makes recommendations about the air interface standards between the RF interrogator and RF tag.<br>• This International Standard only addresses product tagging and does not address product packaging. | ISO TC 122/WG 12 | International standard | 22-Feb-2013 | Application Standard | Application Standard | RFID | Supply chain |  | 156. |
| ISO 18574, Internet of Things (IoT) in the supply chain — Containerized cargo | ISO 18574 specifies the component pieces necessary for the effective implementation of Internet of Things applications for containerized cargo. This International Standard specifies the necessary forms of identification, communications, types of devices, sensors, actuators, means of localization and tracking, appropriate security, methods of storage, and processing of IoT data. | ISO TC 122/WG 12 | AWI | 15-Feb-2013 | Application Standard | Application Standard | IoT | Supply chain | 48 month track | 157. |
| ISO 18575, Internet of Things (IoT) in the supply chain — Products & product packages | ISO 18575 specifies the component pieces necessary for the effective implementation of Internet of Things applications for products and product packaging. This International Standard specifies the necessary forms of identification, communications, types of devices, sensors, actuators, means of localization and tracking, appropriate security, methods of storage, and processing of IoT data. | ISO TC 122/WG 12 | AWI | 15-Feb-2013 | Application Standard | Application Standard | IoT | Supply chain | 48 month track | 158. |
| ISO 18576, Internet of Things (IoT) in the supply chain — Returnable transport items (RTIs) | ISO 18576 specifies the component pieces necessary for the effective implementation of Internet of Things applications for returnable transport items. This International Standard specifies the necessary forms of identification, communications, types of devices, sensors, actuators, means of localization and tracking, appropriate security, methods of storage, and processing of IoT data. | ISO TC 122/WG 12 | AWI | 15-Feb-2013 | Application Standard | Application Standard | IoT | Supply chain | 48 month track | 159. |
| ISO 18577, Internet of Things (IoT) in the supply chain — Transport units | ISO 18577 This International Standard specifies the component pieces necessary for the effective implementation of Internet of Things applications for transport units. This International Standard specifies the necessary forms of identification, communications, types of devices, sensors, actuators, means of localization and tracking, appropriate security, methods of storage, and processing of IoT data. | ISO TC 122/WG 12 | AWI | 15-Feb-2013 | Application Standard | Application Standard | IoT | Supply chain | 48 month track | 160. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO 22742, Packaging — Linear bar code and two-dimensional symbols for product packaging | This International Standard<br>a) specifies the minimum requirements for the design of labels containing a linear bar code and two dimensional symbols on product packages to convey data between trading partners,<br>b) provides guidance for the formatting on the label of data presented in a linear bar code, two dimensional symbols or human readable form,<br>c) provides specific recommendations regarding the choice of linear bar code and 2D symbologies, and specifies quality requirements and classes of bar code density,<br>d) provides specific recommendations regarding 2D symbologies, which allow a broad choice for general use of scanning hardware (e.g. area imagers, linear imagers, single line laser scanners, and rastering laser scanners), and<br>e) makes recommendations as to label placement, size and the inclusion of free text and any appropriate graphics. This International Standard supports item identification and supply chain processes, at the product package level, such as inventory control, picking, and point of use. NOTE 1 ISO 15394 supports the distribution and transportation business processes, so aiding the tracing and tracking of unique shipments. NOTE 2 ISO 28219 addresses the direct part marking. The purpose of this International Standard is to establish the machine readable (e.g. bar code) and human readable data content of labels applied to product packages. Intended applications include, but are not limited to, inventory, warehouse management, maintenance and point of purchase. While guidance is provided, specific label dimensions or marking areas and the location of the information are not defined in this International Standard. Before implementing this specification, suppliers and manufacturers are advised to review and mutually agree on these details with their trading partners. This International Standard does not supersede or replace any applicable safety or regulatory marking or labelling requirements. It is intended to satisfy the minimum product package requirements of numerous applications and industry groups. As such, its applicability is to a wide range of industries, each of which has specific implementation guidelines. This International Standard is also applicable to any other mandated labelling requirements. | ISO TC 122/WG 12 | International standard | 15-Dec-2010 | Application Standard | Application Standard | Bar code & 2D symbols | Supply chain | | 161. |
| ISO 28219, Packaging — Labelling and direct product marking with linear bar code and two-dimensional symbols | This International Standard – defines minimum requirements for identifying items; – provides guidelines for item marking with machine-readable symbols; – covers both labels and direct marking of items; – includes testing procedures for label adhesive characteristics and mark durability; – provides guidance for the formatting on the label of data presented in linear bar code, two-dimensional symbol or human readable form;<br>– is intended for applications which include, but are not limited to, support of systems that automate the control of items during the processes of:<br>– production;<br>– inventory;<br>– distribution; – field service; – point of sale; – repair, and<br>– is intended to include, but it is not limited to, multiple industries including: – automotive; – aerospace;<br>– chemical;<br>– consumer items;<br>– electronics;<br>– health care;<br>– marine;<br>– rail;<br>– telecommunications. The location and application method of the marking are not defined (these will be reviewed and agreed upon by suppliers and manufacturers and their trading partners before implementing this International Standard). This International Standard does not supersede or replace any applicable safety or regulatory marking or labeling requirements. This International Standard is meant to satisfy the minimum item marking requirements of numerous applications and industry groups and as such its applicability is to a wide range of industries, each of which may have specific implementation guidelines for it. This International Standard is to be applied in addition to any other mandated labeling direct-marking requirements. The labeling and direct marking requirement of this International Standard and other standards can be combined | ISO TC 122/WG 12 | International standard | 5-Jan-2009 | Application Standard | Application Standard | Bar code & 2D symbols | Supply chain | Expected revision to begin in 2013 | 162. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | labeling into one label or marking area or appear as separate labels or marking areas. This International Standard uses the terms “part marking” and “item marking” interchangeably. Unless otherwise stated, this document will use the term “item marking” to describe both the labeling and direct part marking (DPM) of an item, where DPM includes, but is not limited to, altering (e.g. dot peen, laser etch, chemical etch) as well as additive type processes (e.g. ink jet, vacuum deposition). The purpose of this International Standard is to establish the machine-readable (linear, two dimensional, and composite symbols) and human readable content for direct marking and labeling of items, parts, and components. This International Standard provides a means for items, parts and components to be marked, and read in either fixtured or handheld scanning environments at any manufacturer’s facility and then read by customers purchasing items for subsequent manufacturing operations or for final end use. Intended applications include, but are not limited to supply chain applications, e.g. inventory, distribution, manufacturing, quality control, acquisition, transportation, supply, repair, and disposal. The figures are illustrative and not necessarily to scale or to the quality requirements specified in this International Standard. |  |  |  |  |  |  |  |  |  |
| ISO 19112:2003 Geographic information – Spatial referencing by geographic identifiers | ISO 19912:2003 defines the conceptual schema for spatial references based on geographic identifiers. It establishes a general model for spatial referencing using geographic identifiers, defines the components of a spatial reference system and defines the essential components of a gazetteer. Spatial referencing by coordinates is not addressed in this document; however, a mechanism for recording complementary coordinate references is included.<br>http://www.iso.org/iso/iso_catalogue/catalogue_tc/<br>catalogue_detail.htm?csnumber=26017 | ISO TC 211 | International Standard | 2003 |  | Geospatial Information |  |  |  | 163. |
| ISO Geographic information harmonized ontology | The ISO Geographic information harmonized ontology is an Internet resources that provides standards OWL ontologies to support semantic description of geographic information concepts for the geosemantic Web. | ISO TC 211/GOM | In development | 2015-01 |  | Interoperability of geographic information | GeoSemantic Web | Web accessibility of geographic information |  | 164. |
| ISO 19136:2007, Geographic information -- Geography Markup Language (GML) | The Geography Markup Language (GML) is an XML encoding in compliance with ISO 19118 for the transport and storage of geographic information modelled in accordance with the conceptual modelling framework used in the ISO 19100 series of International Standards and including both the spatial and non-spatial properties of geographic features.<br>ISO 19136:2007 defines the XML Schema syntax, mechanisms and conventions that:<br>• provide an open, vendor-neutral framework for the description of geospatial application schemas for the transport and storage of geographic information in XML;<br>• allow profiles that support proper subsets of GML framework descriptive capabilities;<br>• support the description of geospatial application schemas for specialized domains and information communities;<br>• enable the creation and maintenance of linked geographic application schemas and datasets;<br>• support the storage and transport of application schemas and data sets;<br>• increase the ability of organizations to share geographic application schemas and the information they describe.<br>Implementers may decide to store geographic application schemas and information in GML, or they may decide to convert | ISO TC 211/WG4 | IS | 2007 |  | Interoperability of geographic information |  | accessibility of geographic information on the Internet |  | 165. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | from some other storage format on demand and use GML only for schema and data transport.<br>NOTE If an ISO 19109 conformant application schema described in UML is used as the basis for the storage and transportation of geographic information, ISO 19136 provides normative rules for the mapping of such an application schema to a GML application schema in XML Schema and, as such, to an XML encoding for data with a logical structure in accordance with the ISO 19109 conformant application schema. | | | | | | | | | |
| ISO/TS 19130:2010, Geographic Information – Imagery Sensor Models for Geopositioning | ISO/TS 19130:2010 identifies the information required to determine the relationship between the position of a remotely sensed pixel in image coordinates and its geoposition. It supports exploitation of remotely sensed images and defines the metadata to be distributed with the image to enable user determination of geographic position from the observations | ISO TC 211/WG6 | TS | 2010 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 166. |
| ISO/TS 19139-2:2012, Geographic information -- Metadata -- XML schema implementation -- Part 2: Extensions for imagery and gridded data | ISO 19139-2:2012 defines Geographic Metadata for imagery and gridded data (gmi) encoding. This is an XML Schema implementation derived from ISO 19115-2. | ISO TC 211/WG6 | TS | 2012 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 167. |
| ISO 19115-1 Geographic Information – Metadata – Part 1: Fundamentals | ISO 19115-1 ISO 19115 defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services. | ISO TC 211/WG7 | FDIS | 2014 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 168. |
| ISO 19150-2, Geographic information -- Ontology -- Part 2: Rules for developing ontologies in the Web Ontology Language (OWL) | ISO/DIS 19150-2 defines the conversion of the UML static view modeling elements used in the ISO geographic information standards into OWL. It further defines conversion rules for describing application schemas based on the General Feature Model defined in ISO 19109 into OWL. | ISO TC 211/WG7 | DIS | 2015-01 | | Interoperability of geographic information | GeoSemantic Web | Web accessibility of geographic information | | 169. |
| ISO/TS 19139:2007, Geographic information -- Metadata -- XML schema implementation | ISO/TS 19139:2007 defines Geographic MetaData XML (gmd) encoding, an XML Schema implementation derived from ISO 19115. | ISO TC 211/WG7 | TS | 2007 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 170. |
| ISO/TS 19150-1:2012, Geographic information -- Ontology -- Part 1: Framework | ISO/TS 19150-1:2012 defines the framework for semantic interoperability of geographic information. This framework defines a high level model of the components required to handle semantics in the ISO geographic information standards with the use of ontologies. | ISO TC 211/WG7 | TS 1st Edition | 2012 | | Interoperability of geographic information | GeoSemantic Web | Web accessibility of geographic information | | 171. |
| ISO 19145:2013, Geographic information -- Registry of representations of geographic point location | ISO 19145:2013 specifies the process for establishing, maintaining and publishing registers of representation of geographic point location in compliance with ISO 19135. It identifies and describes the information elements and the structure of a register of representations of geographic point location including the elements for the conversion of one representation to another.<br>ISO 19145:2013 also specifies the XML implementation of the required XML extension to ISO/TS 19135-2, for the implementation of a register of geographic point location representations. | ISO TC 211/WG9 | IS | 2013 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 172. |
| ISO 19156:2011 Geographic Information – Observations and Measurements | ISO 19156:2011 defines a conceptual schema for observations and for features involved in sampling when making observations. These provide models for the exchange of describing observation acts and their results, both within and between different communities. | ISO TC 211/WG9 | IS | 2011 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 173. |
| ISO 6709:2008, Standard representation of geographic point location by coordinates | ISO 6709:2008 is applicable to the interchange of coordinates describing geographic point location. It specifies the representation of coordinates, including latitude and longitude, to be used in data interchange. It additionally specifies representation of horizontal point location using coordinate types other than latitude and longitude. It also specifies the representation of height and depth that can be associated with horizontal coordinates. Representation includes units of measure and coordinate order. | ISO TC 211/WG9 | IS | 2008 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 174. |
| ISO/TS 19135-2:2012, Geographic information - Procedures for item registration -- Part 2: XML schema implementation | ISO/TS 19135-2:2012 specifies the XML implementation of the XML ISO 19135 for the implementation of a geographic items register. | ISO TC 211/WG9 | TS | 2012 | | Interoperability of geographic information | | accessibility of geographic information on the Internet | | 175. |
| ISO/IEC 13157-1:2010 Information technology — Telecommunications and information exchange between | This International Standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.<br>NOTE 1 NFC-SEC is exclusively designed for the data exchange | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Security, Privacy and Authentication | Security Encryption Framework | NFC (Near Field Communication) | | 176. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| systems — NFC Security —<br>Part 1: NFC-SEC NFCIP-1 security services and protocol | protocol of ISO/IEC 18092.<br>NOTE 2 This International Standard does not address application specific security mechanisms (as typically needed for smart card related use cases and standardized in the ISO/IEC 7816 series). NFC-SEC may complement application specific security mechanisms of ISO/IEC 7816. | | | | | | | | | |
| ISO/IEC 13157-2:2010<br>Information technology — Telecommunications and information exchange between systems — NFC Security —<br>Part 1: NFC-SEC NFCIP-1 security services and protocol | This International Standard specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the PDUs and protocol for those services.<br>NOTE 1 NFC-SEC is exclusively designed for the data exchange protocol of ISO/IEC 18092.<br>NOTE 2 This International Standard does not address application specific security mechanisms (as typically needed for smart card related use cases and standardized in the ISO/IEC 7816 series). NFC-SEC may complement application specific security mechanisms of ISO/IEC 7816. | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Security, Privacy and Authentication | Security Encryption Protocol | NFC (Near Field Communication) | | 177. |
| ISO/IEC 16353:2011<br>Information technology — Telecommunications and information exchange between systems — Front-end configuration command for NFC-WI (NFC-FEC) | This International Standard specifies commands for the Near Field Communication Wired Interface (NFC-WI) specified in ISO/IEC 28361. The commands allow exchange of control and state information between the transceiver and the front-end. | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Communication and Networking | API for NFC Wired Interface | NFC (Near Field Communication) | | 178. |
| ISO/IEC 18092:2013<br>Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) | This International Standard defines communication modes for Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupled devices operating at the centre frequency of 13,56 MHz for interconnection of computer peripherals. It also defines both the Active and the Passive communication modes of Near Field Communication Interface and Protocol (NFCIP-1) to realize a communication network using Near Field Communication devices for networked products and also for consumer equipment. This International Standard specifies, in particular, modulation schemes, codings, transfer speeds, and frame format of the RF interface, as well as initialisation schemes and conditions required for data collision control during initialisation. Furthermore, this International Standard defines a transport protocol including protocol activation and data exchange methods.<br>Information interchange between systems also requires, at a minimum, agreement between the interchange parties upon the interchange codes and the data structure. | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Communication and Networking | RF Interface and Low Level Protocol | NFC (Near Field Communication) | | 179. |
| ISO/IEC 19369:2014<br>Information technology — Telecommunications and information exchange between systems — NFCIP-2 Test Methods | This International Standard specifies requirements to verify NFCIP-2 mode selection and initial communication in the selected modes. The Test Management Service Data Units and the interface over which they are exchanged are out of scope. | ISO/ IEC JTC 1/SC 6 | DIS | 1.9.2014 | Conformance Testing | Communication and Networking | RF Interface and Low Level Protocol | NFC (Near Field Communication) | | 180. |
| ISO/IEC 21481:2012<br>Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol -2 (NFCIP-2) | ISO/IEC 18092, ISO/IEC 14443 and ISO/IEC 15693 specify the radio frequency signal interface, initialization, anti-collision and protocols for wireless interconnection of closely coupled devices and access to contactless integrated circuit cards operating at 13,56 MHz.<br>This International Standard specifies the communication mode selection mechanism, designed not to disturb any ongoing communication at 13,56 MHz, for devices implementing ISO/IEC 18092, ISO/IEC 14443 or ISO/IEC 15693. This International Standard requires implementations to enter the selected communication mode as specified in the respective International Standard. The communication mode specifications, however, are outside the scope of this International Standard. | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Communication and Networking | RF Interface and Low Level Protocol | NFC (Near Field Communication) | | 181. |
| ISO/IEC 22536:2013<br>Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and | This International Standard is part of a suite of standards that specify tests for ISO/IEC 18092. It defines test methods for the RF-interface. This International Standard specifies RF-test methods for NFCIP-1 devices with antennas fitting within the rectangular area of 50 mm by 40 mm.<br>This test standard, the first of two parts, specifies compliance tests for the RF interface of ISO/IEC 18092 devices. The | ISO/ IEC JTC 1/SC 6 | IS | | Confor -mance Testing | Communication and Networking | RF Interface | NFC (Near Field Communication) | | 182. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Protocol (NFCIP-1) — RF interface test methods | companion test standard ISO/IEC 23917 specifies protocol tests for ISO/IEC 18092. | | | | | | | | | |
| ISO/IEC 23917:2005 Information technology — Telecommunications and information exchange between systems — NFCIP-1 — Protocol Test Methods | This International Standard specifies protocol test methods for ISO/IEC 18092 in addition to those specified in ISO/IEC 22536. | ISO/ IEC JTC 1/SC 6 | IS | | Confor -mance Testing | Communication and Networking | Low Level Protocol | NFC (Near Field Communication) | | 183. |
| ISO/IEC 28361 :2007 Information technology — Telecommunications and information exchange between systems — Near Field Communication Wired Interface (NFC-WI) | This Standard specifies the digital wire interface between a Transceiver and a Front-end. The specification includes the signal wires, binary signals, the state diagrams and the bit encodings for three data rates. | ISO/ IEC JTC 1/SC 6 | IS | | Technology | Communication and Networking | PHY for NFC Wired Interface | NFC (Near Field Communication) | | 184. |
| ISO/IEC 14908-4, Information technology -- Control network protocol -- Part 4: IP communication | ISO/IEC 14908-4:2011 specifies the transporting of the Control Network Protocol (CNP) packets for commercial local area control networks over Internet Protocol (IP) networks using a tunnelling mechanism wherein the CNP packets are encapsulated within IP packets. It applies to both CNP nodes and CNP routers. The purpose of ISO/IEC 14908-4:2011 is to ensure interoperability between various CNP devices that wish to use IP networks to communicate using the CNP | ISO/IEC JTC 1/ SC 6 | Technology | | | network level | | | | 185. |
| ISO/IEC 18328-3 ICC-managed devices – Part 3: organization, security and commands for interchange | This standard specifies the logical interface of an application supporting the necessary security features in a card IC which communicates with the external world by a physical interface supporting APDUs. This application supports the usage of electronic devices.<br>This involves the design of commands, data structures and security mechanisms which are required to handle the data and handling the additional devices itself. The handling of the additional devices is always controlled by the card IC. External inputs or outputs shall be managed by the existing interfaces.<br>This International Standard deals not with physical characteristics of the card and interface technology but only with the logical aspects. Management of data for additional devices that is not subdued by the ICC operating system or application control is out of scope of this standard.<br>Definitions of coding requiring for "trust assessment" of the managed data like warning, font, colour etc is in the scope of ISO/IEC 18328 part 2. A description of the logical internal interface functionality used by the operating system of the ICC or by device drivers, if any, is also part of the standard.<br>Due to the fact that relevant technologies may evolve or be adopted very fast, this International Standard defines commands and structures supporting extensions and adaptations. | ISO/IEC JTC 1/SC 17/WG 4 | Working Draft | | | | | | Determines the interchange rules for on and off-card ICC-manages devices including sensors/transducers | 186. |
| ISO/IEC 19286 ICC protocols and services ensuring privacy | This international standard envisions:<br>• to strengthen common technical measures about privacy enabling interchange at card edge, and to facilitate its adoption;<br>• to harmonise privacy properties or privacy framework definitions when existing;<br>• to address generic technical features related to privacy implementation at card edge (interchange) regardless of the cryptographic mechanisms by e.g. considering transactional aspects as asynchronous protocols involving several parties in privacy context;<br>• to specify how the mechanisms for interchange provisioned by ISO IEC 7816 series and ISO/IEC 18328 (Note: not in DIS state) series of standards can contribute to security and privacy;<br>• to specify means for interoperability of privacy enabling attribute discoverability by the outside world;<br>• to specify requirements for attribute based credential handling.<br>This standard identifies and specifies data objects, command sets and interfaces for ICCs and ICC applications in the form of protocols that provide card interfaces that support cryptographically-based privacy protocols. Privacy protocols which are provided in a generic context, are adopted for | ISO/IEC JTC 1/SC 17/WG 4 | Working draft | | | | | | | 187. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | distributed systems including ICCs. Additionally, existing device protocols ensuring authentication and providing a secure channel are enhanced in regard to privacy protection. | | | | | | | | | |
| ISO/IEC 7816 Identification cards - Integrated circuit cards (serie) | All the series but mainly part 4 Organization, security and commands for interchange:<br>This part of **Error! Reference source not found.** is intended to be used in any sector of activity. It specifies:<br>- contents of command-response pairs exchanged at the interface,<br>- means of retrieval of data elements and data objects in the card,<br>- structures and contents of historical bytes to describe operating characteristics of the card,<br>- structures for applications and data in the card, as seen at the interface when processing commands,<br>- access methods to files and data in the card,<br>- a security architecture defining access rights to files and data in the card,<br>- means and mechanisms for identifying and addressing applications in the card,<br>- methods for secure messaging,<br>- access methods to the algorithms processed by the card. It does not describe these algorithms.<br>It does not cover the internal implementation within the card or the outside world.<br>This part of **Error! Reference source not found.** is independent from the physical interface technology. It applies to cards accessed by one or more of the following methods: contacts, close coupling and radio frequency. If the card supports simultaneous use of more than one physical interface, the relationship between what happens on different physical interfaces is out of the scope of this edition of **Error! Reference source not found.**-4. | ISO/IEC JTC 1/SC 17/WG 4 | 3rd edition of part 4 was published in April 2013. | | | | | | Describes most of the security kernel for interchange at SE main I/O interface | 188. |
| ISO/IEC 18023-1:2006 , Information technology – SEDRIS – Part 1: Functional specification | ISO/IEC 18023-1 addresses the concepts, syntax and semantics for the representation and interchange of environmental data. This part of ISO/IEC 18023 specifies a data representation model for expressing environmental data, the data types and classes that constitute the data representation model, and an application program interface that supports the storage and retrieval of data using the data representation model. The standard also specifies topological, rule-based, and other constraints that ensure appropriate data can be available for applications that rely on automatically generated behaviours when interacting with environmental data. | ISO/IEC JTC 1/SC 24 | Published.<br>IS Edition 1, Amd1. | May 2012 | Technology | Interoperability. Environmental information semantics, organization, representation, and sharing. | Representation, semantics, modeling, and sharing of environmental data and concepts. Data models, structures, and relationships of objects and concepts in real and virtual environments. | Heterogeneous and networked applications. Supports autonomous and environment-sensing systems/applications. Large data sets and analytics. Modeling and representation of integrated environmental information. | | 189. |
| ISO/IEC 18025:2014 , Information technology – Environmental Data Coding Specification (EDCS) | ISO/IEC 18025 provides mechanisms to unambiguously specify objects used to model environmental concepts. Labels and codes are specified as a standard way of identifying the concepts. Environmental phenomena are specified in categories that include, but are not limited to, abstract concepts, airborne particulates, animals, atmosphere and atmospheric conditions, bathymetric physiography, electromagnetic and acoustic phenomena, equipment, extraterrestrial phenomena, hydrology, ice, man-made structures, ocean and littoral surface phenomena, oceanographic conditions, physiography, space, surface materials and vegetation. | ISO/IEC JTC 1/SC 24 | Published.<br>IS Edition 2. | February 2014 | Technology | Environmental concept semantics and definitions. Dictionaries of terms. Semantic interoperability. | Definition of environmental concepts and features, and their properties, characteristics, units, and metadata. Extensible through registration of new entries. | Semantics interoperability of concepts and phenomena. Support for human and machine understanding. Information models, representation, and modeling of environmental content in heterogeneous systems. | | 190. |
| ISO/IEC 18026:2009 , Information technology – Spatial Reference Model (SRM) | ISO/IEC 18026 specifies the Spatial Reference Model (SRM) defining relevant aspects of spatial positioning and related information processing. The SRM allows precise and unambiguous specification of geometric properties such as position (location), direction, and distance. The SRM addresses the needs of a broad community of users, who have a range of accuracy and performance requirements in computationally intensive applications. The application program interface supports more than 30 forms of position representation. To ensure that spatial operations are performed consistently, the application program interface specifies conversion operations with functionality defined to ensure high precision transformation between alternative representations of geometric properties. | ISO/IEC JTC 1/SC 24 | Published.<br>IS Edition 2.<br>A revision is under development. | February 2010 | Technology | Interoperability between the representations of position, coordinate, or orientation data. Spatial and time-dependent reference frames. Position, orientation, and distance specifications. Coordinate transformations and other position and orientation related calculations. | Unified specification, definition, and relationships between reference frames, coordinate systems, datums, distance, and rotation/orientation representations and operations for all or parts of Earth and other object. | Position specification and/or inter-conversion for applications that depend on spatial referencing. Computation, transformation or conversion between variety of representations of spatial reference frames, coordinate systems, distances, and orientations. | | 191. |
| ISO/IEC 18521-1:201x – Mixed and Augmented Reality Concepts – Part 1: The reference model | This part of ISO/IEC 18521 defines a structure within which current and future International Standards for augmented and mixed reality area shall be compared and their relationships described. It defines a set of principles, concepts, and their inter- | ISO/IEC JTC 1/SC 24 and ISO/IEC JTC 1/SC 29 Jointly developed | WD | 2016 | Technology | Mixture of real and virtual environments | A device-independent architecture for mixed and augmented reality content, components, | Designed to support a wide variety of application domains and implementation | As this is being developed jointly by SC24 and SC29, it may well be assigned a new | 192. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | relationships, which is applicable to the complete range of future augmented and mixed reality standards. | | | | | | and systems. | environments. | document number that is independent of either SC. | |
| ISO/IEC 18521-2:201x – Mixed and Augmented Reality Concepts – Part 2: Physical sensors | This part of ISO/IEC 18521 defines a framework and base components for representing and controlling sensor based mixed reality worlds. It defines concepts, system functions, and how to integrate 3D virtual worlds and physical sensors and their interfaces in order to provide mixed reality applications with physical sensor interfaces. It defines an exchange format necessary for transferring and storing data between physical sensor based mixed and augmented reality applications | ISO/IEC JTC 1/SC 24 | WD | 2016 | Technology | Integration and general sensor definition of real sensors and their representations in mixed and augmented reality applications. | Definition of behaviours, characteristics, and representations for a variety of sensor devices. | Designed to support a wide variety of application domains and implementation environments. | | 193. |
| ISO/IEC 18521-3:201x – Mixed and Augmented Reality Concepts – Part 3: Real character representation | This part of ISO/IEC 18521 defines a reference model and base components for representing and controlling real characters in mixed and augmented reality (MAR) worlds. It defines concepts, a reference model, system framework, functions, and how to integrate 3D virtual worlds and real characters and their interfaces in order to provide MAR applications with real characters interfaces. It defines an exchange format necessary for transferring and storing data between real characters based MAR applications. | ISO/IEC JTC 1/SC 24 | WD | 2016 | Technology | Integration of the representation of real characters with a variety of virtual environments. | Definition of how images of real characters (e.g. human beings) can interact with a virtual environment. | Designed to support a wide variety of application domains and implementation environments. | | 194. |
| ISO/IEC 19775-1:2013 – Extensible 3D (X3D) – Part 1: Architecture and base components<br>and<br>ISO/IEC 19776 – X3D encodings | ISO/IEC 19775 defines a software system that integrates network-enabled 3D graphics and multimedia. Conceptually, each X3D application is a 3D time-based space that contains graphic and aural objects that can be dynamically modified through a variety of mechanisms. This includes the ability to interact with the presented information.<br>ISO/IEC 19776 specifies the appropriate companion X3D encodings for the presentation and/or transmission of the scene graph. | ISO/IEC JTC 1/SC 24 | Published. IS Edition 3. A revision is under development. | November 2013 | Technology | Visualization and interaction with 2D and 3D computer graphics and multimedia on the World Wide Web and locally. | Architecture and syntax for the representation of dynamic and interactive 3D graphics and multimedia content for local and Internet networks and file systems. | Visualization of large data sets. Modeling and rendering of 3D scenes. Designed to support a wide variety of application domains and implementation environments. | | 195. |
| ISO/IEC 19775-2:2010 – Extensible 3D (X3D) – Part 2: Scene access interface<br>and<br>ISO/IEC 19777 – X3D language bindings | This part of ISO/IEC 19775 specifies a standard set of services that are made available by a browser so that an author can access the scene graph while it is running. Such access is designed to support interaction with, and modification of, the scene graph.<br>ISO/IEC 19777 specifies the appropriate companion X3D language bindings for interacting with the scene graph. | ISO/IEC JTC 1/SC 24 | Published. IS Edition 2. A revision is under development. | September 2011 | Technology | Visualization and interaction with 2D and 3D computer graphics and multimedia on the World Wide Web and locally. | Programmatic access to 3D scene graphs from within the scene graph and from external environments such as HTML and independent application programs | Connection of application content to graphical content. Designed to support a wide variety of application domains and implementation environments. | | 196. |
| ISO/IEC 18372 Information technology – Rapid IO(TM) interconnect specification | Addresses the need for a high-performance low pin count packet-switchedsystem level interconnect to be used in a variety of applications as an open standard | ISO/IEC JTC 1/SC 25 | Technology | | | network level | | | | 197. |
| ISO/IEC 24740 Information technology – Responsive Link (RL) | Specifies the communication protocol and interface of Responsive Link, a real-time communications method for parallel /distributed control | ISO/IEC JTC 1/SC 25 | Technology | | | network level | | | | 198. |
| ISO/IEC 29145-1: IT– Wireless beacon-enabled energy efficient mesh network (WiBEEM) standard for wireless home network services – Part 1: PHY layer | This part of ISO/IEC 29145 specifies the physical (PHY) layer of WiBEEM (Wireless Beacon-enabled Energy Efficient Mesh network) protocol for wireless home network services that supports a low power-consuming wireless mesh network topology as well as device mobility and QoS. | ISO/IEC JTC 1/SC 25 | | | | | | | | 199. |
| ISO/IEC 29145-2: IT– Wireless beacon-enabled energy efficient mesh network (WiBEEM) standard for wireless home network services – Part 2: MAC layer | This part of ISO/IEC 29145 specifies the MAC of the WiBEEM (Wireless Beacon-enabled Energy Efficient Mesh network) protocol for wireless home network services that supports a low power-consuming wireless mesh network as well as device mobility and QoS. | ISO/IEC JTC 1/SC 25 | | | | | | | | 200. |
| ISO/IEC 29145-3: IT– Wireless beacon-enabled energy efficient mesh network (WiBEEM) standard for wireless home network services – Part 3: NWK layer | This part of ISO/IEC 29145 specifies the network layer (NWK) of the WiBEEM (Wireless Beacon-enabled Energy Efficient Mesh network) protocol for wireless home network services that support a low-power-consuming wireless mesh network as well as device mobility and quality of service. | ISO/IEC JTC 1/SC 25 | | | | | | | | 201. |
| ISO/IEC 10192-1: Home electronic system (HES) interfaces – Part 1: Universal Interface (UI) Class 1 | This part of ISO/IEC 10192 is one of a set of standards describing the characteristics of a specific home control system called the Home Electronic System, HES.<br>This standard specifies the characteristics of the Universal Interface Class 1 that connects devices to the home network in an HES for control applications.<br>This standard informs as to the usefulness of the principles of a UI and forms a basis for new work in this field. | ISO/IEC JTC 1/SC 25/WG 1 | Published | | | | | | | 202. |
| ISO/IEC 10192-3: Home Electronic System (HES) interfaces – Part 3: Modular communications interface for energy management | This standard specifies a modular communication interface (MCI) to facilitate communications with residential devices for applications such as energy management as specified in ISO/IEC 15067-3. The MCI provides a standard interface for energy management signals and messages to reach devices. Such devices may include an Energy Management Agent as specified in ISO/IEC 15067-3, a residential gateway as specified in the ISO/IEC 15045 | ISO/IEC JTC 1/SC 25/WG 1 | NP | 2016 | | | | | | 203. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | series, a sensor, a thermostat, an appliance, or other consumer products.<br>The MCI specifies an interface module typically mounted on a residential device in order to connect that device to a communications medium. The interface to the device is a physical wired connection. An optional translation function is specified for interfacing the module to a communications medium. | | | | | | | | | |
| ISO/IEC 14543-2-1: IT - Home Electronic System (HES) Architecture - Part 2-1: Introduction and device modularity | Home Electronic System (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard specifies the general features as well as the basic functional structure of an HES. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2006) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 204. |
| ISO/IEC 14543-3-1: IT - Home Electronic System (HES) architecture - Part 3-1: Communication layers - Application layer for network based control of HES Class 1 | Home Electronic System (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard specifies the services and protocol of the application layer for use in HES. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2006) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 205. |
| ISO/IEC 14543-3-10: IT - Home Electronic System (HES) architecture - Part 3-10: Wireless Short-Packet (WSP) protocol optimised for energy harvesting – Architecture and lower layer protocols | This part of ISO/IEC 14543 specifies a wireless protocol for low-powered devices such as energy harvested devices in a home environment. This wireless protocol is specifically designed to keep the energy consumption of such sensors and switches extremely low.<br>The design is characterised by<br>-keeping the communications very short, infrequent and mostly unidirectional, and<br>-using communication frequencies that provide a good range even at low transmit power and avoid collisions from disturbers. | ISO/IEC JTC 1/SC 25/WG 1 | Published | | | | | | | 206. |
| ISO/IEC 14543-3-11: IT - Home Electronic System (HES) architecture - Part 3-11: Frequency Modulated Wireless Short-Packet (FMWSP) protocol optimised for energy harvesting – Architecture and lower layer protocols | This part of ISO/IEC 14543 specifies a frequency modulated wireless protocol for low-powered devices such as energy harvested devices in a home environment. This wireless protocol is specifically designed to keep the energy consumption of such sensors and switches extremely low.<br>The design is characterised by<br>-keeping the communications very short, infrequent and mostly unidirectional, and<br>-using communication frequencies that provide a good range even at low transmit power and avoid collisions from disturbers. | ISO/IEC JTC 1/SC 25/WG 1 | NWIP | | | | | | | 207. |
| ISO/IEC 14543-3-2: IT - Home Electronic System (HES) Architecture - Part 3-2: Communication layers - Transport, network and general parts of data link layer for network based control of HES Class 1 | Home Electronic System (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard specifies the services and protocol in a physical layer independent way for the data link, network and transport layer for use in HES. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2006) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 208. |
| ISO/IEC 14543-3-3: IT - Home Electronic System (HES) architecture - Part 3-3: User process for network based control of HES Class 1 | Home electronic system (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard specifies the structure and functioning of servers for the group and interface objects which form the interface between the application layer and the application and management. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2007) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 209. |
| ISO/IEC 14543-3-4: IT - Home Electronic System (HES) architecture - Part 3-4: System management - Management procedures for network based control of HES Class 1 | Home electronic system (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard specifies the general principles for network device management. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2007) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 210. |
| ISO/IEC 14543-3-5: IT - Home Electronic System (HES) architecture - Part 3-5: Media and media dependent layers - Powerline for network based control of HES Class 1 | Home Electronic System (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard defines the mandatory and optional requirements for medium specific physical and data link layer of power line Class 1. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2007) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 211. |
| ISO/IEC 14543-3-6: IT - Home Electronic System (HES) architecture - Part 3-6: Media and media dependent layers - Twisted pair for net-work based control of HES Class 1 | Home electronic system (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard defines the mandatory and optional requirements for the medium specific physical and data link layer for HES Class 1, twisted pair. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2007) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 212. |
| ISO/IEC 14543-3-7: IT - Home Electronic System (HES) architecture - Part 3-7: Media and media dependent layers - Radio frequency for network based control of HES Class 1 | Home electronic system (HES) standards describe the architecture of home control systems including communication and interoperability aspects.<br>This International Standard defines the mandatory and optional requirements for the medium specific physical and data link layer for HES products and systems. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2007) | | Technology/ Interoperability | Communications and Networking | | Smart Home | | 213. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 14543-4: IT – Home Electronic System (HES) architecture – Part 4: Home and building automation in a mixed-use building | This part of ISO/IEC 14543 presents methods for overall building management of the home electronic system (HES) architecture. The interaction of building and home control systems requires a demarcation between building manager versus tenant responsibilities. A method for implementing agreements between building managers and tenants regarding user access to and control of applications via a firewall is specified.<br>This technical report augments series ISO/IEC 14543, the architecture of HES (Home Electronic System), in order to accommodate both home and building automation in a mixed-use building. Both systems may coexist in a building with shops, offices and apartments. Some systems are applicable to the whole building versus the systems which are applicable to individual apartments and offices only. In some cases these systems need to interact. | ISO/IEC JTC 1/SC 25/WG 1 | Published | | | | | | | 214. |
| ISO/IEC 14543-4-1: IT - Home Electronic System (HES) architecture - Part 4-1: Communication layers - Application layer for network enhanced control devices of HES Class 1 | ISO/IEC 14543-4-1:2008(E) specifies the services and protocol of the application layer for usage in Home Electronic Systems (HES). It provides the services and the interface to the user process. Some services are targeted to field level communication between devices. Other services are exclusively reserved for management purposes. Some services can be used for both management and run-time communication. This International Standard is based on ECHONET. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2008) | | Technology | Communications and Networking | | Smart Home | | 215. |
| ISO/IEC 14543-4-2: IT - Home Electronic System (HES) architecture - Part 4-2: Communication layers - Transport, network and general parts of data link layer for network enhanced control devices of HES Class 1 | ISO/IEC 14543-4-2:2008(E) specifies the media independent requirements for the data link layer and the requirements for the network layer and the transport layer for Home Electronic Systems (HES). It gives the frame format for the communications middleware block to minimize message size while fulfilling the requirements of the communications layer structure. It can be used as the communication stack on the physical layers as specified in ECHONET specifications. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2008) | | Technology | Communications and Networking | | Smart Home | | 216. |
| ISO/IEC 14543-4-3: IT - Interconnection of information technology equipment - Home Electronic System (HES) Architecture - Part 4-3: Application layer interface to lower communication layers for network enhanced control devices of HES Class 1 | This part of the ISO/IEC 14543 series specifies the message structure, sequences and protocol of the application layer for use in network enhanced control devices of the Home Electronic System (HES) Class 1. It provides the services and the interface for the user-level process. This application layer protocol is independent of lower communication layers, which support MAC addressing or IP addressing. The communications sequence is based on the application services. | ISO/IEC JTC 1/SC 25/WG 1 | DIS | 2014 | Technology | Communications and Networking | | Smart Home | | 217. |
| ISO/IEC 14543-5-1: IT - Home Electronic System (HES) architecture - Part 5-1: Intelligent grouping and resource sharing for Class 2 and Class 3 - Core protocol | ISO/IEC 14543-5-1:2010(E) series specifies the services and protocol of the application layer for use by IGRS Devices in the Home Electronic System. An IGRS Device (Intelligent Grouping and Resource Sharing Device) includes the communications protocol specified in the multiple parts of ISO/IEC 14543-5. The objective of this document is to enable resource sharing and service collaboration among computers, consumer electronics, and communication devices in a Local Area Network (LAN) or Personal Area Network (PAN) environment, especially in a wireless dynamic network. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2010) | | Technology | Communications and Networking | | Smart Home | | 218. |
| ISO/IEC 14543-5-101: IT - Home Electronic System (HES) Architecture - Part 5-101: Intelligent Grouping and Resource Sharing - Remote AV Access Profile | Defines a device and service interaction mechanism for various applications based on the IGRS Part 5-8: Remote Access Core protocol<br>Two profiles are under development. Additional application profiles will be specified in the future.<br>Part 5-101: Remote AV Access Profile. This part defines the common requirements for IGRS RA AV users/devices in IGRS networks. | ISO/IEC JTC 1/SC 25/WG 1 | NP | | Technology | Applications (Profiles) | | Smart Home | | 219. |
| ISO/IEC 14543-5-102: IT - Home Electronic System (HES) Architecture - Part 5-102: Intelligent Grouping and Resource Sharing - Remote Universal Management Profile | Part 5-102: Remote Universal Management Profile. This part specifies a mechanism for integrating devices with both relatively high and low processing capabilities into IGRS networks. It also specifies universal remote device discovery and a management framework. | ISO/IEC JTC 1/SC 25/WG 1 | NP | | Technology | Applications (Profiles) | | Smart Home | | 220. |
| ISO/IEC 14543-5-11: IT- Home Electronic System (HES) Architecture - Part 5-11: Intelligent Grouping and Resource Sharing - Remote User Interface | Specifies adaptive user interface generation and remote device control mechanisms suitable for different remote access applications and devices. | ISO/IEC JTC 1/SC 25/WG 1 | NP | | Technology | Applications (Interfaces) | | Smart Home | | 221. |
| ISO/IEC 14543-5-12: IT - Home Electronic System (HES) Architecture - Part 5-12: Intelligent Grouping and Resource Sharing Remote Access Test and Verification | Remote Access Test & Verification (under consideration)<br>Defines a standard method to test and verify IGRS-RA compliant devices and service interfaces. | ISO/IEC JTC 1/SC 25/WG 1 | NP | | Test and verification | Communications and Networking | | Smart Home | | 222. |
| ISO/IEC 14543-5-21: IT - Home Electronic System (HES) architecture - | ISO/IEC 14543-5-21:2012(E) specifies the media data stream service profile, the device interaction flow, the request and | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Applications (Profiles) | | Smart Home | | 223. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Part 5-21: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Application profile - AV profile | response message format used in device interaction and the description format of services provided by the device. It is applicable to computers, household appliances and communication devices that implement media data streaming by wired or wireless means. | | | | | | | | | |
| ISO/IEC 14543-5-22: IT - Home Electronic System (HES) architecture - Part 5-22: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Application profile - File profile | ISO/IEC 14543-5-22:2010(E) specifies the file data streaming application profile, device interaction flow model, the request and response messages in the device interaction process, and the service description format of the devices based on Intelligent Grouping and Resource Sharing (IGRS), ISO/IEC 14543-5-1. It is applicable to resource sharing and service collaboration of file data stream among computers, consumer electronics, and communication devices in a Local Area Network (LAN) or Personal Area Network (PAN) environment, especially in a wireless dynamic network. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2010) | | Technology | Applications (Profiles) | | Smart Home | | 224. |
| ISO/IEC 14543-5-3: IT - Home Electronic System (HES) architecture - Part 5-3: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Basic application | ISO/IEC 14543-5-21:2012(E) specifies the media data stream service profile, the device interaction flow, the request and response message format used in device interaction and the description format of services provided by the device. It is applicable to computers, household appliances and communication devices that implement media data streaming by wired or wireless means. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Applications | | Smart Home | | 225. |
| ISO/IEC 14543-5-4: IT - Home Electronic System (HES) architecture - Part 5-4: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Device validation | ISO/IEC 14543-5-4:2010(E) specifies device validation methods for information devices that implement ISO/IEC 14543-5-1. It defines an architecture framework for a device validation system used by test devices and devices under test. Also, it describes and specifies the device interaction process, message exchange requirements and conformance rules. It is applicable to resource sharing and service collaboration among computers, consumer electronics, and communication devices in a Local Area Network (LAN) or Personal Area Network (PAN) environment, especially in a wireless dynamic network. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2010) | | Technology | Authentication (Validation) | | Smart Home | | 226. |
| ISO/IEC 14543-5-5: IT - Home Electronic System (HES) architecture - Part 5-5: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Device type | ISO/IEC 14543-5-5:2012(E) specifies the device type of all devices that conform to ISO/IEC 14543-5-1: Core Protocol, and ISO/IEC 14543-5-2#: Application Profile. It is applicable to all devices that are operating in an IGRS network. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Applications (Device Types) | | Smart Home | | 227. |
| ISO/IEC 14543-5-6: IT - Home Electronic System (HES) architecture - Part 5-6: Intelligent grouping and resource sharing for HES Class 2 and Class 3 - Service type | ISO/IEC 14543-5-6:2012(E) specifies the service types that conform to ISO/IEC 14543-5-1. It is applicable to computers, household appliances and communication devices that implement media or data streaming in a local area network (LAN) or personal area network (PAN) environment by wired or wireless means. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Applications (Service Types) | | Smart Home | | 228. |
| ISO/IEC 14543-5-7: IT - Home electronic system (HES) architecture - Part 5-7: Intelligent Grouping and 3 Resource Sharing - Remote Access System Architecture | Specifies the architecture and framework for the remote access of IGRS devices and services in the Home Electronic System. The remote access communications protocol and application profiles are specified in following parts of this series:<br>ISO/IEC 14543-5-8: Remote Access Core Protocol<br>ISO/IEC 14543-5-9: Remote Access Service Platform<br>ISO/IEC 14543-5-101: Remote AV Access Profile<br>ISO/IEC 14543-5-102: Remote Universal Management Profile<br>ISO/IEC 14543-5-11: Remote User Interface<br>ISO/IEC 14543-5-12: Remote Access Test and Verification<br>The relationships among these parts are specified in this part. | ISO/IEC JTC 1/SC 25/WG 1 | CD | 2015 | Technology | Communications and Networking | | Smart Home | | 229. |
| ISO/IEC 14543-5-8: IT - Home Electronic System (HES) Architecture - Part 5-8: Intelligent Grouping and Resource Sharing - Remote Access Core Protocol | Provides detailed system constructions, system function modules, basic conceptions of IGRS remote access elements and their relationships, message exchange mechanisms and security related specifications.<br>Specifies interfaces between IGRS Remote Access (RA) client and service platforms. Defines co-operative procedures among IGRS RA clients. | ISO/IEC JTC 1/SC 25/WG 1 | NP | 2016 | Technology | Communications and Networking | | Smart Home | | 230. |
| ISO/IEC 14543-5-9: IT - Home Electronic System (HES) Architecture - Part 5-9: Intelligent Grouping and Resource Sharing - Remote Access Service Platform | Specifies the IGRS RA service platform architectures and interfaces among servers in service platforms.<br>Based on the IGRS Part 5-8: Remote Access Core protocol. | ISO/IEC JTC 1/SC 25/WG 1 | NP | | Technology | Communications and Networking | | Smart Home | | 231. |
| ISO/IEC 14762: IT - Functional safety requirements for home and building electronic systems (HBES) | ISO/IEC 14762:2009(E) specifies the general functional safety requirements for HBES following the principles of the basic standard for functional safety IEC 61508. This International Standard sets the requirements for functional safety for Home and Building Electronic Systems (HBES) products and systems, a multi-application bus system where the functions are decentralised, distributed and linked through a common communication process. The requirements may also apply to the | ISO/IEC JTC 1/SC 25/WG 1 | Published (2009) | | Technology | Applications | | Smart Home/Building | | 232. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | distributed functions of any equipment connected in a home or building control system if no specific functional safety standard exists for this equipment or system. This International Standard only addresses HBES products. HBES and HES products in this International Standard are for non-safety related applications. | | | | | | | | | |
| ISO/IEC 15045-1: IT - Home Electronic System (HES) Gateway - Part 1: A residential gateway model for HES | The Residential Gateway (RG) is a device of the Home Electronic System (HES) that connects home network domains to network domains outside the house. It supports communications among devices within the premises, and among systems, service providers, operators and users outside the premises. The RG enables service and content providers to deliver services such as entertainment, video and broadband digital streams, monitoring for health care, security and occupancy, home appliance control and preventive maintenance, remote metering, and energy management. The RG specified by this standard does not imply the use of any particular protocol such as IP and it is recognised that many forms of the RG will exist using many types of data such as analogue video and broadband digital streams. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2004) | | Technology | Communications and Networking | | Smart Home | | 233. |
| ISO/IEC 15045-2: IT - Home Electronic System (HES) Gateway - Part 2: Modularity and protocol | ISO/IEC 15045-2:2012(E) specifies a gateway architecture that provides an interconnection between one or more Wide Area Networks (WANs) and one or more Home Area Networks (HANs). It is not needed for a "simple gateway" linking one WAN to one HAN where there is no intention of future expansion. It applies to a "distributed gateway," and is also referred to in ISO/IEC 15045-1 as the Complex Modular Gateway. Also, it specifies how separate gateways in a single house can interoperate to provide coordinated functions. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Communications and Networking | | Smart Home | | 234. |
| ISO/IEC 15067-3: IT - Home Electronic System - (HES) application model - Part 3: Model of an Energy Management System | ISO/IEC 15067-3:2012(E) specifies an energy management model for programs that manage the consumer demand for electricity using a method known as "demand response". Three types of demand response are specified in this standard: direct control, local control and distributed control. It replaces ISO/IEC TR 15067-3, first edition, published in 2000, and constitutes a technical revision. It includes the following significant technical changes with respect to the previous edition:<br>– the demand response options have been expanded;<br>– distributed energy resources such as local generation and storage have been included;<br>– the terminology for demand response has been aligned with smart grid. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Applications | | Smart Home | | 235. |
| ISO/IEC 18012-1: IT - Home Electronic System - Guidelines for product interoperability - Part 1: Introduction | Specifies requirements for product interoperability in the area of home and building automation systems, with sufficient detail needed to design interoperable Home Electronic System products. The widespread development of many national standard and proprietary networks within and to the home has necessitated a standard for interoperability among home system applications and products from multiple manufacturers. Where widely varying devices need to interoperate, it is desirable that they do so seamlessly to present a single, uniform network and hence to deliver a variety of applications. Examples of such applications are lighting control, environmental control, audio/video equipment control and home security.<br><br>Although a single uniform home control system would simplify operations, this standard recognises that multiple different networks may co-exist in the same house, and therefore applies to devices connected to a single home control system or to different home control systems. It ensures that, where applications on the same or dissimilar networks co-exist within premises and are required to interoperate, they will do so in a safe, reliable, predictable and consistent manner. It specifies requirements to assure that devices from multiple manufacturers work together to provide a specific application; a specific device could also be used for multiple applications. Interoperability requirements are given with respect to safety, addressing, applications, transport of information, management, and set-up of devices/elements within home networks - static and/or dynamic binding between objects.<br><br>This part defines the components of interoperability for the purpose of providing a framework within which subsequent parts of the standard will be drafted. This part applies to components within networks, between networks and located within dissimilar networks, as well as to devices located at the junction of | ISO/IEC JTC 1/SC 25/WG 1 | Published (2004) | | Technology | Communications and Networking | | Smart Home | | 236. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | dissimilar networks. | | | | | | | | | |
| ISO/IEC 18012-2: IT - Home Electronic System - Guidelines for product interoperability - Part 2: Taxonomy and application interoperability model | ISO/IEC 18012-2:2012(E) specifies a taxonomy and application interoperability model for the interoperability of products in the area of home systems. It also specifies an interoperability framework to allow products from multiple manufacturers to work together in order to provide a specific application. It describes a application process that exists above the OSI reference model (ISO/IEC 7498-1) stack, with sufficient detail needed to establish interoperable applications in this domain. It is applicable to: single implementation home electronic system networks, connected devices and applications, multiple implementation home electronic system networks, connected devices and applications, automatically configured devices, manually configured devices and manually configured groups/clusters of devices. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2012) | | Technology | Communications and Networking | | Smart Home | | 237. |
| ISO/IEC 18012-3: IT – Interconnection of information technology equipment – Home Electronic System - Guidelines for Product Interoperability - Part 3: Lexicon | A lexicon that defines interoperability domain base objects and their associated properties and input/output event types (i.e., in the form of a list of interoperability domain sensor, actuator, and control objects), and object state actions, which can be used to define application models | ISO/IEC JTC 1/SC 25/WG 1 | NWIP | 2016 | Technology | Communications and Networking | | Smart Home | | 238. |
| ISO/IEC 18012-4: IT – Interconnection of information technology equipment – Home Electronic System - Guidelines for Product Interoperability - Part 4: Event encoding | An event format that defines the encoding of individual events in the Interoperability Domain (ID). This event format will be used to encode events for exchanged across the Event Bus within the ID. | ISO/IEC JTC 1/SC 25/WG 1 | NWIP | 2016 | | | | | | 239. |
| ISO/IEC 18012-5-1: IT – Interconnection of information technology equipment – Home Electronic System - Guidelines for Product Interoperability - Part 5-1 Community interface | Specifies an application interoperability model of a community service to support interoperability between a community system and the HES. The application interoperability model is defined for the link between the community system and the HES in order to provide community services to the residents of a complex. | ISO/IEC JTC 1/SC 25/WG 1 | NWIP | 2016 | | | | | | 240. |
| ISO/IEC 18012-5-2: IT - Interconnection of information technology equipment – Home Electronic System – Guidelines for Product Interoperability – Part 5-2 Home control application model for smart devices | Specifies an application interoperability model to enable use of smart devices (such as smart phones) for management and control of HES devices. The application interoperability model is defined for the link between smart devices and the HES in order to provide home control services through smart devices to the user. | ISO/IEC JTC 1/SC 25/WG 1 | NWIP | 2106 | Technology | Communications and Networking | | Smart Home | | 241. |
| ISO/IEC 24767-1: IT - Home network security - Part 1: Security requirements | ISO/IEC 24767-1:2008 specifies the security requirements that may come from inside or outside a home. This standard gives guidance for the design of security mechanisms applied either inside home networks or through the Internet, and it provides means to analyse the risks for each networked device and to define its specific security requirements. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2008) | | Technology | Security | | Smart Home | | 242. |
| ISO/IEC 24767-2: IT - Home network security - Part 2: Internal security services - Secure communication protocol for middleware (SCPM) | ISO/IEC 24767-2:2009(E) specifies security in a home network for equipment with limited IT capability. Secure Communication Protocol for Middleware (SCPM) is designed to support network security for equipment which is not capable of supporting Internet security protocols. SCPM provides the security services at the network layer and the protocol does not rely on any specific media transmission. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2009) | | Technology | Security | | Smart Home | | 243. |
| ISO/IEC 29341 Series (94 Parts): UPnP Device Architecture | ISO/IEC 29341 defines UPnP technology which describes an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. UPnP technology provides a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices. The UPnP Device Architecture (UDA) is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. A device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. Finally, a device can leave a network smoothly and automatically without leaving any unwanted state behind. The technologies leveraged in the UPnP architecture include Internet protocols such as IP, TCP, UDP, HTTP, and XML. Like the Internet, contracts are based on wire protocols that are declarative, expressed in XML, and communicated via HTTP. | ISO/IEC JTC 1/SC 25/WG 1 | Published (2008~2011) | | Technology | Communications and Networking | | N/A | | 244. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 30100-1: IT - Interconnection of information technology equipment – Home Electronic System - Home Network Resource Management – Part 1: Requirements | ISO/IEC 30100-1 specifies the minimum requirements of a home network resource management architecture to deliver applications in a safe and future-proof way without being prescriptive. The purpose of this standard is to collect all available home network information from different types of home network elements and protocols, and to provide the inter-relationships among the elements of this information. This standard also describes user requirements and functional requirements for the management of home network entities as a resource.<br>ISO/IEC 30100-1 specifies management requirements with respect to<br>device management<br>network topology<br>auto-configuration<br>device diagnosis<br>software management<br>This document specifies how a home resource management system defines, organises, diagnoses, manages home resources and combines them. This document does not specify what kind of resources will be defined.<br>This part of ISO/IEC 30100 specifies the minimum requirements of a home network resource management architecture in order to deliver applications in a safe and future-proof way without being prescriptive. It also describes user requirements and functional requirements.<br>This part of ISO/IEC 30100<br>defines resources of a home network such as devices, networks and services,<br>specifies an information model of the relationship among home network resources and<br>specifies management application procedures based on home resource model.<br>This document defines new terminology for resources (abstraction of device, network, service and location) in the home area network. It also specifies the general information model and relationship of resources.<br>This document specifies how a home resource management system defines, organises, diagnoses, manages the home resources and combines them. This document does not specify what kind of resources will be defined.<br>The architecture of this standard is targeted as generic usage. It is required to have corresponded security countermeasures for each of specific use cases. For example, there are laws and regulations in Smart-Grid, health care, and credit card solutions, etc., and to apply this standard, it is needed to have corresponding security and privacy policy for them.<br>For applying this standard, it is needed to decide on security policies (security requirement) in each usage category, and it is needed to have the suitable data structure (XML schema). | ISO/IEC JTC 1/SC 25/WG 1 | DIS | 2016 | Technology | Communications and Networking | | Smart Home | | 245. |
| ISO/IEC 30100-2: IT - Interconnection of information technology equipment – Home Electronic System - Home Network Resource Management - Part 2: Architecture | ISO/IEC 30100-2 defines the general information model and architecture for managing the resources in a home network. Home network resources are managed objects that provide home network services. Essential home resources include device, network and service resources.<br>The objectives of this document are to:<br>Define terminology that describes logical resources of devices, networks and services in a home area network<br>Specify the logical information model for describing relations among resources<br>Describe the basic logical functional procedures of home area networks (e.g. remote maintenance, auto-configuration, fault processing). | ISO/IEC JTC 1/SC 25/WG 1 | CD | 2016 | Technology | Communications and Networking | | Smart Home | | 246. |
| ISO/IEC 30100-3: IT - Interconnection of information technology equipment - Home Electronic System - Home Network Resource Management - Part 3: Management applications | ISO/IEC 30100-3 specifies a control and management interface for the integrated home network resources at the top of the interoperability framework specified by ISO/IEC 18012-1. Methods are specified for controlling and managing home network resources through a consistent interface regardless of the underlying home network middleware technologies. Based on the home resource management interface, a management application specifies HES device control services and fault management services. This part of the ISO/IEC 30100 series specifies the communications data formats and functions for messages sent between the objects of a resource management process and the objects of one or more management | ISO/IEC JTC 1/SC 25/WG 1 | DIS | 2016 | Technology | Communications and Networking | | Smart Home | | 247. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | applications. |  |  |  |  |  |  |  |  |  |
| ISO/IEC TR 10192-2: Home Electronic System (HES) interfaces – Part 2: Simple Interface Type 1 | This part of ISO/IEC 10192-2 specifies the mechanical, electrical, functional and procedural characteristics of a specific Simple Interface (SI). The SI type 1 is a physical interface realized between the SI type 1 device and the SI type 1 Network Access Unit, NAU. It also serves as a reference point. | ISO/IEC JTC 1/SC 25/WG 1 | Published |  |  |  |  |  |  | 248. |
| ISO/IEC 27009<br>Sector-specific application of ISO/IEC 27001 – Requirements | This International Standard defines the requirements for the use of ISO/IEC 27001 for sector-specific applications. It explains how to include requirements additional to those in ISO/IEC 27001. This International Standard also explains how to include controls or control sets in addition to ISO/IEC 27001 Annex A. This International Standard also specifies principles on the refinement of ISO/IEC 27001 requirements. This International Standard prohibits requirements which are in conflict with ISO/IEC 27001 requirements.<br>The target audience of this International Standard are entities producing sector-specific standards that relate to ISO/IEC 27001. | ISO/IEC JTC 1/SC 27 | WD | Publication by 2016-04 |  |  |  |  |  | 249. |
| ISO/IEC 10116<br>**Modes of operation for an n-bit block cipher algorithm** | ISO/IEC 10116 specifies modes of operation for a block cipher algorithm, i.e., ECB, CBC,OFB, CFB and CTR. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed. | IS |  |  |  |  |  | 250. |
| ISO/IEC 10118<br>**Hash-functions**<br>Part 1: General<br>Part 2: Hash-functions using an n-bit block cipher<br>Part 3: Dedicated hash-functions<br>Part 4: Hash-functions using modular arithmetic | ISO/IEC 10118 specifies some kinds of hash-functions which map arbitrary strings of bits to a given range. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. (P. 1)<br>3rd ed. (P. 2)<br>3rd ed. (P. 3)<br>1st ed. (P. 4) | IS |  |  |  |  |  | 251. |
| ISO/IEC 11770<br>**Key management**<br>Part 1: Framework<br>Part 2: Mechanisms using symmetric techniques<br>Part 3: Mechanisms using asymmetric techniques 2nd ed. 2008<br>Part 4: Mechanisms based on weak secrets<br>Part 5: Group key management | ISO/IEC 11770 describes general models on which key management mechanisms are based, defines the basic concepts of key management,<br>and defines several kinds of key establishment mechanisms. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed.(P. 1)<br>2nd ed.(P. 2)<br>2nd ed.(P. 3)<br>1st ed.(P. 4)<br>1st ed.(P. 5) | IS |  |  |  |  |  | 252. |
| ISO/IEC 13888<br>**Non-repudiation**<br>Part 1: General<br>Part 2: Mechanisms using symmetric techniques<br>Part 3: Mechanisms using asymmetric techniques | ISO/IEC 13888 specifies for the provision of nonrepudiation services. The goal of the nonrepudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or nonoccurrence<br>of the event or action. The event or act on can be the generation of a message, sending of a message, receipt of a message, submission of a message transport of a message. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed.(P. 1)<br>2nd ed.(P. 2)<br>2nd ed.(P. 3) | IS |  |  |  |  |  | 253. |
| ISO/IEC 14888<br>**Digital signatures with appendix**<br>Part 1: General<br>Part 2: Integer factorization based mechanisms<br>Part 3: Discrete logarithm based mechanisms | ISO/IEC 14888 specifies digital signature mechanisms with appendix. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. (P. 1)<br>2nd ed. (P. 2)<br>2nd ed. (P. 3) | IS |  |  |  |  |  | 254. |
| ISO/IEC 15408<br>Evaluation criteria for IT security<br>Evaluation criteria for IT security | ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed |  | IS |  |  |  |  | 255. |
| ISO/IEC 15945<br>Specification of TTP services to support the application of digital signatures | This International Standard defines the services required to support the application of digital signatures for non-repudiation of creation of a document. Since this implies integrity of the document and authenticity of the creator, the services described can also be combined to implement integrity and authenticity services. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. |  | IS |  |  |  |  | 256. |
| ISO/IEC 15946<br>**Cryptographic techniques based on elliptic curves**<br>Part 1: General<br>Part 5: Elliptic curve generation | ISO/IEC 15946 describes the mathematical background and general techniques in addition to the elliptic curve generation techniques. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. (P. 1)<br>1st ed. (P. 5) | IS |  |  |  |  |  | 257. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 17825 Testing methods for the mitigation of noninvasive attack classes against cryptographic modules | This International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4. | ISO/IEC JTC 1/SC 27 | 4th WD | Publication by 2015-10 | IS | | | | | 258. |
| ISO/IEC 18014<br>**Time-stamping services**<br>Part 1: Framework<br>Part 2: Mechanisms producing independent tokens<br>Part 3: Mechanisms producing linked tokens<br>Part 4: Traceability of time sources | ISO/IEC 18031 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed.(P. 1)<br>2nd ed.(P. 2)<br>2nd ed.(P. 3)<br>DIS (P. 4) | IS | | | | | | 259. |
| ISO/IEC 18028-4<br>IT network security – Part 4: Securing remote access | This International Standard provides guidance for securely using remote access – a method to remotely connect a computer either to another computer or to a network using public networks – and its implication for IT security. In this it introduces the different types of remote access including the protocols in use, discusses the authentication issues related to remote access and provides support when setting up remote access securely. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | Data Carrier | | | | 260. |
| ISO/IEC 18031<br>**Random bit generation** | ISO/IEC 18031 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. | IS | | | | | | 261. |
| ISO/IEC 18032<br>**Prime number generation** | ISO/IEC 18032 presents methods for generating prime numbers as required in cryptographic protocols and algorithms. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | IS | | | | | | 262. |
| ISO/IEC 18033<br>Encry**ption algorithms**<br>Part 1: General<br>Part 2: Asymmetric ciphers<br>Part 3: Block ciphers<br>Part 4: Stream ciphers<br>Part 5: Identity-based ciphers | ISO/IEC 18033 specifies asymmetric ciphers (including identity-based ciphers) and symmetric ciphers (block ciphers and stream ciphers) | ISO/IEC JTC 1/SC 27 | Published<br>1st ed.<br>CD (Part 5) | IS | | | | | | 263. |
| ISO/IEC 18043<br>Selection, deployment and operations of intrusion detection systems | This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection System (IDS). In particular, it addresses the selection, deployment and operations of IDS. It also provides background information from which these guidelines are derived. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed.<br>(under revision as ISO/IEC 27039) | | IS | etc. | etc. | etc. | | 264. |
| ISO/IEC 18045<br>Methodology for IT security evaluation | ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. | | IS | | | | | 265. |
| ISO/IEC 18367<br>Cryptographic algorithms and security mechanisms conformance testing | This International Standard (IS) describes cryptographic algorithms and security mechanisms conformance testing methods.<br>This International Standard is related to ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 specifies the security requirements for cryptographic modules. At a minimum, a cryptographic module shall implement at least one approved security function (i.e., cryptographic algorithm or security mechanism). ISO/IEC 24759 addresses the test requirements for each of the security requirements in ISO/IEC 19790. However ISO/IEC 24759 does not address test methods for cryptographic algorithms and security mechanisms conformance testing.<br>This International Standard is related to SC27/WG2 Cryptographic and security mechanism specifications and the implementation of standardised algorithms and security mechanisms. It takes into account IS 29128 verification of cryptographic algorithms.<br>Conformance testing assures that an implementation of a cryptographic algorithms or security mechanisms is correct whether implemented in hardware, software or firmware or how it performs in a specific operating environment. Testing may consist of known-answer or Monte Carlo testing, or a combination of test methods. Testing may be performed on the actual implementation or modelled in a simulation environment. This standard does not address the efficiency of the algorithms or security mechanisms nor the intrinsic performance. This International Standard will focus on the correctness of the implementation. | ISO/IEC JTC 1/SC 27 | WD | Publication by 2015-10 | IS | | | | | 266. |
| ISO/IEC 18370<br>**Blind digital signatures**<br>Part 1: General<br>Part 2: Discrete logarithm based mechanisms | ISO/IEC 18370 specifies blind digital signature mechanisms which allow a recipient to obtain a signature without giving signer any information about the actual message or resulting signature | ISO/IEC JTC 1/SC 27 | WD (P. 1)<br>WD (P. 2) | IS | Publication by 2016-05 | | | | | 267. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 19592<br>**Secret sharing**<br>Part 1: General<br>Part 2: Fundamental mechanisms | ISO/IEC 19592 specifies mechanisms of secret sharing. | ISO/IEC JTC 1/SC 27 | NP (P. 1)<br>NP (P. 2) | IS | | | | | | 268. |
| ISO/IEC 19772<br>**Authenticated encryption** | ISO/IEC 19772 specifies methods for authenticated encryption, i.e., defined ways of processing a data string for data confidentiality, data integrity and data origin authentication. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | IS | | | | | | 269. |
| ISO/IEC 19790<br>Security requirements for cryptographic modules | ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. | | IS | | | | | 270. |
| ISO/IEC 19792<br>Security evaluation of biometrics | ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 271. |
| ISO/IEC 20008<br>**Anonymous digital signatures**<br>Part 1: General<br>Part 2: Mechanisms using a group public key | ISO/IEC 20008 specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. (P. 1)<br>1st ed. (P. 2) | IS | | | | | | 272. |
| ISO/IEC 20009<br>**Anonymous entity authentication**<br>Part 1: General<br>Part 2: Mechanisms based on signatures using a group public key<br>Part 3: Mechanisms based on blind signatures<br>Part 4: Mechanisms based on weak secrets | ISO/IEC 20009 specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. (P. 1)<br>1st ed. (P. 2)<br>NP (P. 3)<br>WD (P. 4) | IS | | | | | | 273. |
| ISO/IEC 21827<br>Systems Security Engineering -- Capability Maturity Model® (SSECMM®) | ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. | | IS | | | | | 274. |
| ISO/IEC 24745<br>Biometric information protection | ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.It does not include general management issues related to physical security, environmental security and key management for cryptographic techniques. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 275. |
| ISO/IEC 24759<br>Test requirements for cryptographic modules | ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed | | IS | | | | | 276. |
| ISO/IEC 24760-1<br>A framework for identity management --<br>Part 1: Terminology and concepts<br>Part 2: Reference architecture and requirements<br>Part 3: Practice | ISO/IEC 24760-1<br>• defines terms for identity management, and<br>• specifies core concepts of identity and identity management and their relationships.<br>To address the need to efficiently and effectively implement systems that make identity-based decisions ISO/IEC 24760 specifies a framework for the issuance administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations.<br>ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations.<br>Pat 1 of ISO/IEC 24760 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.<br><br>**ISO/IEC 24760-2**<br>This International Standard<br> describes a life cycle model of identity information,<br> provides guidelines for the implementation of systems for the management of identity information, and<br> specifies requirements for the implementation and operation of a framework for identity management. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. (P.1)<br>CD (P.2)<br>WD (P.3) | | IS | | | | | 277. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | This International Standard is applicable to any information system where information relating to identity is processed or stored.<br>**ISO/IEC 24760-3**<br>This part of International Standard provides guidance for good practices for administrating identity management systems.<br>This International Standard is applicable to any information system where information relating to identities is processed or stored. Both identity management system (IMS) in enterprise network and IMS on the Internet are dealt. |  |  |  |  |  |  |  |  |  |
| ISO/IEC 24761 | ISO/IEC 24761 specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. It allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.<br>ISO/IEC 24761 also specifies the cryptographic syntax of an ACBio instance based on an abstract Cryptographic Message Syntax (CMS) schema. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. |  | IS |  |  |  |  | 278. |
| ISO/IEC 27000<br>**Information security management systems --** Overview and vocabulary | This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed. |  | IS |  |  |  |  | 279. |
| ISO/IEC 27001<br>Information security management systems – Requirements | This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system within the context of the organization's business activities and the risks it faces. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed |  | IS |  |  |  |  | 280. |
| ISO/IEC 27002<br>Code of practice for information security controls | This International Standard offers a collection of commonly accepted information security control objectives and controls and includes guidelines for implementing these controls. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed |  | IS |  |  |  |  | 281. |
| ISO/IEC 27003<br>Information security management system implementation guidance | This will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review and improve the ISMS. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed |  | IS |  |  |  |  | 282. |
| ISO/IEC 27004<br>Information security management measurements | This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed<br>under revision |  | IS |  |  |  |  | 283. |
| ISO/IEC 27005<br>Information security risk management | This standard ISO/IEC 27005 provides guidelines for information security risk management. This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed.<br>under revision |  | IS |  |  |  |  | 284. |
| ISO/IEC 27006<br>International accreditation guidelines for the accreditation of bodies operating certification /Registration of information security management systems | The scope of this standard is to specify general requirements a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration. This International Standard follows the structure of ISO/IEC 17021 with the inclusion of additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021 for ISMS certification. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed<br>under revision |  | IS |  |  |  |  | 285. |
| ISO/IEC 27007<br>Guidelines for information security management systems auditing | This International Standard provides guidance on conducting information security management system (ISMS) audits, as well as guidance on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. It is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed |  | IS |  |  |  |  | 286. |
| ISO/IEC 27010<br>Information security management for inter-sector and interorganisational communications | This International Standard provides guidelines in addition to guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-sector communications. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed |  | IS |  |  |  |  | 287. |
| ISO/IEC 27013<br>Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 | This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations which are intending to either: a. Implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa; b. Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or c. Align existing ISO/IEC 27001 and ISO/IEC 20000-1 management | ISO/IEC JTC 1/SC 27 | Published<br>1st ed<br>under revision |  | IS |  |  |  |  | 288. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | system (MS) implementations. | | | | | | | | | |
| ISO/IEC 27017<br>Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002 | The scope of this Technical Specification/ International Standard is to define guidelines supporting the implementation of Information<br>Security Management for the use of cloud service. The adoption of this Technical Specification/ International Standard allows cloud consumers and providers to meet baseline information security<br>management with the selection of appropriate controls and implementation guidance based on risk assessment for the use of cloud service. | ISO/IEC JTC 1/SC 27 | CD | Publication by 2015-10 | IS | | | | | 289. |
| ISO/IEC 27031<br>Guidelines for ICT readiness for business continuity | This International Standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 290. |
| ISO/IEC 27032<br>Guidelines for cybersecurity | This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 291. |
| ISO/IEC 27033-1<br>Network Security – Part 1: Overview and concepts | This International Standard provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices,applications/services and end-users, in addition to security of the information being transferred across the communication links.) Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 292. |
| ISO/IEC 27033-2<br>Network Security – Part 2: Guidelines for the design and implementation of network security | This International Standards provides guidelines for organizations to plan, design, implement and document network security. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 293. |
| ISO/IEC 27033-3<br>Network Security – Part 3: Reference networking scenarios – Risks, design techniques and control issues | This International Standard describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks.The information in this International Standard is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 294. |
| ISO/IEC 27033-4<br>Network security -- Part 4: Securing communications between networks using security gateways | This part of ISO/IEC 27033 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with<br>a documented information security policy of the security gateways, including:<br>a) identifying and analysing network security threats associated with security gateways;<br>b) defining network security requirements for security gateways based on threat analysis;<br>c) using techniques for design and implementation to address the threats and control aspects<br>associated with typical network scenarios; and<br>d) addressing issues associated with implementing, operating, monitoring and reviewing network security gateway controls. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 295. |
| ISO/IEC 27033-5<br>Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs) | This part of ISO/IEC 27033 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 296. |
| ISO/IEC 27034-1<br>Application security – Part 1: Overview and concepts | ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications. This International Standard presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 297. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 27035<br>Information security incident management | This International Standard provides a structured and planned approach to detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed.<br>Under revision | | IS | | | | | 298. |
| ISO/IEC 27036-1<br>Information security for supplier relationships -- Part 1: Overview and concepts | This part of ISO/IEC 27036 is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. This part of ISO/IEC 27036 addresses perspectives of both acquirers and suppliers. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 299. |
| ISO/IEC 27036-2 | This part of ISO/IEC 27036 specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.<br>These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, Build-Operate-Transfer and cloud computing services.<br>These requirements are intended to be applicable to all organisations, regardless of type, size and nature.<br>To meet these requirements, an organisation should have already internally implemented a number of foundational processes, or be actively planning to do so. These processes include, but are not limited to, the following: governance, business management, risk management, operational and human resources management, and information security. | ISO/IEC JTC 1/SC 27 | FDIS | Publication by 2014-06 | IS | | | | | 300. |
| ISO/IEC 27036-3<br>Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security | This part of ISO/IEC 27036 provides product and service acquirers and suppliers in ICT supply chain with guidance on:<br>a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains;<br>b) responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services.<br>These risks can be related to organizational as well as technical aspects (e.g. insertion of malicious code or presence of the counterfeit information technology (IT) products);<br>c) integrating information security processes and practices into the system and software lifecycle processes, described in ISO/IEC 15288 and ISO/IEC 12207, while supporting information security controls, described in ISO/IEC 27002.<br>This part of ISO/IEC 27036 does not include business continuity management/resiliency issues involved with the ICT supply chain. ISO/IEC 27031 addresses business continuity. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 301. |
| ISO/IEC 27037<br>Guidelines for the identification, collection, acquisition and preservation of digital evidence | ISO/IEC 27037 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 302. |
| ISO/IEC 27038:<br>Specification for digital redaction | This international standard specifies characteristics of techniques for performing digital redaction on digital documents. This international standard also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed.<br>This international standard does not include the redaction of information from databases. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 303. |
| ISO/IEC 27039<br>Selection, deployment and operation of intrusion detection and prevention systems (IDPS) | This International Standard provides guidelines to assist organizations in preparing to deploy Intrusion Detection Prevention System (IDPS). In particular, it addresses the selection, deployment and operations of IDPS. It also provides background information from which these guidelines are derived. | ISO/IEC JTC 1/SC 27 | FDIS<br>(revision of ISO/IEC 18043) | Publication by 2014-06 | IS | | | | | 304. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 27040<br>Storage security | This International Standard provides detailed technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.<br><br>Storage security is relevant to anyone involved in owning, operating or using data storage devices, media and networks. This includes senior managers, acquirers of storage product and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or storage security, storage operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of storage network security.<br>This standard provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other international standards and technical reports that address existing practices and techniques that can be applied to storage security. | ISO/IEC JTC 1/SC 27 | DIS | Publication by 2014-10 | IS |  |  |  |  | 305. |
| ISO/IEC 27041<br><br>Guidance on assuring suitability and adequacy of incident investigation methods | This International Standard provides guidance on mechanisms for ensuring that methods and processes used in the investigation of Information Security Incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process.<br>This document aims to<br> provide guidance on the capture and analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation;<br> give guidance on the use of validation as a means of assuring suitability of processes involved in the investigation;<br> provide guidance on assessing the levels of validation required and the evidence required from a validation exercise; and<br> give guidance on how external testing and documentation can be incorporated in the validation process. | ISO/IEC JTC 1/SC 27 | DIS | Publication by 2014-10 | IS |  |  |  |  | 306. |
| ISO/IEC 27042<br><br>Guidelines for analysis and interpretation of digital evidence | This International Standard provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility and repeatability. It encapsulates best practice for selection, design and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.<br>Analysis and interpretation of digital evidence can be a complex process. In some circumstances there may be several methods which could be applied and members of the investigative team will be required to justify 10 their selection of a particular process and show how it is equivalent to another process used by other investigators. In other circumstances, investigators may have to devise new methods for examining digital evidence which has not been previously been considered and should be able to show that the method produced is "fit for purpose".<br>Application of a particular method may influence the interpretation of digital evidence processed by that method. The available digital evidence may influence the selection of methods for further analysis of digital evidence which has already been acquired.<br>This International Standard provides a common framework, for the analytical and interpretational elements of information | ISO/IEC JTC 1/SC 27 | DIS | Publication by 2014-10 | IS |  |  |  |  | 307. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | systems security incident handling, which can be used to assist in the implementation of new methods and provide a minimum common standard for digital evidence produced from such activities.<br>20 | | | | | | | | | |
| ISO/IEC 27043<br>Incident investigation principles and processes | This International Standard provides guidelines that encapsulate idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation up to and including returning evidence for storage or dissemination as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes or corporate breaches of information security as well as any other digital investigation.<br>In summary, this International Standard provides a general overview of all incident investigation principles and processes without prescribing particular details within each of the investigation principles and processes covered in this International Standard. Many other relevant International Standards, where referenced in this International Standard, provide more detailed content of specific investigation principles and processes. | ISO/IEC JTC 1/SC 27 | DIS | Publication by 2014-10 | IS | | | | | 308. |
| ISO/IEC 27044<br>Guidelines for Security Information and Event Management (SIEM) | This International Standard provides guidelines to assist organizations in preparing to deploy Security Information and Event Management Systems (SIEM) and related process. In particular, it addresses the selection, deployment and operations of SIEM.<br>This International Standard is intended to be helpful to:<br>a) An organization in satisfying the following requirements of ISO/IEC 27001:2013:<br>The organization shall implement procedures and other controls capable of enabling prompt detection of and response to security incidents;<br>The organization shall execute monitoring and review procedures and other controls to properly identify attempted and successful security breaches and incidents;<br>b) An organization in implementing controls that meet the following security objectives of ISO/IEC 27002:2013:<br>To detect unauthorized information processing activities;<br>Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified;<br>An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities;<br>System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model;<br>An organization should recognize that deploying SIEM is not a sole and/or exhaustive solution to satisfy or meet the above-cited requirements. Furthermore, this International Standard is not intended as criteria for any kind of conformity assessments, e.g., Information Security Management System (ISMS) certification, IDPS services or products certification | ISO/IEC JTC 1/SC 27 | WD | Publication by 2016-10 | IS | | | | | 309. |
| ISO/IEC 27050<br>Electronic discovery<br>Part 1: Overview and concepts<br>Part 2: Guidance for governance and management of electronic discovery<br>Part 3: Code of Practice for electronic discovery<br>Part 4: ICT readiness for electronic discovery | Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or both parties involved in an investigation and any resulting actions. This International Standard provides an overview of electronic discovery. In addition, it defines related definitions and describes the concepts, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of ESI. This International Standard also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities. This International Standard is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities, and It is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements. | ISO/IEC JTC 1/SC 27 | WD | Publication by 2016-10 (P. 1)<br>2017-10 (P. 2-4) | IS | | | | | 310. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 29003 - Security techniques -- Identity proofing | This International Standard (IS) provides best practices and guidance on required processes for the initial establishment and subsequent confirmation of an entity's identity for parties using, or expecting to use, ISO/IEC 29115 or other similar standards. The material is used to establish and/or confirm identity and thus should give greater confidence in an entity's identity prior to the issuance of identity credentials or delivery of a service to that entity, by or for that entity.<br>In scope:<br>• The development of identity proofing and verification (IPV) processes to be used as a national body standard in support of the enrolment of entities. Definitions and controls are provided for IPV principles and risk assessments that are sufficient to meet the requirements of ISO identity management standards for entities, notably ISO/IEC 29115. These controls take account of threats, counter-fraud requirements and best practice guidance described by national policy specifications from government organisations.<br>• Entities that require identity proofing and verification in accordance with this and associated ISO standards are:<br>• Persons.<br>• Devices or Security Modules, particularly (but not limited to) for computer and telecommunication use cases, including e.g. Trusted Platform Module (TPM), Mobile Trusted Module (MTM) and similar approved standards. This includes products with parts or identifiable components whose integrity and authenticity is being asserted.<br>• Software. Services, which may include network and application protocols such as SSL/TLS and VPN, which employ trust-based models using certificates, etc. Software, which may include firmware, operating system code, application code or executable scripts.<br>• Organisations, non-person entities that exist to carry out business in all kinds of organisations, including government, industry and voluntary.<br><br>NB: For the purposes of trust, all persons, devices and software have a relationship with one or more organisations for reasons of employment, ownership, issuance and management.<br>• A resulting International Standard that is sufficient for: • Nations and industry to have confidence in using identities proven according to requirements of that standard<br>• Nations and industry to have confidence in the results of each others' national IPV systems and the credentials<br>• Certification bodies to develop assessment and audit criteria against which certified auditors can successfully conduct audit and assurance of IPV service providers.<br>• Establishing a foundation for mutual recognition of identity proofing arrangements between nations and industries.<br><br>Out of Scope:<br>• Vetting is outside the scope of this International Standard (See clause 3.2.29) | ISO/IEC JTC 1/SC 27 | Publication by 2016-05 | | IS | | | | | 311. |
| ISO/IEC 29100<br>Privacy framework | ISO/IEC 29100 provides a privacy framework which<br>• specifies a common privacy terminology;<br>• defines the actors and their roles in processing personally identifiable information (PII);<br>• describes privacy safeguarding considerations; and<br>• provides references to known privacy principles for information technology.<br>ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 312. |
| ISO/IEC 29101<br>Information technology — Security techniques — Privacy architecture framework | This International Standard defines a privacy architecture framework that:<br>— specifies concerns for ICT systems that process PII;<br>— lists components for the implementation of such systems; and<br>— provides architectural views contextualizing these components. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 313. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | This International Standard is applicable to entities involved in specifying, procuring, architecting, designing,<br>testing, maintaining, administering and operating ICT systems that process PII.<br>It focuses primarily on ICT systems that are designed to interact with PII principals. | | | | | | | | | |
| ISO/IEC 29128<br>Verification of cryptographic protocols | ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 314. |
| ISO/IEC 29146 - Security techniques - A framework for access management | This International Standard defines and establishes a framework for Access Management (AM) and the secure management of the process to access information and ICT information resources, associated with the accountability of a subject within some context.<br>This International Standard provides concepts, terms and definitions applicable to distributed access management techniques in network environments.<br>This International Standard also provides explanations about related architecture, components and management functions.<br>The subjects involved in access management might be uniquely recognized to access information systems, as defined in ISO/IEC 24760," A framework for identity management".<br>The nature and qualities of physical access control involved in access management systems are outside the scope of this document. | ISO/IEC JTC 1/SC 27 | Publication by 2015-05 | | IS | | | | | 315. |
| ISO/IEC 29147<br>Vulnerability disclosure | This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 316. |
| ISO/IEC 29150<br>**Signcryption** | ISO/IEC 29150 specifies mechanisms for signcryption that employ public key cryptographic techniques requiring both the originator and the recipient of protected data to their own public and private key pairs | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | IS | | | | | | 317. |
| ISO/IEC 29151 - Privacy impact assessment | This International Standard establishes commonly accepted control objectives, controls and guidelines for implementing controls, which are usable for the treatment of risks that have been generated on PII principals and previously assessed, for example, by a PIA when processing of PII by an organization.<br>In particular, this International Standard specifies guidelines based on ISO/IEC 27002 in accordance with the privacy principles in ISO/IEC 29100, taking into consideration the regulatory requirements for processing PII which may be applicable within the context of an organization's information security risk environment(s) as well as privacy controls.<br>This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, such as PII controllers that collect personally identifiable information and determine the purposes for which it is processed, and PII processors that process personally identifiable information on behalf of the PII controller. | ISO/IEC JTC 1/SC 27 | Publication by 2016-05 | | IS | | | | | 318. |
| ISO/IEC 29192<br>**Lightweight cryptography**<br>Part 1: General<br>Part 2: Block ciphers<br>Part 3: Stream ciphers<br>Part 4: Mechanisms using asymmetric techniques<br>Part 5:Hash-functions | ISO/IEC 29192 specifies symmetric ciphers (block ciphers and stream ciphers) and mechanisms using asymmetric techniques (authentication, key exchange and identity based signature) which are suitable for lightweight cryptographic applications | ISO/IEC JTC 1/SC 27 | Published<br>1st ed.<br>WD (Part 5) | IS | | | | | | 319. |
| ISO/IEC 30111<br>Vulnerability handling processes | This International Standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 320. |
| ISO/IEC 7064<br>**Check character systems** | ISO/IEC 7064 specifies a set of check character systems capable of protecting strings against errors. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | IS | | | | | | 321. |
| ISO/IEC 9796<br>**Digital signature schemes giving message recovery**<br>Part 2: Integer factorization based mechanisms<br>Part 3: Discrete logarithm based mechanisms | ISO/IEC 9796-2 specifies digital signature mechanisms giving partial<br>or total message recovery aiming at reducing storage and transmission<br>overhead. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed. (P. 2)<br>2nd ed. (P. 3) | IS | | | | | | 322. |
| ISO/IEC 9797<br>**Message authentication codes (MACs)**<br>Part 1: Mechanisms using a block | ISO/IEC 9797 specifies message authentication code (MAC) algorithms, which are data integrity mechanisms that compute a short string. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. (P. 1)<br>2nd ed. (P. 2)<br>1st (P. 3) | IS | | | | | | 323. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| cipher<br>Part 2: Mechanisms using a dedicated hash-function<br>Part 3: Mechanisms using a universal hash-function | | | | | | | | | | |
| ISO/IEC 9798<br>**Entity authentication**<br>Part 1: General<br>Part 2: Mechanisms using symmetric encipherment algorithms<br>Part 3: Mechanisms using digital signature techniques (+Amd1)<br>Part 4: Mechanisms using cryptographic check function<br>Part 5: Mechanisms using zero knowledge techniques<br>Part 6: Mechanisms using manual data transfer | ISO/IEC 9798 specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret. | ISO/IEC JTC 1/SC 27 | Published<br>3rd ed.(P. 1)<br>3rd ed.(P. 2)<br>2nd ed.(P. 3)<br>2nd ed.(P. 4)<br>3rd ed.(P. 5)<br>2nd ed.(P. 6) | IS | | | | | | 324. |
| ISO/IEC TR 15443<br>A framework for IT security assurance | ISO/IEC TR 15443 guides the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed. | | IS | | | | | 325. |
| ISO/IEC TR 15446<br>Guide for the production of Protection Profiles and Security Targets | ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed | | TR | | | | | 326. |
| ISO/IEC TR 19249<br>Catalogue of architectural and design principles for secure products, systems, and applications | This Technical Report provides a catalogue of architectural and design principles that can be used in the development of secure products, systems, and applications together with guidance on how to use those principles effectively. Each architectural and design principle is described using a common structure, identifying the purpose and advantage of the design principle, how it can contribute to develop a secure product, system, or application, its dependency on other principles described in the catalogue.<br>Examples are provided for each principle on how it may be implemented, how it may contribute to security properties and functions and what other aspects have to be taken into account in the example provided to also address non-security related requirements like usability and performance. | ISO/IEC JTC 1/SC 27 | WD | Publication by 2016-10 | TR | | | | | 327. |
| ISO/IEC TR 19791<br>Security assessment of operational systems | ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems. | ISO/IEC JTC 1/SC 27 | Published<br>2nd ed.<br>(under revision) | | TR | | | | | 328. |
| ISO/IEC TR 20004<br>Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 | ISO/IEC TR 20004:2012 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed<br>(under revision) | | TR | | | | | 329. |
| ISO/IEC TR 27008<br>Guidelines for auditors on ISMS controls | This Technical Report provides guidance for assessing the implementation of ISMS controls selected through a risk-based approach for information security management. It supports the information security risk management process and assessment of ISMS controls by explaining the relationship between the ISMS and its supporting controls. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed | | TR | | | | | 330. |
| ISO/IEC TR 27015<br>Guidelines for information security management system for financial services | This International Standard provides requirements, guidelines and general principles for initiating, implementing, maintaining, and improving the information security management within finance and insurance sectors based upon ISO/IEC 27001 and ISO/IEC 27002. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | TR | | | | | 331. |
| ISO/IEC TR 27016<br>Information security management – organisational economics | This technical report provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. This Technical Report is applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by managers who have responsibility for information security decisions. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | TR | | | | | 332. |
| ISO/IEC TR 29149<br>Best practice on the provision and use of time-stamping services | This Technical Report explains how to provide and use times-tamping services so that time-stamp tokens are effective when used to provide timeliness and data integrity services, or nonrepudiation services (in conjunction with other mechanisms). It covers time-stamp services, explaining how to generate, renew, and verify time-stamp tokens. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | TR | | | | | 333. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC TS 30104<br>Physical security attacks, mitigation techniques and security requirements | This Technical Specification addresses how security assurance can be stated for products where the risk of the security environment requires the support of physical protection mechanisms. | ISO/IEC JTC 1/SC 27 | PDTS | Publication by 2014-10 | TS | | | | | 334. |
| ITU-T X.1051 \| ISO/IEC 27011<br>Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 | This Recommendation \| International Standard:<br>a) establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications organizations based on ISO/IEC 27002;<br>b) provides an implementation baseline of Information Security Management within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities and services. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed | | IS | | | | | 335. |
| ITU-T X.1054 \| ISO/IEC 27014<br>Governance of information security | This International Standard provides guidance on the development and use of governance of information security (GIS) through which organisations direct and control the information security management system (ISMS) process as specified in ISO/IEC 27001. This International Standard provides guiding principles and processes for top management of organisations on the effective, efficient, and acceptable use of information security within their organisations. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 336. |
| ITU-T X.831 I ISO/IEC 15816<br>Security information objects for access control | This International Standard provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1). | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | IS | | | | | 337. |
| ITU-T X.842 I ISO/IEC TR 14516<br>Guidelines for the use and management of Trusted Third Party services | This Technical Report provides guidance for the use and management of Trusted Third Party (TTP) services, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. This Technical Report identifies different major categories of TTP services including time stamping, non-repudiation, key management, certificate management, and electronic notary public. | ISO/IEC JTC 1/SC 27 | Published<br>1st ed. | | TR | | | | | 338. |
| ISO/IEC 19762, Information technology -- Automatic identification and data capture techniques -- Harmonized vocabulary | | ISO/IEC JTC 1/SC 31 | 10.60 | | | | | | | 339. |
| ISO/IEC 19762-1, Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 1: General terms relating to AIDC | ISO/IEC 19762-1:2008 provides general terms and definitions in the area of automatic identification and data capture techniques on which are based further specialized sections in various technical fields, as well as the essential terms to be used by non-specialist users in communication with specialists in automatic identification and data capture techniques. | ISO/IEC JTC 1/SC 31 | International Standard<br>NP for a single part document & translation to French, German, and Russian | 2008-06-11 | | AIDC | | | | 340. |
| ISO/IEC 19762-2, Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 2: Optically readable media (ORM) | ISO/IEC 19762-2:2008 provides terms and definitions unique to optically readable media (ORM) in the area of automatic identification and data capture techniques. This glossary of terms enables the communication between non-specialist users and specialists in ORM through a common understanding of basic and advanced concepts. | ISO/IEC JTC 1/SC 31 | International Standard<br>NP for a single part document & translation to French, German, and Russian | 2008-06-11 | | AIDC | | | | 341. |
| ISO/IEC 19762-3, Information technology -- Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 3: Radio frequency identification (RFID) | ISO/IEC 19762-3:2008 provides terms and definitions unique to radio frequency identification (RFID) in the area of automatic identification and data capture techniques. This glossary of terms enables the communication between non-specialist users and specialists in RFID through a common understanding of basic and advanced concepts. | ISO/IEC JTC 1/SC 31 | International Standard<br>NP for a single part document & translation to French, German, and Russian | 2008-06-11 | | AIDC | | | | 342. |
| ISO/IEC 19762-4, Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 4: | ISO/IEC 19762-4:2008 provides general terms and definitions relating to radio communications in the area of automatic identification and data capture techniques. This glossary of terms enables the communication between non-specialist users and | ISO/IEC JTC 1/SC 31 | International Standard<br>NP for a single part document & | 2008-06-11 | | AIDC | | | | 343. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| General terms relating to radio communications | specialists in radio communications through a common understanding of basic and advanced concepts. | | translation to French, German, and Russian | | | | | | | |
| ISO/IEC 19762-5, Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary – Part 5: Locating systems | ISO/IEC 19762-5:2008 provides terms and definitions unique to locating systems in the area of automatic identification and data capture techniques. This glossary of terms enables the communication between non-specialist users and specialists in locating systems through a common understanding of basic and advanced concepts. | ISO/IEC JTC 1/SC 31 | International Standard<br>NP for a single part document & translation to French, German, and Russian | 2008-06-11 | | AIDC | | | | 344. |
| ISO/IEC 15415:2011, Information technology -- Automatic identification and data capture techniques -- Bar code symbol print quality test specification -- Two-dimensional symbols | | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 | | | | | | | 345. |
| ISO/IEC 15416:2000, Information technology -- Automatic identification and data capture techniques -- Bar code print quality test specification -- Linear symbols | | ISO/IEC JTC 1/SC 31/WG 1 | 90.93 | | | | | | | 346. |
| ISO/IEC 15420:2009, Information technology -- Automatic identification and data capture techniques -- EAN/UPC bar code symbology specification | | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 | | | | | | | 347. |
| ISO/IEC 15420:2009/NP Cor 1, Information technology -- Automatic identification and data capture techniques -- EAN/UPC bar code symbology specification -- Technical Corrigendum 1 | | ISO/IEC JTC 1/SC 31/WG 1 | 10.60 | | | | | | | 348. |
| ISO/IEC 15424:2008, Information technology -- Automatic identification and data capture techniques -- Data Carrier Identifiers (including Symbology Identifiers) | | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 | | | | | | | 349. |
| ISO/IEC 16022:2006, Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification | | ISO/IEC JTC 1/SC 31/WG 1 | 90.93 | | | | | | | 350. |
| ISO/IEC 16022:2006/Cor 1:2008, Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification -- Technical Corrigendum 1 | | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 | | | | | | | 351. |
| ISO/IEC 16022:2006/Cor 2:2011, Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification -- Technical Corrigendum 2 | | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 | | | | | | | 352. |
| ISO/IEC 16480, Information technology -- Automatic identification and data capture | | ISO/IEC JTC 1/SC 31/WG 1 | 30.20<br>(Start date: 2012- | | | | | | | 353. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| techniques -- Reading and display of ORM by mobile devices |  |  | 07-13<br>End date: 2012-10-14) |  |  |  |  |  |  |  |
| ISO/IEC 18004, Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification |  | ISO/IEC JTC 1/SC 31/WG 1 | 10.60 |  |  |  |  |  |  | 354. |
| ISO/IEC 18004:2006, Information technology -- Automatic identification and data capture techniques -- QR Code 2005 bar code symbology specification |  | ISO/IEC JTC 1/SC 31/WG 1 | 90.60 |  |  |  |  |  |  | 355. |
| ISO/IEC 18004:2006/Cor 1:2009, Information technology -- Automatic identification and data capture techniques -- QR Code 2005 bar code symbology specification -- Technical Corrigendum 1 |  | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 |  |  |  |  |  |  | 356. |
| ISO/IEC 24778:2008, Information technology -- Automatic identification and data capture techniques -- Aztec Code bar code symbology specification |  | ISO/IEC JTC 1/SC 31/WG 1 | 60.60 |  |  |  |  |  |  | 357. |
| ISO/IEC 15418:2009, Information technology -- Automatic identification and data capture techniques -- GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance |  | ISO/IEC JTC 1/SC 31/WG 2 | 60.60 |  |  |  |  |  |  | 358. |
| ISO/IEC 15434:2006, Information technology -- Automatic identification and data capture techniques -- Syntax for high-capacity ADC media |  | ISO/IEC JTC 1/SC 31/WG 2 | 90.60 |  |  |  |  |  |  | 359. |
| ISO/IEC 15459-1, Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units | This standard provides unique identification at the transport unit level.<br>This standard serves as the basis for identification in ISO 15394 (for bar codes) and ISO 17365 (for RFID) | ISO/IEC JTC 1/SC 31/WG 2 | FDIS |  |  | AIDC |  |  |  | 360. |
| ISO/IEC 15459-2, Information technology – Automatic identification and data capture techniques – Unique identification – Part 2: Registration procedures | Unique identification can occur at many different levels in the supply chain, at the transport unit, at the item level, and elsewhere. Such distinct entities are often handled by several parties: the sender, the receiver, one or more carriers, customs authorities, etc. Each of these parties must be able to identify and trace the item so that reference can be made to associated information such as address, order number, contents of the item, weight, sender, batch or lot number, etc. There are considerable benefits if the identity of the item is common between all the relevant parties.<br>ISO/IEC 15459-2:2006 specifies the procedural requirements to maintain a non-significant, unique identifier for item management applications, and outlines the obligations of the Registration Authority and Issuing Agencies.<br>ISO/IEC 15459-2:2006 excludes those items where ISO has designated Maintenance Agencies or Registration Authorities to | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-06-29 |  | AIDC |  |  |  | 361. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | provide identification schemes. It does not apply to<br>- freight containers, because their unique coding is specified in ISO 6346, Freight containers -- Coding, identification and marking;<br>- vehicles, because their unique identification is specified in ISO 3779, Road vehicles -- Vehicle identification number (VIN) -- Content and structure;<br>- car radios, because their unique identification is specified in ISO 10486, Passenger cars -- Car radio identification number (CRIN).<br>The exclusion also applies to ISO 2108, Information and documentation -- International standard book number (ISBN) and ISO 3297, Information and documentation -- International standard serial number (ISSN). | | | | | | | | | |
| ISO/IEC 15459-3, Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules for unique | Unique identification can occur at many different levels in the supply chain, at the transport unit, at the item level, and elsewhere. Such distinct entities are often handled by several parties - the sender, the receiver, one or more carriers, customs authorities, etc. Each of these parties must be able to identify and trace the item so that reference can be made to associated information such as configuration, maintenance history, address, order number, contents of the item, weight, sender, batch or lot number, etc.<br>The information is often held on computer systems, and may be exchanged between parties involved via EDI (Electronic Data Interchange) and XML (eXtensible Markup Language) messages.<br>There are considerable benefits if the identity of the item is represented in bar code format, or other AIDC (Automatic Identification and Data Capture) media and attached to or made a constituent part of that which is being uniquely identified so that<br>- it can be read electronically, thus minimising errors;<br>- one identity can be used by all parties;<br>- each party can use the identity to look up its computer files to find the data associated with the item;<br>- the identifier is unique within the class and cannot appear on any other item of the class during the lifetime of the item.<br>ISO/IEC 15459-3:2006 specifies the common rules that apply for unique identifiers for item management that are required to ensure full compatibility across classes of unique identifiers. | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-06-29 | | AIDC | | | | 362. |
| ISO/IEC 15459-4, Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual items | Unique identification can occur at many different levels in the supply chain, at the transport unit, at the item level, and elsewhere. Such distinct entities are often handled by several parties: the sender, the receiver, one or more carriers, customs authorities, etc. Each of these parties must be able to identify and trace the item so that reference can be made to associated information such as configuration, maintenance history, address, order number, contents of the item, weight, sender, batch or lot number, etc.<br>The information is often held on computer systems, and may be exchanged between parties involved via EDI (Electronic Data Interchange) and XML (eXtensible Markup Language) messages.<br>There are considerable benefits if the identity of the item is represented in bar code format, or other AIDC (Automatic Identification and Data Capture) media and attached to or made a constituent part of that which is being uniquely identified so that<br>- it can be read electronically, thus minimising errors;<br>- one identity can be used by all parties;<br>- each party can use the identity to look up its computer files | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-06-29 | | AIDC | | | | 363. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | to find the data associated with the item;<br>- the identifier is unique within the class and cannot appear on any other item of the class during the lifetime of the item.<br>The unique identifier for individual items defined in ISO/IEC 15459-4:2008 and represented in a bar code label, two-dimensional symbol, radio-frequency identification tag, or other AIDC media attached to the item meets these needs.<br>All AIDC technologies have the potential to encode a unique identifier. It is expected that application standards for items, using various automatic identification technologies, will be developed based upon the unique identifier as a prime key. These application standards may be made available from the Issuing Agency.<br>ISO/IEC 15459-4:2008 specifies a unique, non-significant string of characters for the unique identifier for individual items. The character string is intended to be represented in a bar code label or other AIDC media attached to the item to meet supply chain needs. To address management needs, different classes of items are recognized in the various parts of ISO/IEC 15459, which allows different requirements to be met by the unique identifiers associated with each class. The rules are defined for the individual items to identify the unique occurrence of an item, understood to mean the layers zero and one as will be defined in two future International Standards (ISO 17367 and ISO 17366, respectively). |  |  |  |  |  |  |  |  |  |
| ISO/IEC 15459-5, Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Unique identifier for returnable transport items (RTIs) | ISO/IEC 15459-5:2007 specifies a unique, non-significant string of characters for the unique identification of returnable transport items (RTIs). The character string is intended to be represented in a radio frequency identification (RFID) transponder, bar code label or other automatic identification and data capture (AIDC) media attached to the item to meet supply chain management needs. To address management needs different classes of RTI are recognised in the various parts of ISO/IEC 15459, which allows different requirements to be met by the unique identifiers associated with each class. The rules for the unique identifier for RTIs, to identify the unique occurrence of an item, with the identity being relevant for the complete life cycle of the item, are defined and supported by an example. | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-06-29 |  | AIDC |  |  |  | 364. |
| ISO/IEC 15459-6, Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units | ISO/IEC 15459-6:2007 specifies a unique, non-significant string of characters for the unique identifier of product groupings. The character string is intended to be represented in linear bar code and two-dimensional symbols, radio frequency identification (RFID) transponder or other automatic identification and data capture (AIDC) media attached to the product and/or material to meet the management needs in a batch or lot unit. To address management needs, different classes of item are recognised in the various parts of ISO/IEC 15459. This allows different requirements to be met by the unique identifiers of each class.<br>The unique identifier for product grouping enables a product grouping defined by a batch or lot number to be uniquely identified from all other lots and batches compliant with ISO/IEC 15459-6:2007. Encoding this unique identifier in a data carrier enables information about the quality of product and end-of-life processing to be clearly identified.<br>The rules for the unique identifier for product grouping, to identify the unique occurrence of that quality, are defined and supported by an example. | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-06-29 |  | AIDC |  |  |  | 365. |
| ISO/IEC 15459-8, Information technology – Automatic identification | ISO/IEC 15459-8:2009 specifies a unique, non-significant, string of characters for the unique identifier for grouping of transport | ISO/IEC JTC 1/SC 31/WG 2 | International Standard | 2009-08-31 |  | AIDC |  |  |  | 366. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| and data capture techniques – Unique identification – Part 8: Grouping of transport units | units. The character string might be represented in a bar code label or other AIDC media associated with the items that make up the grouping to meet supply chain needs and regulatory needs (e.g. customs clearance). An individual instance of an entity is aptly identified by a unique identifier defined in other parts of ISO/IEC 15459. This relationship has to be communicated to the business partners according to the business need and the unique identifier for the grouping might be used as a reference number only or marked in addition to the existing identifier. To address management needs, different classes of items are recognized in the various parts of ISO/IEC 15459, which allows different requirements to be met by the unique identifiers associated with each class. ISO/IEC 15459-8:2009 defines the rules for the grouping of transport units to identify the multiple physical units that make up a single shipment from a consignor and are treated as a single logical grouping for customs and other shipping requirements. | | | | | | | | | |
| ISO/IEC 29161, Automatic identification and data capture techniques – Unique identification | This International Standard establishes a scheme of unique digital identification for products, product packages, transport units, assets, and other items. This International Standard specifies the common rules applicable for unique digital identification that are required to ensure full compatibility across different identities. The unique digital identification is a universal binary identifier for any physical object. It is used in information systems that need to track or otherwise refer to physical objects. It is intended for use within any AIDC media capable of encoding binary structures. | ISO/IEC JTC 1/SC 31/WG 2 | WD | | | AIDC | | | | 367. |
| ISO/IEC TR 29162:2012, Information technology -- Guidelines for using data structures in AIDC media | | ISO/IEC JTC 1/SC 31/WG 2 | 60.60 | | | | | | | 368. |
| ISO/IEC 15961-1, Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 1: Application interface | | ISO/IEC JTC 1/SC 31/WG 4 | 50.60 | | | | | | | 369. |
| ISO/IEC 15961-2, Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 2: Registration of RFID data constructs | | ISO/IEC JTC 1/SC 31/WG 4 | 60.00 | | | | | | | 370. |
| ISO/IEC 15961-3, Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 3: RFID data constructs | | ISO/IEC JTC 1/SC 31/WG 4 | 60.00 | | | | | | | 371. |
| ISO/IEC 15961-4, Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 4: Application interface commands for battery assist and sensor functionality | | ISO/IEC JTC 1/SC 31/WG 4 | 30.60 | | | | | | | 372. |
| ISO/IEC 15962, Information technology -- Radio frequency identification (RFID) for item management -- Data protocol: data encoding rules and logical memory functions | | ISO/IEC JTC 1/SC 31/WG 4 | 50.60 | | | | | | | 373. |
| ISO/IEC 15963, Information technology – Radio frequency | ISO/IEC 15963:2009 describes numbering systems that are available for the identification of RF tags. | ISO/IEC JTC 1/SC 31/WG 4 | International Standard | 2009-08-31 | | RFID | | | | 374. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| identification for item management – Unique identification for RF tags | The unique ID can be used<br>- for the traceability of the integrated circuit itself for quality control in its manufacturing process,<br>- for the traceability of the RF tag during its manufacturing process and along its lifetime,<br>- for the completion of the reading in a multi-antenna configuration,<br>- by the anti-collision mechanism to inventory multiple tags in the reader's field of view, and<br>- for the traceability of the Item to which the RF tag is attached. | | | | | | | | | |
| ISO/IEC 18000-3, Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz | ISO/IEC 18000 has been developed in order to:<br>- provide a framework to define common communications protocols for Internationally useable frequencies for radio frequency identification (RFID), and, where possible, to determine the use of the same protocols for all frequencies such that the problems of migrating from one to another are diminished;<br>- minimize software and implementation costs;<br>- enable system management and control and information exchange to be common as far as is possible.<br>ISO/IEC 18000-1 provides explanation of the concepts behind ISO/IEC 18000-3:2010.<br>ISO/IEC 18000-3:2010 has 3 MODES of operation, intended to address different applications. The detailed technical differences between the modes are shown in parameter tables.<br>ISO/IEC 18000-3:2010 provides physical layer, collision management system and protocol values for RFID systems for item identification operating at 13,56 MHz in accordance with the requirements of ISO/IEC 18000-1.<br>It provides definitions for systems for each MODE determined in ISO/IEC 18000-3:2010.<br>It defines three non-interfering MODES.<br>- The MODES are not interoperable.<br>- The MODES, whilst not interoperable, are non-interfering. | ISO/IEC JTC 1/SC 31/WG 4 | International Standard | 2010-11-04 | | RFID | | | | 375. |
| ISO/IEC 18000-4, Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz Mode 3 | This part of ISO/IEC 18000 defines the air interface for radio frequency identification (RFID) devices operating in the 2,45 GHz Industrial, Scientific, and Medical (ISM) band used in item management applications. This part of ISO/IEC 18000 provides a common technical specification for RFID devices that can be used by ISO committees developing RFID application standards. This part of ISO/IEC 18000 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. This part of ISO/IEC 18000 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum equivalent isotropically radiated power (EIRP), spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and where appropriate operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. This part of ISO/IEC 18000 further defines the communications protocol used in the air interface.<br>This part of ISO/IEC 18000 contains three modes. Mode 1 is an interrogator talks first with passive tag. Mode 2 is a tag talks first with battery-assisted passive tag. Mode 3 is a globally available, ubiquitous network supporting (but not limited to) the logistics and transportation industry; agnostic to any device, commercial or otherwise, requiring global availability. The detailed technical | ISO/IEC JTC 1/SC 31/WG 4 | | | | | | | | 376. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | differences between the modes are shown in the parameter tables. | | | | | | | | | |
| ISO/IEC 18000-4, Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz Mode 4 | This part defines the physical layer of band 2.45GHz air interface for radio frequency identification (RFID), as well as data link layer, tag memory structure, tag state transition, interrogator commands and tag responses, protocol operation mode, anti-collision method and so on.<br>This part applies to designing, producing, testing and using of 2.45GHz RFID active tags and interrogators. | ISO/IEC JTC 1/SC 31/WG 4 | | | | | | | | 377. |
| ISO/IEC 18000-4:2008, Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz | This part of ISO/IEC 18000 defines the air interface for radio frequency identification (RFID) devices operating in the 2,45 GHz Industrial, Scientific, and Medical (ISM) band used in item management applications. This part of ISO/IEC 18000 provides a common technical specification for RFID devices that can be used by ISO committees developing RFID application standards. This part of ISO/IEC 18000 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. This part of ISO/IEC 18000 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum equivalent isotropically radiated power (EIRP), spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and where appropriate operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. This part of ISO/IEC 18000 further defines the communications protocol used in the air interface.<br>This part of ISO/IEC 18000 contains two modes. The first is a passive tag operating as an interrogator talks first and the second is a battery-assisted tag operating as a tag talks first. The detailed technical differences between the modes are shown in the parameter tables. | ISO/IEC JTC 1/SC 31/WG 4 | 90.92 | | | | | | | 378. |
| ISO/IEC 18000-63, Information technology – Radio frequency identification for item management – Part 63: Parameters for air interface communications at 860 MHz to 960 MHz | ISO/IEC 18000-6:2010 defines the air interface for radio frequency identification (RFID) devices operating in the 860 MHz to 960 MHz Industrial, Scientific, and Medical (ISM) band used in item management applications. It provides a common technical specification for RFID devices that can be used by ISO committees developing RFID application standards. ISO/IEC 18000-6:2010 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. It defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum effective isotropic radiated power (EIRP), spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and, where appropriate, operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. It further defines the communications protocol used in the air interface.<br>ISO/IEC 18000-6:2010 specifies the physical and logical requirements for a passive-backscatter, Interrogator-Talks-First (ITF) or tag-talks-only-after-listening (TOTAL) RFID system. The system comprises Interrogators, and tags, also known as labels. An Interrogator receives information from a tag by transmitting a continuous-wave (CW) RF signal to the tag; the tag responds by modulating the reflection coefficient of its antenna, thereby backscattering an information signal to the Interrogator. The system is ITF, meaning that a tag modulates its antenna reflection coefficient with an information signal only after being directed to do so by an Interrogator, or TOTAL, meaning that a tag modulates its antenna reflection coefficient with an information signal upon entering an Interrogator's field after first listening for Interrogator modulation in order to determine if the system is ITF or not.<br>In detail, ISO/IEC 18000-6:2010 contains one mode with four | ISO/IEC JTC 1/SC 31/WG 4 | International Standard | 2013-01-16 | | RFID | | | | 379. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | types. The detailed technical differences between the four types are shown in the associated parameter tables.<br>Types A, B and C are ITF. Type A uses Pulse-Interval Encoding (PIE) in the forward link and an adaptive ALOHA collision-arbitration algorithm. Type B uses Manchester in the forward link and an adaptive binary-tree collision-arbitration algorithm. Type C uses PIE in the forward link and a random slotted collision-arbitration algorithm.<br>Type D is TOTAL based on Pulse Position Encoding or Miller M=2 encoded subcarrier.<br>ISO/IEC 18000-6:2010 specifies<br>- physical interactions (the signalling layer of the communication link) between Interrogators and tags,<br>- Interrogator and tag operating procedures and commands,<br>- the collision arbitration scheme used to identify a specific tag in a multiple-tag environment. |  |  |  |  |  |  |  |  |  |
| ISO/IEC 18000-7, Information technology – Radio frequency identification for item management – Part 7: Parameters for active air interface communications at 433 MHz | ISO/IEC 18000-7:2009 defines the air interface for radio frequency identification (RFID) devices operating as an active RF tag in the 433 MHz band used in item management applications. It provides a common technical specification for RFID devices that can be used by ISO technical committees developing RFID application standards. ISO/IEC 18000-7:2009 is intended to allow for compatibility and to encourage inter-operability of products for the growing RFID market in the international marketplace. ISO/IEC 18000-7:2009 defines the forward and return link parameters for technical attributes including, but not limited to, operating frequency, operating channel accuracy, occupied channel bandwidth, maximum power, spurious emissions, modulation, duty cycle, data coding, bit rate, bit rate accuracy, bit transmission order, and, where appropriate, operating channels, frequency hop rate, hop sequence, spreading sequence, and chip rate. ISO/IEC 18000-7:2009 further defines the communications protocol used in the air interface. | ISO/IEC JTC 1/SC 31/WG 4 | International Standard to be revised |  |  | RFID |  |  |  | 380. |
| ISO/IEC 24753:2011, Information technology -- Radio frequency identification (RFID) for item management -- Application protocol: encoding and processing rules for sensors and batteries |  | ISO/IEC JTC 1/SC 31/WG 4 | 60.60 |  |  |  |  |  |  | 381. |
| ISO/IEC 24791-1:2010, Information technology -- Radio frequency identification (RFID) for item management -- Software system infrastructure -- Part 1: Architecture |  | ISO/IEC JTC 1/SC 31/WG 4 | 60.60 |  |  |  |  |  |  | 382. |
| ISO/IEC 24791-2:2011, Information technology -- Radio frequency identification (RFID) for item management -- Software system infrastructure -- Part 2: Data management |  | ISO/IEC JTC 1/SC 31/WG 4 | 60.60 |  |  |  |  |  |  | 383. |
| ISO/IEC 24791-3, Information technology -- Radio frequency identification (RFID) for item management -- Software system infrastructure -- Part 3: Device management |  | ISO/IEC JTC 1/SC 31/WG 4 | 40.99 |  |  |  |  |  |  | 384. |
| ISO/IEC 24791-5, Information technology -- Radio frequency identification (RFID) for item |  | ISO/IEC JTC 1/SC 31/WG 4 | 50.20<br>(Start date: 2012- |  |  |  |  |  |  | 385. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| management -- Software system infrastructure -- Part 5: Device interface | | | 08-15<br>End date: 2012-10-16) | | | | | | | |
| ISO/IEC 18305, Information technology -- Real time locating systems -- Test and evaluation of localization and tracking systems | | ISO/IEC JTC 1/SC 31/WG 5 | 10.99 | | | | | | | 386. |
| ISO/IEC 24730-1, Information technology -- Real-time locating systems (RTLS) -- Part 1: Application program interface (API) | | ISO/IEC JTC 1/SC 31/WG 5 | 30.60 | | | | | | | 387. |
| ISO/IEC 24730-2:2012, Information technology -- Real time locating systems (RTLS) -- Part 2: Direct Sequence Spread Spectrum (DSSS) 2,4 GHz air interface protocol | | ISO/IEC JTC 1/SC 31/WG 5 | 60.60 | | | | | | | 388. |
| ISO/IEC 24730-21:2012, Information technology -- Real time locating systems (RTLS) -- Part 21: Direct Sequence Spread Spectrum (DSSS) 2,4 GHz air interface protocol: Transmitters operating with a single spread code and employing a DBPSK data encoding and BPSK spreading scheme | | ISO/IEC JTC 1/SC 31/WG 5 | 60.60 | | | | | | | 389. |
| ISO/IEC 24730-22:2012, Information technology -- Real time locating systems (RTLS) -- Part 22: Direct Sequence Spread Spectrum (DSSS) 2,4 GHz air interface protocol: Transmitters operating with multiple spread codes and employing a QPSK data encoding and Walsh offset QPSK (WOQPSK) spreading scheme | | ISO/IEC JTC 1/SC 31/WG 5 | 60.60 | | | | | | | 390. |
| ISO/IEC 24730-61, Information technology -- Real time locating systems (RTLS) -- Part 61: Low rate pulse repetition frequency Ultra Wide Band (UWB) air interface | | ISO/IEC JTC 1/SC 31/WG 5 | 40.60 | | | | | | | 391. |
| ISO/IEC 24730-62, Information technology -- Real time locating systems (RTLS) -- Part 62: High rate pulse repetition frequency Ultra Wide Band (UWB) air interface | | ISO/IEC JTC 1/SC 31/WG 5 | 40.60 | | | | | | | 392. |
| ISO/IEC 29134 - Automatic identification and data capture techniques -- Air interface specification for Mobile RFID interrogators | This International Standard establishes guidelines for the conduct of privacy impact assessments that are used for the protection of personally identifiable information (PII).<br>It should be used by organizations that are establishing, operating or significantly changing programs, systems or business processes that involve the processing of PII. This International Standard also provides guidance on privacy risk treatment options. Privacy Impact Assessments can be conducted at various stages in the life cycle of a programme, system or business process ranging from the requirement analysis phase to decommissioning. In order to support Privacy by Design, the results of privacy impact assessments have to be considered in the specification of the system.<br>In particular, it will provide a specific method for privacy impact assessment.<br>It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and | ISO/IEC JTC 1/SC 31/WG 6 | Publication by 2016-05 | | IS | | | | | 393. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | not-for-profit organizations. This standard is relevant to any staff involved in designing or implementing projects, including operating data processing systems and services, which will have an impact on privacy within an organization and, where appropriate, external parties are supporting such activities.<br>This Standard describes privacy risk assessment as introduced by ISO/IEC 29100:2011. For the basic elements of the privacy framework and the privacy principles, reference is made to ISO/IEC 29100:2011.<br>For principles and guidelines on risk management, reference is made to ISO 31000:2009. ISO 31000 forms a baseline reference for a risk management framework that can be used in a PIA. Organizations need to select a risk management framework that is consistent with the organization's risk strategy and approach and leverage it in their deployment of this standard.<br>[Editor's note: The following is the scope defined at 2013 Incheon sessions. It is the proposal that is foreseen as the scope to be requested with the scope change]<br>This International Standard:<br>- gives guidelines for a process for the conducting of privacy impact assessments;<br>- describes a structure and content of a PIA report.<br>It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.<br>This International Standard is relevant to those involved in designing or implementing projects, including operating data processing systems and services, that use PII that may have an impact on privacy within an organization and, where appropriate, external parties are supporting such activities | | | | | | | | | |
| ISO/IEC 29143, Information technology – Automatic identification and data capture techniques – Air interface specification for Mobile RFID interrogators | ISO/IEC 29143:2011 specifies<br>- Mobile RFID interrogator media access control,<br>- interrogator to interrogator and multiple interrogator to tag collision arbitration scheme including interrogator requirements,<br>- interrogator to interrogator and multiple interrogator to tag collision avoidance scheme, and<br>- tag memory use for Mobile RFID applications.<br>ISO/IEC 29143:2011 does not specify<br>- physical interactions (the signaling layer of the communication link) between interrogators and tags,<br>- interrogator and tag operating procedures and commands, and<br>- the collision arbitration algorithm used to singulate (separate to the current response slot) a specific tag in a multiple-tag environment. | ISO/IEC JTC 1/SC 31/WG 6 | International Standard | 2011-01-31 | | MIIM | | | | 394. |
| ISO/IEC 29143:2011, Information technology -- Automatic identification and data capture techniques -- Air interface specification for Mobile RFID interrogators | | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 | | | | | | | 395. |
| ISO/IEC 29173-1, Information technology -- Mobile item identification and management -- Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-63 Type C | | ISO/IEC JTC 1/SC 31/WG 6 | 50.20<br>(Start date: 2012-09-05<br>End date: 2012-11-06) | | | | | | | 396. |
| ISO/IEC 29173-1, Information technology – Mobile item identification and management – Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-6 Type C | ISO/IEC 29173-1 defines an interface protocol between a device driver of a mobile AIDC application platform and a mobile RFID interrogator within a mobile AIDC terminal. In accordance to the ISO/IEC 18000-6 type C and ISO/IEC 29143 RFID air interface standard, this standard will include: types of command / response / notification protocol messages and their usages; protocol message format; and protocol message exchange procedures, as | ISO/IEC JTC 1/SC 31/WG 6 | International Standards | 2012-11-30 | | MIIM | | | 2008-11-05 | 397. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | the communication protocol between an interrogator and phone. |  |  |  |  |  |  |  |  |  |
| ISO/IEC 29174-1, Information technology -- UII scheme and encoding format for Mobile AIDC services -- Part 1: Identifier scheme for multimedia information access triggered by tag-based identification | ISO/IEC 29174-1 defines an identifier scheme for Mobile AIDC services and Registration Authority (RA) and registration procedures of the ID that was developed to support service requirements of an identifier scheme for Mobile AIDC services. This standard consists of two parts. Part 1 (ISO/IEC 29174-1) defines requirements, structure and encoding formats of the ID. | ISO/IEC JTC 1/SC 31/WG 6<br>(2009 ~ 2012) | DIS posted 31n3564 2011-08-26 to 2012-02-24 | 2012-07-01 |  | MIIM |  |  | 2011-01-24, registered as single part standard on 2008-11-05 | 398. |
| ISO/IEC 29174-1, Information technology -- UII scheme and encoding format for Mobile AIDC services -- Part 1: Identifier scheme for multimedia information access triggered by tag-based identification |  | ISO/IEC JTC 1/SC 31/WG 6 | 50.20<br>(Start date: 2012-07-17<br>End date: 2012-09-18) |  |  |  |  |  |  | 399. |
| ISO/IEC 29174-2, Information technology -- UII scheme and encoding format for Mobile AIDC services -- Part 2: Registration procedures | ISO/IEC 29174-2 defines an identifier scheme for Mobile AIDC services and Registration Authority (RA) and registration procedures of the ID that was developed to support service requirements of an identifier scheme for Mobile AIDC services. This standard consists of two parts. Part 2 (ISO/IEC 29174-2) defines procedures of ID scheme, obligations and requirements of Registration Authority (RA) as managing the ID. | ISO/IEC JTC 1/SC 31/WG 6<br>(2009 ~ 2012) | DIS ballot passed DoC meeting 2012-03-12 | 2012-07-01 |  | MIIM |  |  | 2011-01-24, registered as single part standard on 2008-11-05 | 400. |
| ISO/IEC 29174-2, Information technology -- UII scheme and encoding format for Mobile AIDC services -- Part 2: Registration procedures |  | ISO/IEC JTC 1/SC 31/WG 6 | 50.60 |  |  |  |  |  |  | 401. |
| ISO/IEC 29175, Information technology – Mobile item identification and management – User data for Mobile AIDC services | ISO/IEC 29175 defines user data for the purpose of encoding and identifying user data in Mobile AIDC services using ISO/IEC 29143 RF tags, ISO/IEC 18000-6, REV1 Type C RF tags, and ISO/IEC 15434-applied ORM such as linear bar codes and two-dimensional symbols. Identifiers for user data follow ASC MH10 Data Identifiers, which are given in ANSI MH10.8.2, hereafter referred to as the “ASC MH10 Data Identifiers”, are standardized in ANSI MH10.8.2 and ISO/IEC 15418. | ISO/IEC JTC 1/SC 31/WG 6 | International Standard | 2012-03 |  | MIIM |  |  | 2008-11-05 | 402. |
| ISO/IEC 29176, Information technology – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID services | ISO/IEC 29176 defines a privacy protocol between a Mobile RFID interrogator and a Mobile RFID tag. This international standard does not deal with security issues such as mutual authentication method, data encryption method, and cipher algorithm suite. This international standard does cover the operation procedure of the interrogator for the protection of the consumer’s privacy. This international standard can be applied to tags and interrogators conforming to ISO/IEC 18000-6 Type C and ISO/IEC 18000-3 MODE 3 RFID air interfaces without any modification of hardware and additional commands. | ISO/IEC JTC 1/SC 31/WG 6 | International Standards | 2012-10-06 |  | MIIM |  |  | 2008-11-05 | 403. |
| ISO/IEC 29177, Information technology -- Automatic identification and data capture technique -- Identifier resolution protocol for multimedia information access triggered by tag-based identification |  | ISO/IEC JTC 1/SC 31/WG 6 | 50.60 |  |  |  |  |  |  | 404. |
| ISO/IEC 29178, Information technology – Mobile item identification and management – Service broker for Mobile AIDC services | ISO/IEC 29178 defines the functions of a service broker supporting service control, MII recognition and MII resolution related functions in Mobile AIDC service architecture, which uses MII (ISO/IEC 29174) as an identifier. For the use of a service broker by a Mobile AIDC terminal, definition is required of the interface between a terminal and a service broker. This standard describes that interface. | ISO/IEC JTC 1/SC 31/WG 6 | International Standard | 2012-03 |  | MIIM |  |  | 2008-11-05 | 405. |
| ISO/IEC 29179, Information | ISO/IEC 29179 defines the Mobile AIDC application programming | ISO/IEC JTC 1/SC | International | 2012-01-20 |  | MIIM |  |  | 2008-11-05 | 406. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| technology – Mobile item identification and management – Mobile AIDC application programming interface | interface to give a standardized functional view over different Mobile AIDC application platforms. In addition, ISO/IEC 29179 provides a description of Mobile AIDC applications and specifies the functional requirements of Mobile AIDC application interfaces. | 31/WG 6 | Standard |  |  |  |  |  |  |  |
| ISO/IEC TR 29172, Information technology – Mobile item identification and management – Reference architecture for Mobile AIDC services | ISO/IEC 29172 defines an overall service architecture to provide Mobile AIDC services. It describes various architectural configurations enabled by a set of Mobile AIDC-relevant standards such as ISO/IEC 18004, 15424, 16480, 29143, 18000-3 Mode 3, 18000-6, 29173, 29174, 29175, 29176, 29177, 29178, 29179, 29168, and 9834-9, in terms of relevant standards and their roles and positions in various implementations. The overall service architecture deals with all of the relevant standards, their interface relationships and how to incorporate them to develop Mobile AIDC services based on resulting Mobile AIDC technologies. | ISO/IEC JTC 1/SC 31/WG 6 | International Standard | 2011-11-08 |  | MIIM |  |  | 2008-11-05 | 407. |
| ISO/IEC/IEEE 21450 - Information technology – Smart Transducer Interface for Sensors and Actuators – Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats | ISO/IEC/IEEE 21450:2010 provides a common basis for members of the ISO/IEC/IEEE 21451 series of International Standards to be interoperable. It defines the functions that are to be performed by a transducer interface module (TIM) and the common characteristics for all devices that implement the TIM. It specifies the formats for Transducer Electronic Data Sheets (TEDS). It defines a set of commands to facilitate the setup and control of the TIM as well as reading and writing the data used by the system. Application programming interfaces (APIs) are defined to facilitate communications with the TIM and with applications. | ISO/IEC JTC 1/SC 31/WG 6 | Published by ISO/IEC/IEEE | 2011-12-15 |  | Sensor and actuator |  |  | N/A | 408. |
| ISO/IEC/IEEE 21450:2010, Information technology -- Smart transducer interface for sensors and actuators -- Common functions, communication protocols, and Transducer Electronic Data Sheet (TEDS) formats |  | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 |  |  |  |  |  |  | 409. |
| ISO/IEC/IEEE 21451-1 - Information technology – Smart Transducer Interface for Sensors and Actuators – Network Capable Application Processor (NCAP) Information Model | ISO/IEC/IEEE 21451-1:2010 defines an object model with a network-neutral interface for connecting processors to communication networks, sensors, and actuators. The object model contains blocks, services, and components; it specifies interactions with sensors and actuators and forms the basis for implementing application code executing in the processor. | ISO/IEC JTC 1/SC 31/WG 6 | PSDO Standard published | 2010-05-20 |  | Sensor and actuator |  |  | N/A | 410. |
| ISO/IEC/IEEE 21451-1:2010, Information technology -- Smart transducer interface for sensors and actuators -- Part 1: Network Capable Application Processor (NCAP) information model |  | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 |  |  |  |  |  |  | 411. |
| ISO/IEC/IEEE 21451-2 - Information technology – Smart Transducer Interface for Sensors and Actuators – Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats | ISO/IEC/IEEE 21451-2:2010 defines a digital interface for connecting transducers to microprocessors. It describes a Transducer Electronic Data Sheet (TEDS) and its data formats. It defines an electrical interface, read and write logic functions to access the TEDS, and a wide variety of transducers. ISO/IEC/IEEE 21451-2:2010 does not specify signal conditioning, signal conversion, or how the TEDS data is used in applications. | ISO/IEC JTC 1/SC 31/WG 6 | PSDO Standard published | 2010-05-20 |  | Sensor and actuator |  |  | N/A | 412. |
| ISO/IEC/IEEE 21451-2:2010, Information technology -- Smart transducer interface for sensors and actuators -- Part 2: Transducer to microprocessor communication protocols and Transducer Electronic Data Sheet (TEDS) formats |  | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 |  |  |  |  |  |  | 413. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC/IEEE 21451-4 - Information technology – Smart Transducer Interface for Sensors and Actuators – Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats | ISO/IEC/IEEE 21451-4:2010 defines the protocol and interface that allows analog transducers to communicate digital information with an ISO/IEC/IEEE 21451 object. It also defines the format of the Transducer Electronic Data Sheet (TEDS), which is based on the ISO/IEC/IEEE 21451-2 TEDS. It does not specify the transducer design, signal conditioning, or the specific use of the TEDS. | ISO/IEC JTC 1/SC 31/WG 6 | PSDO Standard published | 2010-05-20 | | Sensor and actuator | | | N/A | 414. |
| ISO/IEC/IEEE 21451-4:2010, Information technology -- Smart transducer interface for sensors and actuators -- Part 4: Mixed-mode communication protocols and Transducer Electronic Data Sheet (TEDS) formats | | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 | | | | | | | 415. |
| ISO/IEC/IEEE 21451-5 - Information technology – Smart Transducer Interface for Sensors and Actuators – Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats | ISO/IEC/IEEE 21451-5 defines a wireless interface for sensors. It specifies radio-specific protocols for this wireless interface. It defines communication modules that connect the wireless transducer interface module (WTIM) and the network capable applications processor (NCAP) using the radio-specific protocols. It also defines the transducer electronic data sheets (TEDS) for the radio-specific protocols. | ISO/IEC JTC 1/SC 31/WG 6 | 2011-10-03 Corrigendum to IEEE Standard 1451.5-2007 PAR approved 17-Jun-2010. In final approval "pre-ballot" Once approved to WG 6 FDIS ballot | B4 2014-12-31 | | Sensor and actuator | | | 2010-06-17 | 416. |
| ISO/IEC/IEEE 21451-7 - Information technology – Standard for a Smart Transducer Interface for Sensors and Actuators - Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats | ISO/IEC/IEEE 21451-7 defines data formats to facilitate communications between radio frequency identification (RFID) systems and smart RFID tags with integral transducers (sensors and actuators). The standard defines new transducer electronic data sheet (TEDS) formats based on the ISO/IEC/IEEE 21451 family of standards.<br>This standard also defines a command structure and specifies the communication methods with which the command structure is designed to be compatible. | ISO/IEC JTC 1/SC 31/WG 6 | PSDO Standard published<br>2010-05-20 | 2010-05-20 | | Sensor and actuator | | | N/A | 417. |
| ISO/IEC/IEEE 21451-7:2011, Information technology -- Smart transducer interface for sensors and actuators -- Part 7: Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats | | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 | | | | | | | 418. |
| ISO/IEC/IEEE 8802-15-4 - Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs) | ISO/IEC/IEEE 8802-15-4 defines the protocol and compatible interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN). | ISO/IEC JTC 1/SC 31/WG 6 | PSDO Standard published<br>2010-10-13 | 2010-10-13 | | Sensor and actuator | | | N/A | 419. |
| ISO/IEC/IEEE 8802-15-4:2010, Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless | | ISO/IEC JTC 1/SC 31/WG 6 | 60.60 | | | | | | | 420. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| personal area networks (WPANs) | | | | | | | | | | |
| ISO/IEC 29167-1, Information technology -- Automatic identification and data capture techniques -- Part 1: Air interface for security services and file management for RFID architecture | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 421. |
| ISO/IEC 29167-1:2012, Information technology -- Automatic identification and data capture techniques -- Part 1: Air interface for security services and file management for RFID architecture | | ISO/IEC JTC 1/SC 31/WG 7 | 60.60 | | | | | | | 422. |
| ISO/IEC 29167-10, Information technology -- Automatic identification and data capture techniques -- Part 10: Air Interface for security services crypto suite AES128 | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 423. |
| ISO/IEC 29167-11, Information technology -- Automatic identification and data capture techniques -- Part 11: Air Interface for security services crypto suite PRESENT-80 | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 424. |
| ISO/IEC 29167-12, Information technology -- Automatic identification and data capture techniques -- Part 12: Air Interface for security services crypto suite ECC-DH | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 425. |
| ISO/IEC 29167-13, Information technology -- Automatic identification and data capture techniques -- Part 13: Air Interface for security services crypto suite Grain-128A | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 426. |
| ISO/IEC 29167-14, Information technology -- Automatic identification and data capture techniques -- Part 14: Air Interface for security services crypto suite - AES OFB-like | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 427. |
| ISO/IEC 29167-15, Information technology -- Automatic identification and data capture techniques -- Part 15: Air Interface for security services crypto suite XOR | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 428. |
| ISO/IEC 29167-16, Information technology -- Automatic identification and data capture techniques -- Part 16: Air Interface for security services crypto suite ECDSA-ECDH | | ISO/IEC JTC 1/SC 31/WG 7 | 10.99 | | | | | | | 429. |
| ISO/IEC 29167-17, Information Technology -- Automatic Identification and Data Capture Techniques -- Part 17: Air Interface | | ISO/IEC JTC 1/SC 31/WG 7 | 10.60 | | | | | | | 430. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
| for Security Services Crypto Suite cryptoGPS |  |  |  |  |  |  |  |  |  |  |
| ISO/IEC 29168-2, Information technology – Open Systems Interconnection – Procedures for the Object Identifier Resolution System Operational Agency | This International Standard specifies the mechanisms and criteria that shall be applied for the selection and approval of the operational agency, and includes procedures that the operational agency shall follow.<br>It also addresses any future modification of the procedures, and the procedures for any change of the operational agency.<br>It lists the OID nodes for which the operational agency is required to provide ORS support.<br>It gives the required level of support for these nodes.<br>It gives the procedures by which lower level nodes can apply for ORS support (class A, class B, or class C), and the role of the operational agency in providing these levels of support.<br>It determines the basis for charges that might be levied for these levels of support. | ISO/IEC JTC 1/SC 6 | International Standard | 2011-09-12 |  | NID |  |  |  | 431. |
| ISO/IEC TR 29181-1:2012 Information technology -- Future Network -- Problem statement and requirements -- Part 1: Overall aspects | ISO/IEC TR 29181-1:2012 describes the definition, general concept, problems and requirements for Future Network (FN). It also discusses a milestone for standardization on FN. The scope includes: motivation of FN; definition, general concept, and terminologies of FN; services and applications in FN; problems with current networks; design goals and high-level requirements for FN; milestones for standardization on FN. | ISO/IEC JTC 1/SC 6/WG 7 | Published |  |  | Network | Future Network |  | SC 6 Future Network project is based on recognition that "explosion of application areas demands a more rigid, reliable, and complete networking technology " (6N13295). new communication needs may require new network platforms, and newly designed network architectures may also have huge impact on new applications.<br>IoT (M2M) is one of the communication services that FN intends to support with new network architectural designs.<br>The significance of SC 6 FN with regard to IoT(M2M) is:<br>it brings new perspectives on how the network architecture should be changed or created to provide adequate support to IoT(M2M).<br>it encourages technology developers to consider how to take advantage of the clean slate designed FN structure to optimize IoT(M2M) communications.<br>other than rely on existing networks or place hopes on modifying current networks, FN provides | 432. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | a third alternative which is to design networks to satisfy the needs of IoT(M2M) communications. | |
| ISO/IEC TR 29181-2:2012 Information technology -- Future Network -- Problem statement and requirements -- Part 2: Naming and Addressing | ISO/IEC TR 29181-2 describes the general characteristics of Future Network Naming and Addressing Schemes including problem statement, design objectives, gap analysis, and development directions. The topics include: the characteristics and deficiencies of existing NAS in existing network; a list of major technical challenges to assure that the FN-NAS will be able to provide solid technical support from the base level to meet the objectives of FN; the general characteristics of Future Network are discussed and their impact on NAS design; examines the gap between existing network NAS and future network performance expectations; specify objectives and principles for NAS design. | ISO/IEC JTC 1/SC 6/WG 7 | DTR ballot | 6-Mar.-2014 | | Network | Future Network | | Ibid. | 433. |
| ISO/IEC TR 29181-3:2013 Information technology -- Future Network -- Problem statement and requirements -- Part 3: Switching and routing | ISO/IEC TR 29181-3:2013 contains the problem statement and requirements for switching and routing in the Future Network, in particular: 1, description of the requirements for carrying data over digital networks; 2, description of the ways in which these requirements are not satisfied by current networks; 3, functional architecture for switching and routing in the Future Network; 4, and requirements for control plane information flows for finding, setting up, and tearing down routes. The requirements in 4 include support for both current ("legacy") and future ("new") switching technologies, to aid the transition between them. | ISO/IEC JTC 1/SC 6/WG 7 | Published | | | Network | Future Network | | Ibid. | 434. |
| ISO/IEC TR 29181-4:2013 Information technology -- Future Network -- Problem statement and requirements -- Part 4: Mobility | ISO/IEC TR 29181-4:2013 describes the problem statements of current network and the requirements for Future Network in the mobility perspective. It mainly specifies problems of the current network in mobile environment, and requirements for mobility support in Future Network. In addition, ISO/IEC TR 29181-4:2013 gives information on existing mobility control schemes in the current network, examples of high-level mobility control architecture for Future Network, distributed mobility control in the Proxy Mobile IPv6 networks, and additional considerations for Future Network mobility. | ISO/IEC JTC 1/SC 6/WG 7 | Published | | | Network | Future Network | | Ibid. | 435. |
| ISO/IEC TR 29181-5 Information technology -- Future Network -- Problem statement and requirements -- Part 5: Security | ISO/IEC TR 29181-5 describes the problem statements of current network and the requirements for Future Network in the security perspective. It mainly specifies Problems of the current network in security environment and requirements for security support in Future Network. | ISO/IEC JTC 1/SC 6/WG 7 | DTR ballot | 6-Mar.-2014 | | Network | Future Network | | Ibid. | 436. |
| ISO/IEC TR 29181-6:2013 Information technology -- Future Network -- Problem statement and requirements -- Part 6: Media Distribution | ISO/IEC TR 29181-6:2013 describes the problem statement and requirements for the Future Network in the perspective of media transport. ISO/IEC TR 29181-6:2013 specifies: detailed description of the media transport requirements in the Future Network; identification and definition of services, basic and media services, which will fit the requirements for communications over heterogeneous environments supporting various user preferences, for any kind of media content, either time-dependent or time-independent; requirements and functionalities of Media Aware Network Elements, which are intended to be nodes in the network to provide seamless media experiences to users. | ISO/IEC JTC 1/SC 6/WG 7 | Published | | | Network | Future Network | | Ibid. | 437. |
| ISO/IEC TR 29181-7:2013 Information technology -- Future Network -- Problem statement and requirements -- Part 7: Service Composition | ISO/IEC TR 29181-7:2013 describes the problem statement, requirements and a functional building block for the Future Network (FN) from the perspective of service composition. The goal of is to: analyse and classify problems of the current solutions on the service composition, identify requirements on the service composition for the FN, describe some technical aspects of the service composition for the FN, and propose a functional building block of the service composition including functional components and their reference points among them. ISO/IEC TR 29181-7:2013 also introduces various on-going | ISO/IEC JTC 1/SC 6/WG 7 | Published | | | Network | Future Network | | Ibid. | 438. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | standardization and research activities related to service composition. | | | | | | | | | |
| ISO / IEC 10030, Information technology -- Telecommunications and information exchange between systems -- End System Routeing Information Exchange Protocol for use in conjunction with ISO/IEC 8878 | Cancels and replaces the first edition (1990). Defines a protocol for the exchange of routeing information between an End System and a Subnetwork Address Resolution Entity, and between an Intermediate System and a Subnetwork Address Resolution Entity. Applicable to: End Systems which operate according to the main body of ISO/IEC 8878 to provide and support the OSI Connection-mode Network Service using ISO/IEC 8208; Subnetwork Address Resolution Entities which operate ISO/IEC 8208; Intermediate Systems which operate ISO/IEC 8208 | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 439. |
| ISO / IEC 10747, Information technology -- Telecommunications and information exchange between systems -- Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs | Specifies a protocol to be used by boundary intermediate systems to acquire and maintain information for the purpose of routeing NPDUs between different routeing domains. Lays down the procedures for the exchange of inter-domain reachability and path information between BISs, the procedures for maintaining inter-domain routeing information bases within a BIS, the encoding of protocol data units used to distribute inter-domain routeing information between BISs, the functional requirements for implementations that claim conformance to this standard. The protocol described operates at the level of IETF routeing domains. Does not cover the establishment of administrative domains | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 440. |
| ISO/IEC 10028,Information technology -- Telecommunications and information exchange between systems -- Definition of the relaying functions of a Network layer intermediate system | Is intended for use in guiding the design and application of real interworking units and real subnetworks (e.g. local area networks and private packet switched networks) which are to support the OSI network service. As the principal means for expressing the definition, the concept of the network internal layer service is used. The definition includes the invocation of network routing functions as a necessary element of the network relaying functions. The definition of network relaying functions applies both to a subnetwork supporting all elements of the network service and to a network relay system interconnecting two subnetworks | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 441. |
| ISO/IEC 10177, Information technology -- Telecommunications and information exchange between systems -- Provision of the connection-mode Network internal layer service by intermediate systems using ISO/IEC 8208, the X.25 Packet Layer Protocol | Specifies the method by which a network-layer interworking unit (IWU) uses the X.25 packet layer protocol to support the OSI connection-mode network service. The specification is expressed in terms of a mapping between the network internal layer service defined in ISO/IEC 10028 and the virtual call and permanent virtual circuit services of the X.25 packet layer protocol. Provides the PICS (Protocol Implementation Conformance Statement) proforma in compliance with the relevant requirements, and in accordance with the relevant guidance, given in ISO/IEC 9646-2 | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 442. |
| ISO/IEC 10589, Information technology -- Telecommunications and information exchange between systems -- Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473) | The protocol defined in this International Standard is positioned with respect to other related standards by the layers defined in ISO 7498 and by the structure defined in ISO 8648. In particular, it is a protocol of the Network Layer. This protocol permits Intermediate Systems within a routeing domain to exchange configuration and routeing information to facilitate the operation of the routeing and relaying functions of the Network Layer. The protocol is designed to operate in close conjunction with ISO 9542 and ISO 8473. ISO 9542 is used to establish connectivity and reachability between End Systems and Intermediate Systems on IETF subnetworks. Data is carried using the protocol specified in ISO 8473. The related algorithms for route calculation and maintenance are also described | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 443. |
| ISO/IEC 10733, Information technology -- Elements of management information related to the OSI Network Layer | This Recommendation \| International Standard is positioned with respect to other related Recommendations and International Standards by the layers defined in the Reference Model for Open System Interconnection (see ITU-T Rec. X.200 \| ISO/IEC 7498-1). In particular, it is concerned with the definition of Network Layer management information. | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 444. |
| ISO/IEC 11577, Information technology -- Open Systems Interconnection -- Network layer security protocol | Specifies a protocol to be used by End Systems and Intermediate Systems in order to provide security services in the Network layer, which is defined by CCITT Rec. X.213, ISO/IEC 8348 and ISO 8648. The protocol defined herein is called the Network Layer Security Protocol (NLSP) | ISO/IEC JTC 1/SC6 | Technology | | | network level | Security | | | 445. |
| ISO/IEC 8208, Information technology -- Data communications -- X.25 Packet Layer Protocol for Data Terminal Equipment | This International Standard specifies the procedures, formats and facilities at the Packet Layer for Data Terminal Equipment (DTE) operating in conformance with ITU-T Recommendation X.25. Both Virtual Call and Permanent Virtual Circuit modes of operation are covered | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 446. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 8348, Information technology -- Open Systems Interconnection -- Network service definition | ISO/IEC 8348:2002 defines the set of capabilities, in terms of abstract service definition, provided by the Network Layer to the Transport Layer. For designers of Transport Layer protocols, it provides a definition of the Network service to allow design and implementation independent of details of the Network Layer protocol. For designers of Network Layer protocols, it defines the set of capabilities to be made available through the action of the protocol | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 447. |
| ISO/IEC 8473-1, Information technology -- Protocol for providing the connectionless-mode network service: Protocol specification | This Recommendation \| International Standard is positioned with respect to other related Recommendations and International Standards by the layers defined in ITU-T Rec. X.200 \| ISO/IEC 7498-1. In particular, it is a protocol of the Network layer. The protocol specified by this Recommendation International Standard may be used between Network entities in end systems, between Network entities in intermediate systems, or between a Network entity in an end system and a Network entity in an intermediate system. In an end system, it provides the connectionless-mode Network service defined in ITU-T Rec. X.213 \| ISO/IEC 8348 | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 448. |
| ISO/IEC 8473-2, Information technology -- Protocol for providing the connectionless-mode network service -- Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork | Differs from the other related International Standards by the layers defined in ISO/IEC 7498-1. In particular, it defines the way in which a local area network that conforms to ISO/IEC 8802 may be used as a subnetwork within the network layer to provide the abstract underlying service with respect to which the protocol defined by ISO/IEC 8473-1 is specified | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 449. |
| ISO/IEC 8473-3, Information technology -- Protocol for providing the connectionless-mode network service: Provision of the underlying service by an X.25 subnetwork | Specifies the way in which the underlying service assumed by the protocol defined by ITU-T Rec. X.233 ISO/IEC 8473-1 is provided by a subnetwork that conforms to ITU-T Recommendation X.25 through the operation of a Subnetwork Dependent Convergence Function (SNDCF) as described in ISO/IEC 8648. Also provides the PICS proforma for this protocol, in compliance with the relevant requirements and in accordance with the relevant guidance | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 450. |
| ISO/IEC 8473-4, Information technology -- Protocol for providing the connectionless-mode network service: Provision of the underlying service by a subnetwork that provides the OSI data link service | Specifies the way in which the underlying service assumed by the protocol defined by ITU-T Rec. X.233 ISO/IEC 8473-1 is provided by a subnetwork that provides the OSI Data Link service defined by CCITT Rec. X.212 ISO/IEC 8886, through the operation of a Subnetwork Dependent Convergence Function (SNDCF) as described in ISO/IEC 8648. Also provides the PICS proforma for this protocol, in compliance with the relevant requirements and in accordance with the relevant guidance | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 451. |
| ISO/IEC 8473-5,Information technology -- Protocol for providing the connectionless-mode network service: Provision of the underlying service by ISDN circuit-switched B-channels | This Recommendation International Standard is positioned with respect to other related Recommendations and International Standards by the layers defined in ITU-T Rec. X.200 I ISO/IEC 7498-l. In particular, it defines the way in which the B-channels of an ISDN subnetwork may be used within the Network layer to provide the abstract underlying service with respect to which the protocol defined by ITU-T Rec. X.233 I ISO/IEC 8473-l is specified | ISO/IEC JTC 1/SC6 | International standard | | | network level | | | | 452. |
| ISO/IEC 8602-am1, Amendment 1 - Information technology -- Protocol for providing the OSI connectionless-mode transport service - Addition of connectionless-mode multicast capability | Defines additional assumptions concerning the services optionally provided by the Network layer and adds no new functions of its own. The identical text is published as ITU-T Rec. X.234/Amd. 1 | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 453. |
| ISO/IEC 8878, Information technology -- Telecommunications and information exchange between systems -- Use of X.25 to provide the OSI Connection-mode Network Service | For a protocol to support the CONS, there must be a mapping between the abstract primitives and parameters of the CONS and the real elements of the protocol. For the X.25 Packet Layer Protocol (PLP), the main body of this standard provides such a mapping for the X.25/PLP-1984 using Virtual Calls. Also provides a mapping of the CONS primitives and parameters to the X.25/PLP-1980 plus an SNDCP. These mappings apply to the X.25 VC service. Specifies two sets of procedures from which three classes of implementation are described | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 454. |
| ISO/IEC TR 12861,Information technology -- Telecommunications and information exchange between systems -- Next Generation Corporate Networks (NGCN) -- Identification and routing | ISO/IEC TR 12861:2009 is one of a series of publications that explore IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on inter-domain communication, including communication between parts of the same enterprise, between enterprises and between enterprises and carriers. ISO/IEC TR 12861:2009 discusses issues related to user identities and routing and | ISO/IEC JTC 1/SC6 | Technology | | | network level | | | | 455. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | builds upon concepts introduced in ISO/IEC TR 12860 |  |  |  |  |  |  |  |  |  |
| ISO/IEC/TR 10029, Information technology -- Telecommunications and information exchange between systems -- Operation of an X.25 interworking unit | Describes the function of the Interworking unit (IWU) in terms of the mapping between Protokol Data Units (PDUs) that it receives from one interface, and PDUs that it then transmits which could be on either interface of the IWU. Also describes procedures an IWU can initiate on each interface independently. Each interface corresponds to one instance of a DTE/DXE connection, and both interfaces of the Interworking Unit operate as a DTE as specified by ISO 8208. References: ISO 8208; 8880-2; 8881 | ISO/IEC JTC 1/SC6 | Technology |  |  | network level | X.25 |  |  | 456. |
| ISO/IEC/TR 9575, Information technology -- Telecommunications and information exchange between systems -- OSI Routeing Framework | Provides a framework in which OSI protocols for routeing may be developed and to expedite the progression of routeing protocols through the standardisation process. Reflects the current state of OSI routeing and does not preclude future extensions and developments. Replaces the first edition, which has been technically revised | ISO/IEC JTC 1/SC6 | Technology |  |  | network level | Routing |  |  | 457. |
| ISO/IEC/TR 9577, Information technology -- Protocol identification in the network layer | This Recommendation \| Technical Report provides: ——the description of a means to permit a protocol to be identified; ——a record of the structure and allowable ranges of protocol identifier(s) which can be assigned by ITU-T, ISO/IEC and other authorities; ——a record of the values of protocol identifiers used by OSI Network layer protocols and non-OSI protocols occupying a similar position: in particular, protocols with protocol control information commencing in octet 1 of the protocol data unit (header-oriented protocols), and protocols with protocol control information commencing in the final octet of the protocol data unit (trailer-oriented protocols), are covered ——a record of the values that are in use as protocol control information in non-Network layer protocols where they impact on Network layer protocol identification | ISO/IEC JTC 1/SC6 | Technology |  |  | network level |  |  |  | 458. |
| ISO/IEC 20005, Information technology - Sensor Networks: Services and interfaces supporting collaborative information processing in intelligent sensor networks | This international standard specifies services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks which includes:<br>- CIP functionalities and CIP functional model<br>- Common services supporting CIP<br>- Common service interfaces to CIP | ISO/IEC JTC 1/WG 7 | FDIS | 1-Jul-2013 | Technology | Information Processing | Sensor Network | N/A |  | 459. |
| ISO/IEC 20005, Services and Interfaces Supporting Collaborative Information Processing in Intelligent Sensor Networks | Services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks | ISO/IEC JTC 1/WG 7 | DIS | 2013-10 |  | Sensor networks |  |  | 2010-04 | 460. |
| ISO/IEC 29182-1, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 1: General overview and requirements | This part of ISO/IEC 29182 provides a general overview of the characteristics of a sensor network and the organisation of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks. | ISO/IEC JTC 1/WG 7 | IS 1st Edition | 1-Jun-2013 | Technology | Architecture | Sensor Network | N/A |  | 461. |
| ISO/IEC 29182-1, Reference architecture for sensor network applications and services | General overview and the requirements identified for the reference architecture | ISO/IEC JTC 1/WG 7 | IS | 2103-05 |  | Sensor networks |  |  | 2010-03 | 462. |
| ISO/IEC 29182-2, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 2: Vocabulary and terminology | This part of ISO/IEC 29182 is intended to facilitate the development of international standards in sensor networks. It presents terms and definitions for selected concepts relevant to the field of sensor networks. It establishes a general description of concepts in this field and identifies the relationships among those concepts. It may also be used as guidance for development of other parts of ISO/IEC 29182 and any other sensor network related standard. | ISO/IEC JTC 1/WG 7 | IS 1st Edition | 1-Jun-2013 | Technology | Vocabulary and terminology | Sensor Network | N/A |  | 463. |
| ISO/IEC 29182-2, Reference architecture for sensor network applications and services – Part 2: Vocabulary/Terminology | Definitions of all the terminology and vocabulary used in the sensor network reference architecture | ISO/IEC JTC 1/WG 7 | IS | 2013-06 |  | Sensor networks |  |  | 2010-03 | 464. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 29182-3, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 3: Reference architecture views | This International Standard (IS) provides Sensor Network Reference Architecture (SNRA) views. The architecture views include business, operational, systems, and technical perspectives, and these views are presented in functional, logical, and/or physical views where applicable. This IS focuses on high-level architecture views which can be further developed by system developers and implementers for specific applications and services. This International Standard provides reference architecture views consistent with the requirements which are defined in Part 1 (General overview and requirements) and can be utilized more effectively with other Parts, especially with Part 4 (Entity Models) and Part 5 (Interface Definitions). | ISO/IEC JTC 1/WG 7 | FDIS | 1-Dec-2013 | Technology | Architecture | Sensor Network | N/A | | 465. |
| ISO/IEC 29182-3, Reference architecture for sensor network applications and services – Part 3: Reference architecture views | Reference architecture from various viewpoints, such as business, operational, system, technical, functional, and logical views | ISO/IEC JTC 1/WG 7 | DIS | 2015-09 | | Sensor networks | | | 2010-03 | 466. |
| ISO/IEC 29182-4, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 4: Entity models | This part of ISO/IEC 29182 presents models for the entities that enable sensor network applications and services according to the Sensor Network Reference Architecture (SNRA). | ISO/IEC JTC 1/WG 7 | FDIS | 1-Sep-2013 | Technology | Architecture | Sensor Network | N/A | | 467. |
| ISO/IEC 29182-4, Reference architecture for sensor network applications and services – Part 4: Entity models | Categorizes entities comprising a sensor network into two categories of physical and functional entities and presents models for all such entities | ISO/IEC JTC 1/WG 7 | DIS | | | Sensor networks | | | 2010-03 | 468. |
| ISO/IEC 29182-5, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 5: Interface definitions | This international standard provides the definitions and requirements of sensor network (SN) interfaces of the entities in the Sensor Network Reference Architecture and covers the following aspects:<br>- Interfaces between functional layers to provide service access for the modules in upper layer to exchange messages with modules in the lower layer<br>- Interfaces between entities introduced in the Sensor Network Reference Architecture enabling sensor network services and applications | ISO/IEC JTC 1/WG 7 | FDIS | 1-Sep-2013 | Technology | Architecture (Interface) | Sensor Network | N/A | | 469. |
| ISO/IEC 29182-5, Reference architecture for sensor network applications and services – Part 5: Interface definitions | Detailed information on the interfaces among various entities in the reference architecture | ISO/IEC JTC 1/WG 7 | FDIS | 2015-09 | | Sensor networks | | | 2010-03 | 470. |
| ISO/IEC 29182-6, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 6: Applications | This part of ISO/IEC 29182 gives<br>- a compilation of sensor network applications for which International Standardized Profiles (ISPs) are needed,<br>- guidelines for the structured description of sensor network applications and<br>- an example for a structured sensor network application description as a template.<br>Other sensor netwo+B19rk applications shall be described in the same way. These descriptions will support the development of ISPs in a second step. It does not cover ISPs for which drafting rules are described in ISO/IEC TR 10000. Due to the generic character of ISO/IEC 29182 fully developed ISPs cannot be expected here. | ISO/IEC JTC 1/WG 7 | CD | 1-Jun-2014 | Technology | Applications | Sensor Network | N/A | | 471. |
| ISO/IEC 29182-6, Reference architecture for sensor network applications and services – Part 6: Application Profiles | Application profiles that are derived from studies of use cases, scenarios, etc., for sensor network-based applications and services | ISO/IEC JTC 1/WG 7 | CD | 2015-09 | | Sensor networks | | | 2010-03 | 472. |
| ISO/IEC 29182-7, Information technology - Sensor Networks: Sensor Network Reference Architecture (SNRA) - Part 7: Interoperability guidelines | This part of ISO/IEC 29182 provides a general overview and guidelines for achieving interoperability between sensor network services and related entities in a heterogeneous sensor network. | ISO/IEC JTC 1/WG 7 | DIS | 1-Mar-2014 | Technology, Interoperability Testing | Architecture | Sensor Network | N/A | | 473. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ISO/IEC 29182-7, Reference architecture for sensor network applications and services – Part 7: Interoperability guidelines | Design principles for the reference architecture that take the interoperability requirements into account | ISO/IEC JTC 1/WG 7 | CD | 2015-09 | | Sensor networks | | | 2010-03 | 474. |
| ISO/IEC 30101, Information technology - Sensor Networks: Sensor Network and its interfaces for smart grid system | This International Standard (IS) is for sensor networks in order to support smart grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications and associated environmental challenges. This standard characterizes the requirements for sensor networks to support the aforementioned applications and challenges. Data from sensors in smart grid systems is collected, transmitted, published and acted upon to ensure efficient coordination of the various systems and<br>subsystems. The intelligence derived through the sensor networks supports synchronization, monitoring and responding, command and control, data/information processing, security, information routing, and human-grid<br>display/graphical interfaces. This International standard (IS) specifies:<br>- Interfaces between the sensor networks and other networks for smart grid system applications<br>- Sensor network architecture to support smart grid systems<br>- Interface between sensor networks with smart grid systems<br>- Sensor network based emerging applications and services to support smart grid systems | ISO/IEC JTC 1/WG 7 | CD | 1-Jun-2014 | Technology | Communications and Networking | Sensor Network | Smart Grid | | 475. |
| ISO/IEC 30101, Sensor Network and its Interface for Smart Grid System | Interfaces between the sensor networks and other networks for smart grid system applications, Sensor network architecture to support smart grid systems, Interface between sensor networks with smart grid systems | ISO/IEC JTC 1/WG 7 | CD | 2016-02 | | Sensor networks | | | 2010-08 | 476. |
| ISO/IEC 30128, Generic Sensor Network Application Interface | This international standard specifies generic (specific application neutral and specific sensor network protocol neutral) sensor network application interface which is used between any sensor network client (application, or sensor network integration platform) and any sensor network gateway. The scope of this interface is entitled as Protocol A of Interface 3 in Clause 7.4 of ISO/IEC 29182 Part 5.<br>This international standard covers:<br>- Overview of sensor network applications<br>- Overview of sensor network capabilities<br>- Generic sensor network application interface specification | ISO/IEC JTC 1/WG 7 | CD | 2015 | | Sensor networks | | | 2012 | 477. |
| ISO/IEC 30128, Information technology - Sensor Networks: Generic Sensor Network Application Inte | This international standard specifies the interface between the application layers of service providers and sensor network gateways, which is Protocol A in interface 3, defined in ISO/IEC 29182-5. This international standard covers<br>- Description of generic sensor network application operations<br>- Description of sensor network capabilities<br>- Specification of interface between the application layers of service providers and sensor network gateways | ISO/IEC JTC 1/WG 7 | CD | 1-Jun-2014 | Technology | Communications (Interface) | Sensor Network | N/A | | 478. |
| ITU-R M.2001, Objectives, characteristics and functional requirements of wide-area sensor and/or actuator network (WASN) systems | This Recommendation provides the objectives, system characteristics, functional requirements, service applications and fundamental network functionalities for mobile wireless access systems providing communications to a large number of ubiquitous sensors and/or actuators scattered over wide areas in the land mobile service.<br>The key objective of WASN systems is to support machine-to-machine service applications irrespective of machine locations. | ITU-R SG 5 WP 5A Q.250/5 | Draft new Recommendation | 2012-03 | | WASN | | | May 2009 | 479. |
| System design guidelines for wide area sensor and/or actuator network | This report provides detailed information for service applications, network architecture, system design guidelines, wireless applications and examples of wide area sensors and/or actuators | ITU-R SG 5 WP 5A Q.250/5 | Draft new Report | November 2011 | | WASN | | | May 2009 | 480. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| (WASN) systems | network (WASN) systems. | | | | | | | | | |
| Q.930, ISDN user-network interface layer 3 – General aspects | This Recommendation describes in general terms the D-channel layer 3 functions and protocol employed across an ISDN user-network interface. Details are provided in Recommendations in the Q.930-Series and in the Q.950-Series | ITU-T SG 11 | Recommendation | | | network level | | | | 481. |
| Q.931, ISDN user-network interface layer 3 specification for basic call control | This Recommendation specifies the procedures for the establishing, maintaining and clearing of network connections at the ISDN user-network interface. These procedures are defined in terms of messages exchanged over the D-channel of basic and primary rate interface structures. The functions and procedures of this protocol, and the relationship with other layers, are described in general terms in Recommendation Q.930/I.450 [1]. Annex M contains the additional basic call signalling requirement for the support of private network interconnection for VPN applications. | ITU-T SG 11 | Recommendation | | | network level | | | | 482. |
| Q.932,Digital subscriber signalling system No. 1 – Generic procedures for the control of ISDN supplementary services | This Recommendation defines the generic procedures applicable for the control of supplementary services at the user-network interface. These procedures may be used for the invocation and operation of supplementary services in association with existing calls or outside any existing calls. A significant new area addressed by this Recommendation is the support of Virtual Private Networks by means of new optional extensions | ITU-T SG 11 | Recommendation | | | network level | | | | 483. |
| Q.939: Typical DSS1 service indicator codings for ISDN telecommunications services | This Recommendation provides supplementary information on the usage of the compatibility information elements forIETF telecommunications services. It considers the telecommunications services as they are specified for publicISDNs. It does not specify additional codings of the compatibility information elements (BC, HLC and LLC) which might be required to support the request and provision of telecommunications services by private networks. | ITU-T SG 11 | Recommendation | | | network level | | | | 484. |
| Q.933 bis: Abstract test suite – Signalling specification for frame mode basic call control conformance testing for permanent virtual connections (PVCs) | test suite – Signalling specification for frame mode basic call control conformance testing for permanent virtual connections (PVCs) | ITU-T SG 13 | Recommendation | | | network level | | | | 485. |
| Q.933: ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring | This Recommendation specifies the architecture and the signalling using ITU-T Rec. Q.931 for establishing, maintaining and clearing circuit-switched bearers at the ISDN user-network interface for both basic and primary rate interfaces to access a Remote Frame Handler. Within a circuit switched bearer, one or more frame relay virtual circuits may be established. Establishing, maintaining and clearing frame relay switched virtual circuits are performed using X.36 signalling | ITU-T SG 13 | Recommendation | | | network level | | | | 486. |
| Q.3950, Testing and model network architecture for tag-based identification systems and functions | A set of standards and relevant implementations are necessary to enable tag-based identification applications and services over the NGN and other communication networks. The implementations are recommended to be verified according to given standards to evaluate their conformance and interoperability.<br>This Recommendation specifies a testing and model network architecture that describes target systems, target functions and system configurations in terms of model network, general procedures and testing requirements | ITU-T SG11 Q12<br>(2009 ~ 2012) | Recommendation | 2011-11 | | NID | | | January 2010 | 487. |
| Y.2062, Framework of object-to-object communication for ubiquitous networking in NGN | This draft Recommendation describes concept and high-level architectural model of object-to-object communication for ubiquitous networking in NGN and presents several requirements and mechanism for identification of all objects and providing connectivity to them. For this, this draft Recommendation covers the followings:<br>- General overview of ubiquitous networking in NGN in the end-user perspective;<br>- Basic concept and high-level architectural model for object to object communication with NGN;<br>- Requirements and technical considerations of object-to-object communication for ubiquitous networking;<br>- A mechanism for object to object communication. | ITU-T SG13 Q12<br>(2009 ~ 2012) | Recommendation | 2012-03 | | | | | | 488. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Y.2063, Framework of Web of Things | The scope of this Recommendation is to addresses Web of Things to realize the ubiquitous networking [ITU-T Y.2002]. The draft Recommendation covers:<br>- Requirement analysis of Web of Things<br>- Deployment model of Web of Things<br>- Identify the capabilities for Web of Things<br>- Functional architecture for Web of Things | ITU-T SG13 Q12<br>(2009 ~ 2012) | Recommendation | 2012-07 | | | | | | 489. |
| Y.energy-hn, Energy saving using smart objects in next generation home network | This draft Recommendation describes requirements and capabilities for energy saving using smart objects in next generation home network (NG-HN) and present several mechanisms for energy saving of constraint smart objects. For this, this draft Recommendation covers the following:<br>- General overview of energy saving using smart objects in NG-HN;<br>- Requirements for energy saving using smart objects in NG-HN;<br>- Functional model for energy saving using smart objects in NG-HN;<br>- Mechanisms for energy saving of constraint smart objects in NG-HN.<br>Basically, this draft Recommendation consider fixed smart environment like home/building and mobile smart environment like networked vehicle which support ubiquitous networking among objects. | ITU-T SG13 Q12<br>(2009 ~ 2012) | | | | | | | | 490. |
| ITU-T Y.2213, NGN service requirements and capabilities for network aspects of applications and services using tag-based identification | This Recommendation covers:<br>- description and scope of tag-based identification applications and services with some example scenarios;<br>- high-level service requirements of tag-based identification applications and services; and<br>- extended or new NGN capabilities based on the high-level service requirements.<br>Functional requirements and related NGN architecture extensions for support of the described capabilities are out of scope of this Recommendation. | ITU-T SG13 Q2<br>(2009 ~ 2012) | Recommendation | 2008-09-12 | | NID | | | | 491. |
| Y.DM-IoT-Reqts, | This Recommendation studies the requirements and capabilities of device management in IoT.<br>The scope of this Recommendation includes:<br>- the requirements of device management in IoT;<br>- the reference technical framework of device management in IoT;<br>- the capabilities of device management in IoT. | ITU-T SG13 Q2 | Draft Recommendation | | | IoT | | | 2013-02 | 492. |
| Y.IoT-app-models, IoT application support models | This Recommendation studies application support models of Internet of Things (IoT). The basis of the study of application support models of IoT includes IoT applications classification, application-oriented services, and application adaptable capabilities.<br>The Recommendation intends to show the applicability of application support models to the IoT requirements specified in [ITU-T Y.IoT-common-reqts].<br>The Recommendations also provides security considerations for IoT application support models. | ITU-T SG13 Q2 | Draft Recommendation | | | IoT | | | 2013-02 | 493. |
| Y.IoT-funct-framework | This Recommendation provides the functional framework and associated capabilities of Internet of Things (IoT), in particular components of the functional framework, their capabilities, and the relationships among these components.<br>The Recommendation also describes the relationships between | ITU-T SG13 Q2 | Draft Recommendation | | | IoT | | | 2013-02 | 494. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | the IoT requirements specified in [ITU-T Y.IoT-common-reqts] and the capabilities specified in this Recommendation.<br>Finally, the Recommendation provides security considerations for the IoT functional framework. | | | | | | | | | |
| Y.3001 (Future Networks: Objectives and Design Goals) | This Recommendation describes objectives and design goals for Future Networks. The scope of this Recommendation covers:<br>- Fundamental issues to which not enough attention was paid in designing current networks, and which are recommended to be the objective of Future Networks<br>- High-level capabilities and characteristics that are recommended to be supported by Future Networks<br>- Target timeframe for Future Networks<br>Ideas and research topics of Future Networks that are important and may be relevant to future ITU-T standardization are included in the Appendix of this Recommendation. | ITU-T SG13 Q21<br>(2009 ~ 2012) | Recommendation | 2011-05 | | FN | | | January 2009 | 495. |
| Y.3031, Identification framework in future networks | The scope of this Recommendation includes the following items:<br>- Specification of important objects requiring new identifiers in future networks (FNs);<br>- Analysis of the identifiers being used in existing networks and FNs projects;<br>Framework and generic requirements for identifiers in FNs. | ITU-T SG13 Q21<br>(2009 ~ 2012) | Recommendation | 2012-05-07 | | FN | | | January 2011 | 496. |
| Y.2069, Terms and definition for Internet of Things | This Recommendation specifies terms and definitions related to Internet of Things from an ITU-T perspective. | ITU-T SG13 Q25<br>(2009 ~ 2012) | Recommendation | 2012-07 | | | | | | 497. |
| ITU-T Y.2221, Requirements for support of Ubiquitous Sensor Network (USN) applications and services in NGN environment | The scope of this Recommendation includes:<br>- Description and general characteristics of USN and USN applications and services;<br>- Service requirements to support USN applications and services;<br>- Requirements of extended or new NGN capabilities based on the service requirements. | ITU-T SG13 Q3<br>(2009 ~ 2012) | Recommendation | 2010-01-13 | | USN | | | | 498. |
| Supplement NGN Security Planning and Operations Guidelines, Draft Supplement NGN Security Planning and Operations Guidelines | | ITU-T SG13 Q3<br>(2009 ~ 2012) | | | | | | | | 499. |
| Supplement to Y.2704 (formerly Y.NGN Certificate Management), Certificate Management | | ITU-T SG13 Q3<br>(2009 ~ 2012) | | | | | | | | 500. |
| Y.2060, Overview of Internet of Things | This Recommendation provides an overview of the Internet of Things (IoT) with the main objectives to introduce to this important area for future standardization.<br>More specifically, this Recommendation covers the following:<br>- IoT related terms and definitions;<br>- concept and scope of IoT;<br>- characteristics of IoT;<br>- high level requirements of IoT;<br>- IoT reference models.<br>IoT ecosystem and business models related information is provided in Appendix I. | ITU-T SG13 Q3<br>(2009 ~ 2012) | Recommendation | 2012-06 | | IoT | | | 2011-05 | 501. |
| Y.2061, Requirements for support of machine oriented communication applications in the NGN environment | This Recommendation covers extensions and additions to NGN capabilities [ITU-T Y.2201] and MOC device domain capabilities in order to support machine oriented communication (MOC) applications in the NGN environment. Although this Recommendation deals with support of MOC applications in the NGN environment, these capabilities can conceptually be | ITU-T SG13 Q3<br>(2009 ~ 2012) | Recommendation | | | MOC | | | | 502. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | applicable to other networks.<br>The scope of this Recommendation includes:<br>- Service overview, description of MOC ecosystem and key supporting features of MOC applications;<br>- Service requirements to support MOC applications;<br>- Requirements of extended or new NGN capabilities based on the MOC service requirements;<br>- Requirements of MOC device domain capabilities (for supporting MOC applications over NGN)<br>- Reference framework for MOC capabilities. | | | | | | | | | |
| Y.2222, Sensor Control Networks and related applications in Next Generation Network environment | This Recommendation provides a description and general characteristics of sensor control networks (SCN) applications. This Recommendation describes objectives and fundamental characteristics of SCNs and identifies capabilities required for the support of SCN applications in NGN. | ITU-T SG13 Q3<br>(2009 ~ 2012) | Recommendation | 2013-02 | | | | | | 503. |
| Y.EHM-Reqts, Requirements and Capabilities for E-health Monitoring Applications | This Recommendation describes requirements for supporting e-Health monitoring services, and specifies corresponding network capabilities.<br>The scope of this Recommendation includes:<br>- Classification of scenarios for E-Health monitoring services;<br>- Description of features of E-Health monitoring services from network perspective;<br>- Requirements for supporting E-Health monitoring services from network perspective;<br>- Capabilities for supporting E-Health monitoring services from network perspective. | ITU-T SG13 Q3<br>(2009 ~ 2012) | Draft Recommendation | | | | | | | 504. |
| Y.gw-IoT-arch, Functional architecture of gateway for IoT applications | This Recommendation studies the functional architecture of gateway for IoT application. The scope of this Recommendation includes:<br>- The functional architecture of gateway for IoT applications.<br>- The functional entities of gateway for IoT applications<br>- The internal/external interface of gateway for IoT applications | ITU-T SG13 Q3 | Draft Recommendation | | | IoT | | | 2013-02 | 505. |
| Y.gw-IoT-Reqts, Common requirements and capabilities of gateways for IoT applications | This Recommendation studies the common requirements and capabilities of gateway for IoT applications. The scope of this Recommendation includes:<br>- Relevant use cases of gateway for IoT applications.<br>- General features of gateway of IoT applications<br>- Common requirements of gateway for IoT applications<br>- Technical framework of gateway for IoT applications<br>- Common capabilities for gateway for IoT applications | ITU-T SG13 Q3<br>(2009 ~ 2012) | Draft Recommendation | 2013-02 | | IoT | | | 2012-05 | 506. |
| Y.IoT-common-reqts, Common requirements of Internet of Things | This Recommendation provides the common requirements of Internet of Things (IoT) based on abstracted use cases and cross-domain use cases of IoT. The abstracted use cases are derived from application use cases, or derived from the definition and characteristics of the IoT regarded as general abstract use cases. The cross-domain use cases refer to use cases that cover multiple application domains (e.g. e-Health, ITS, Smart Home, etc.).<br>This Recommendation builds on the overview of IoT [ITU-T Y.2060], developing the common requirements based on the IoT reference model.<br>The scope of this Recommendation includes:<br>- Abstracted use cases<br>- Cross-domain use cases<br>- Key areas of consideration from a requirements perspective<br>- Common requirements of IoT | ITU-T SG13 Q3<br>(2009 ~ 2012) | Draft Recommendation | 2013-12 | | IoT | | | 2012-05 | 507. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Appendix I provides typical application use cases. | | | | | | | | | |
| ITU-T Y.2016, Functional requirements and architecture of the NGN for applications and services using tag-based identification | This Recommendation describes functional requirements, functional architecture and functional entities in order to support the NGN service requirements and capabilities defined in [ITU-T Y.2213].<br>This Recommendation covers:<br>- Support of capabilities defined in [ITU-T Y.2213] from an architectural viewpoint;<br>- Functional requirements of the NGN architecture to support applications and services using tag-based identification;<br>- Functional architecture and entities extensions for applications and services using tag-based identification in NGN. | ITU-T SG13 Q5<br>(2009 ~ 2012) | Recommendation | 2009-08-22 | | NID | | | | 508. |
| ITU-T F.771, Service description and requirements for multimedia information access triggered by tag-based identification | This Recommendation specifies the service description and the requirements for multimedia information access triggered by tag-based identification. This service enables users to access multimedia information through users' electronic devices equipped with ID tag readers and communication functions. | ITU-T SG16 Q22<br>(2009 ~ 2012) | Recommendation | 2008-08-06 | | NID | | | | 509. |
| ITU-T H.621, Architecture of a system for multimedia information access triggered by tag-based identification | This Recommendation defines the following issues to cover multimedia information access services triggered by tag-based identification as defined in [ITU-T F.771]:<br>- a functional architecture reference model with descriptions of corresponding elements;<br>- interface protocols between communication elements; and<br>- a generic work flow to support multimedia information access triggered by tag-based identification.<br>Moreover, this Recommendation describes implementation examples with work flows. | ITU-T SG16 Q22<br>(2009 ~ 2012) | Recommendation | 2008-08-06 | | NID | | | | 510. |
| ITU-T H.642.3 \| ISO/IEC 29177, Information technology – Automatic identification and data capture technique – Identifier resolution protocol for multimedia information access triggered by tag-based identification | This Recommendation \| International Standard defines the identifier (ID) resolution protocol for multimedia information access triggered by tag-based identification which is described in ITU-T Recommendations F.771 and H.621. | ITU-T SG16 Q22 \| ISO/IEC JTC 1/SC 31/WG 6<br>(2009 ~ 2012) | Recommendation \| FDIS to ISO/CS (2012-01-17) | 2012-06 | | NID/<br>MIIM | | | 2008-11-05 | 511. |
| F.747.1, Capabilities of ubiquitous sensor network (USN) for supporting requirements of smart metering systems | The main purpose of this Recommendation is to identify capabilities of ubiquitous sensor network which supports requirements of smart metering services. The scope of this Recommendation covers the following:<br>- Overview of smart metering;<br>- Smart metering scenarios;<br>- Requirements of smart metering services;<br>USN capabilities for supporting requirements of smart metering services. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2012-06 | | USN | | | 2010-07 | 512. |
| F.747.2, Deployment guidelines for ubiquitous sensor network (USN) applications and services for mitigating the climate change | This Recommendation describes deployment guideline of Ubiquitous Sensor Network (USN) applications and services for mitigating the climate change. The scope of this Recommendation includes:<br>- Analysis of environmental impact by USN applications and services;<br>Deployment guideline of USN applications and services for mitigating the climate change. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2012-06 | | USN | | | 2009-10 | 513. |
| F.747.3, Requirements and functional model for ubiquitous network robot platform to support USN applications and services | This Recommendation covers the following:<br>- Overview of network robot platform in terms of USN applications and services;<br>- Use cases of USN applications and services for network robot platform;<br>USN service requirements for network robot platform. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2013-03 | | USN | | | 2010-03 | 514. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| F.OpenUSN, Requirements and reference architecture for open USN service framework | The objective of this Recommendation is to define an open USN service framework, and provide requirements, and reference architecture of open USN service framework. The use of standard interfaces of open USN service framework will ensure USN service reusability, portability across several USN services, as well as accessibility and interoperability by USN application providers and/or developers.<br>This Recommendation describes requirements and reference architecture for open USN service framework. The scope of this Recommendation includes:<br>- Concept of open USN service framework<br>- Requirements of open USN service framework<br>- Reference architecture of open USN service framework<br>Functional entities of open USN service framework | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | USN | | | 2011-11 | 515. |
| F.USN-ALI, Requirements and reference structure of automatic location identification capability for USN applications and services | Automatic Location Identification capability enables a device to discover its own location. Within USN scheme, ALI locates between the application and service layers. The ALI can be deployed with the network equipment, or independently integrated by end-node devices. It can be used in various networks such as hybrid mobile networks, internet, low power wireless network (smart gird), and other USN communication systems.<br>The scope of this recommendation includes:<br>- The specific scenario of ALI for USN;<br>- The requirements of ALI for USN;<br>The reference structure of ALI system within USN scheme. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | USN | | | 2011-11 | 516. |
| H.IoT-ID, Requirements and Common Characteristics of IoT Identifier for IoT Service | The objective of this Recommendation is to analyse identifiers in existing technologies and networks for IoT service, and describe the requirements of IoT identifier, common characteristics of IoT identifier, and the general architecture of IoT identifier.<br>This Recommendation describes the requirements and common characteristics of IoT identifier for IoT service. The scope of this Recommendation includes:<br>- Analysis of identifiers in existing technologies and networks<br>- Describe requirements of IoT identifier<br>- Describe common characteristics of IoT identifier<br>- Describe the general architecture of IoT identifier | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | IoT | | | 2012-05 | 517. |
| H.IoT-reqs, Common Service Requirements for Internet of Things (IoT) applications and services | This draft Recommendation defines the common services requirements for Internet of Things applications and services based on [ITU-T Y.IoT-overview].<br>This Recommendation covers the following from the service point of view:<br>- General overview of Internet of Things applications and services, and;<br>- Characteristics of Internet of Things applications and services, and;<br>- Common services requirements for Internet of Things applications and services<br>NOTE: This draft Recommendation mainly focuses on the view point of applications and services. Network layer aspect of Internet of Things is out of scope of this draft Recommendation. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | IoT | | | 2012-05 | 518. |
| H.USN-WQA, Requirements of water quality assessment services in USN | This Recommendation identifies USN requirements and scenarios of water quality assessment services. The scope covers the following:<br>- Overview of water quality assessment;<br>- Water quality assessment scenarios;<br>- Requirements of water quality assessment services;<br>- USN capabilities for supporting the requirements of water quality assessment services; | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | USN | | | 2012-05 | 519. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| H.WoT-SA, Web of Things service architecture | The objective of this Recommendation is to define the reference architecture of Web of things for its deployment. The scope of this Recommendation covers the followings:<br>- Overview of WoT Service Architecture;<br>- WoT accessibility;<br>- WoT findability;<br>- WoT sharing;<br>- WoT composition;<br>- WoT interface. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Draft Recommendation | 2013 | | | | | 2012-05 | 520. |
| ITU-T F.744, Service description and requirements for ubiquitous sensor network middleware | This Recommendation describes USN services and requirements for ubiquitous sensor network (USN) middleware. This Recommendation covers:<br>- description of the USN services;<br>- description of the USN middleware;<br>- use cases of USN services that use USN middleware;<br>- functional model of USN middleware;<br>- – requirements for USN middleware to support functions commonly required by USN services. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2009-12-14 | | USN | | | | 521. |
| ITU-T H.641, SNMP-based sensor network management framework | This Recommendation provides an SNMP-based sensor network management framework. The primary purpose of this Recommendation is to describe the framework of integrated sensor network management which can be used to manage heterogeneous sensor networks. The scope of this Recommendation includes:<br>- Overall architecture of framework<br>- Functional entities of framework<br>- Object identifier allocation for MIB<br>- Object identifier translation between SNMP and sensor network management protocol | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2012-02 | | USN | | | | 522. |
| ITU-T H.642.1, Identification scheme for multimedia information access triggered by tag-based identification – Part 1: Identification scheme” | This Recommendation defines an Identifier (ID) scheme for the multimedia information access triggered by tag-based identification. This ID scheme is mainly used in the multimedia information system architecture defined in ITU-T H.621. It also satisfies the requirements defined in ITU-T F.771.<br>This Recommendation does not define encoding rules to store the identifier value into data carriers such as barcode tags and RFID tags. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2012-06 | | NID | | | | 523. |
| ITU-T H.642.2, Identification scheme for multimedia information access triggered by tag-based identification – Part 2: Registration procedure | This Recommendation defines registration procedures of identification scheme defined by ITU-T Recommendation H.IDscheme. The identification scheme consists of High Level Code (HLC), Top Level Code (TLC), Class and elements such as Second Level Organization Code (SLOC), and Serial Code (SC). TLC is allocated by RA and then SLOC is allocated by the registrant of TLC which is called second level RA. The mechanism is meant for distributed RA hierarchy. | ITU-T SG16 Q25<br>(2009 ~ 2012) | Recommendation | 2012-07 | | NID | | | | 524. |
| F.VGP-REQ, Service and functional requirements of vehicle gateway platforms | This Recommendation provides the service description, application scenarios and requirements for Vehicle Gateway Platforms.<br>A series of Recommendations for Vehicle Gateway Platforms is currently opened in ITU- T SG 16. This Recommendation is part of that series and gives the service description, application scenarios and requirements. | ITU-T SG16 Q27 | Draft Recommendation | | | IoT | | | | 525. |
| G.SAM, Mechanisms for managing the situational awareness of drivers | N/A | ITU-T SG16 Q27 | Draft Recommendation | | | IoT | | | 2013-01 | 526. |
| G.V2A, Communications interface | N/A | ITU-T SG16 Q27 | Draft | | | IoT | | | 2013-01 | 527. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| between external applications and a Vehicle Gateway Platform | | | Recommendation | | | | | | | |
| H.VGP-FAM, Functional architecture model of vehicle gateway platforms | N/A | ITU-T SG16 Q27 | Draft Recommendation | | | IoT | | | | 528. |
| HSTP.EHMSI, Multimedia Service and Interfaces for e-health | This Technical Paper describes requirements and use cases of multimedia services for e-health and their interfaces. | ITU-T SG16 Q28<br>(2009 ~ 2012) | Draft Technical Paper | | | e-Health Application | | | 2009 | 529. |
| ITU-T X.1275, Guidelines on protection of personally identifiable information in the application of RFID technology | This Recommendation provides guidance to radio frequency identification (RFID) users and vendors (including RFID service providers and manufacturers) in protecting personally identifiable information for the privacy of individuals in the context of RFID technology.<br>These guidelines can be applied to cases wherein the RFID system may be used to invade individual privacy; e.g., personally identifiable information is recorded in an RFID tag and subsequently collected, or the object information collected by means of RFID is linked to personally identifiable information. However, it does not apply to such cases where the object information is collected and used without any risk of disclosure of personally identifiable information and invasion of privacy.<br>These guidelines seek to protect personally identifiable information for the privacy of individuals potentially affected by an RFID system and to promote a safe environment for RFID use. These guidelines are intended to provide the basic rules for the RFID service provider and guidance to the RFID service provider, manufacturers and user with regard to privacy in RFID and are subject to local and national laws. | ITU-T SG17 Q10<br>(2009 ~ 2012) | Recommendation | 2010-12-17 | | RFID | | | | 530. |
| ITU-T X.660 \| ISO/IEC 9834-1, Information technology – Procedures for the operation of Object Identifier Registration Authorities: General procedures and top arcs of the International Object Identifier tree | This Recommendation \| International Standard:<br>- specifies a tree structure for allocations made by a hierarchical structure of Registration Authorities, called the international OID tree, which supports the ASN.1 OBJECT IDENTIFIER type and the ASN.1 OID IRI type (see Rec. ITU-T X.680 \| ISO/IEC 8824-1);<br>- registers top-level arcs of the international object identifier tree;<br>- specifies procedures which are generally applicable to registration at any level of the international OID tree;<br>- provides guidelines for the establishment and operation of International Registration Authorities for use, when needed, by other ITU-T Recommendations and/or International Standards;<br>- provides guidelines for additional ITU-T Recommendations and/or International Standards which choose to reference the procedures in this Recommendation \| International Standard;<br>- provides a recommended fee structure for lower-level Registration Authorities. | ITU-T SG17 Q10 \| ISO/IEC JTC 1/SC 6/WG 9<br>(2009 ~ 2012) | Recommendation \| International Standard | 2011-07-29 | | General | | | | 531. |
| ITU-T X.668 \| ISO/IEC 9834-9, Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification | This Recommendation \| International Standard specifies the procedures for operating the Registration Authority for object identifiers under the arc {joint-iso-itu-t(2) tag-based(27)}, that supports tag-based applications and services. | ITU-T SG17 Q12 \| ISO/IEC JTC 1 SC 6/WG 9<br>(2009 ~ 2012) | Recommendation \| International Standard | 2008-05-29 | | NID | | | | 532. |
| ITU-T X.672 \| ISO/IEC 29168-1, Information technology – Open systems interconnection – Object identifier resolution system (ORS) | This Recommendation \| International Standard specifies the OID resolution system, including the overall architecture and a DNS-based resolution mechanism.<br>It specifies the means for inserting any application-defined | ITU-T SG17 Q12 \| ISO/IEC JTC 1/SC 6<br>(2009 ~ 2012) | Recommendation \| International Standard | 2010-08-29 \|<br>2011-09-12 | | NID | | | | 533. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | information associated with an OID node into the DNS and the means of retrieval of that information using the ORS.<br>It does not restrict the number of applications it can support.<br>It specifies the required operation of an ORS client, including the mapping of an OID-IRI value by the ORS client into a DNS name to produce a DNS query for the specified application information and the processing of any returned information. The ORS has no role in the allocation or registration of OID nodes.<br>The required behavior of an ORS client is specified, but the interfaces to it are specified only in terms of the semantics of the interaction. A bit-level application program interface is platform and software dependent, and is not in the scope of this Recommendation \| International Standard.<br>It does not include a tutorial or complete specification on the management of DNS zone files (for that, see IETF RFC 1035 and IETF RFC 3403); it specifies (only) the DNS resource records that need to be inserted in the zone files in order to support ORS access to the information associated with an OID node.<br>This Recommendation \| International Standard specifies required DNS zone file resource records, and prohibits the use of other resource records of a similar form but with different semantics (in DNS zone files in the .oid-res.org domain). It does not otherwise restrict the general use of DNS zone files. | | | | | | | | | |
| ITU-T X.520 AMD 3, Information technology – Open Systems Interconnection – The Directory: Selected attribute types | X.520 defines attribute types for Directory Services. The amendment 3 to X.520 will extend it to support identification management in Directory Services | ITU-T SG17 Q2<br>(2009 ~ 2012) | Draft Recommendation | | | NID | | | | 534. |
| ITU-T X.1171, Threats and requirements for protection of personally identifiable information in applications using tag-based identification | The scope of this Recommendation covers the following objectives including threats and requirements for protection of personally identifiable information (PII) in applications using tag based identification as described below:<br>- To describe PII threats in a business-to-customer (B2C)-based environment of applications using tag based identification;<br>- To identify requirements for PII protection in a B2C-based environment of applications using tag based identification. | ITU-T SG17 Q6<br>(2009 ~ 2012) | Recommendation | 2009-02-20 | | NID | | | | 535. |
| ITU-T X.1311, Security requirements and framework of ubiquitous networking | This Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this Recommendation categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the security model of the Ubiquitous Sensor Network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are presented. | ITU-T SG17 Q6<br>(2009 ~ 2012) | Recommendation | 2011-02-13 | | | | | | 536. |
| ITU-T X.1312, Ubiquitous sensor networks (USN) middleware security guidelines | This Recommendation provides guidelines for USN middleware security and also covers the following:<br>- overview of USN middleware security;<br>- the functional model of USN middleware;<br>- security threats on USN middleware;<br>- security requirements for USN middleware;<br>- guidelines for USN middleware security. | ITU-T SG17 Q6<br>(2009 ~ 2012) | Recommendation | 2011-02-13 | | USN | | | | 537. |
| ITU-T X.1313, Security requirements for wireless sensor network routing | This Recommendation provides security requirements for wireless sensor network routing and also covers as follow;<br>- Overview of USN architecture<br>- General network topologies and routing protocols for WSN | ITU-T SG17 Q6<br>(2009 ~ 2012) | Recommendation | 2012-10-14 | | USN | | | | 538. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | - Security threats of WSN routing<br>- Security requirements for WSN routing | | | | | | | | | |
| ITU-T X.1311 \| ISO/IC 29180, Security framework for ubiquitous sensor network | This draft Recommendation describes the security threats to and security requirements of the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes the security technologies according to the security functions that satisfy said security requirements and by the place to which the security technologies are applied in the security model of USN. Finally, the security requirements and security technologies for USN are presented. | ITU-T SG17 Q6 \| ISO/IEC JTC 1/SC 6<br>(2009 ~ 2012) | Recommendation \| International Standard | 2011-02-13 | | USN | | | | 539. |
| ITU-T E.101, Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations | This Recommendation provides terms and definitions for use in the field of identifiers (e.g., names, numbers, addresses and other identifiers (IDs)) for public telecommunication services and networks. | ITU-T SG2 Q1<br>(2009 ~ 2012) | Recommendation | 2009-11-24 | | General | | | | 540. |
| J.295, Functional Requirements for Advanced Cable Set-Top Box | This Recommendation defines functional requirements for the advanced cable set-top box to enable cable television operators to provide advanced services to their subscribers. The advanced cable set-top box is intended to apply to cable television operators' service provision, where many types of access network technologies have been recently introduced, e.g. HFC, PON, RFoG. Cable television operators have a capability of providing both broadcasting and interactivity over its own network originally intended to distribute broadcasting television programs, and the advanced cable set-top box is a core device for the delivery of attractive advanced services. | ITU-T SG9 Q5<br>(2009 ~ 2012) | Recommendation | 2012-01-30 | | M2M | | | | 541. |
| ITU-T J.360,<br>IPCablecom2 architecture framework | The initial release of IPCablecom [ITU-T J.160-J.178] provides for telephony. IPCablecom multimedia [ITU-T J.179] creates a bridge that allows for the expansion of IPCablecom into a full range of multimedia services. This Recommendation provides the architectural framework, technical background and project organization for the second release of the IPCablecom family of Recommendations providing for the extension into the multimedia domain. | ITU-T SG9 Q8<br>(2009 ~ 2012) | Recommendation | 2008-06-13 | | USN | | | | 542. |
| ITU-T J.366.0,<br>IPCablecom2 IP Multimedia Subsystem (IMS): Delta Recommendations overview | This Recommendation is an overview document introducing the family of IMS delta Recommendations that adapt the wireless industries IMS initiative to the needs of the cable industry. A delta Recommendation references another document and then shows only the changes necessary to adapt the other document to the current needs. It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0. | ITU-T SG9 Q8<br>(2009 ~ 2012) | Recommendation | 2006-11-29 | | M2M | | | | 543. |
| ITU-T J.700, IPTV service requirements and framework for secondary distribution | This Recommendation describes the service requirements and functional framework architecture for<br>support of IPTV services to provide enhanced broadcasting, where broadcasting programs are<br>delivered over existing cable-based secondary distribution networks composed of HFC or FTTx<br>with some enhancements by applications and/or services provided over IP-enabled networks. It<br>addresses the service requirements, use cases and functional | ITU-T SG9 Q8<br>(2009 ~ 2012) | Recommendation | 2009-12-14 | | USN | | | | 544. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | components required to support these<br>requirements. Where possible, this Recommendation utilizes the material already developed, or<br>under development, in ITU-T Recommendations related to video service delivery over secondary<br>networks. | | | | | | | | | |
| ITU-T J.lasdp-req, Functional and Application Programming Interface Requirements for Local Application and Service Delivery Platform for Cable Home Networks | This draft new Recommendation defines functional requirements for the local application and service delivery platform (LASDP) in the cable home network environment. The local application service delivery platform is a conceptual platform which resides within the home network to provide programming interfaces and functionalities to enable the cable service provider and third party entities to deliver advanced and innovative applications and services to cable subscribers in the home network. The LASDP can communicate and interwork with network service delivery platforms to create more value for customers and the service provider. | ITU-T SG9 Q9<br>(2009 ~ 2012) | Draft Recommendation | | | USN | | | | 545. |
| Data Distribution Service for Real-Time Systems Version 1.2, OMG Available specification formal/07-01-01 | OMG's Data Distribution Service (DDS) standard is a protocol for the Industrial Internet. It enables network interoperability for connected machines, enterprise systems and mobile devices. It provides scalability, performance, and Quality of Service required to support IoT and Industrial Internet Internet applications. DDS can be deployed in platforms ranging from low-footprint devices to the Cloud and supports efficient bandwidth usage as well as agile orchestration of system components. It provides a global data space for analytics and enables flexible M2M real-time system integration. | Object Management Group (OMG) | V1.0 adopted<br>V1.1 adopted<br>V1.2 adopted | December 2004<br>December 2005<br>January 2007 | Performance, Scalability, Real-time Data sharing, Qualities of Service (22+ user controllable QoS defined as part of the standard) | Communications and Networking | Data Distribution Service for Device to Device (D2D) , or Machine to Machine (M2M), or Device to Cloud real-time data sharing | DDS is already deployed in many IoT application domains, including Industrial Control, Healthcare, Aerospace, Telecommunications, Defense, Energy, Smart Cities and Transportation | | 546. |
| City Geography Markup Language (CityGML) Encoding Standard<br>OGC Document<br>08-007r1 | This document is an OpenGIS® Encoding Standard for the representation, storage and exchange of virtual 3D city and landscape models. CityGML is implemented as an application schema of the Geography Markup Language version 3.1.1 (GML3). CityGML models both complex and georeferenced 3D vector data along with the semantics associated with the data. In contrast to other 3D vector formats, CityGML is based on a rich, general purpose information model in addition to geometry and appearance information. For specific domain areas, CityGML also provides an extension mechanism to enrich the data with identifiable features under preservation of semantic interoperability.<br>http://www.opengeospatial.org/standards/citygml | OGC | Implementation Standard | 2008-08-20 | | Geospatial Information | | | | 547. |
| Geography Markup Language (GML) Encoding Standard<br>Version 3.2.1<br>Document 07-036<br>Also published as ISO 19136 | GML is an XML grammar for expressing geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet. As with most XML based grammars, there are two parts to the grammar – the schema that describes the document and the instance document that contains the actual data. A GML document is described using a GML Schema. This allows users and developers to describe generic geographic data sets that contain points, lines and polygons. However, the developers of GML envision communities working to define community-specific application schemas that are specialized extensions of GML. Using application schemas, users can refer to roads, highways, and bridges instead of points, lines and polygons.<br>http://www.opengeospatial.org/standards/gml | OGC | Implementation Standard | 2007-12-28 | | Geospatial Information | | | | 548. |
| KML<br>OGC Document 07-147r2 | KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the | OGC | Implementation Standard | 2008-04-14 | | Geospatial Information | | | | 549. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | sense of where to go and where to look.<br>http://www.opengeospatial.org/standards/kml | | | | | | | | | |
| Observations and Measurements - XML Implementation<br>OGC Document 10-025r1 | This standard specifies an XML implementation for the OGC and ISO Observations and Measurements (O&M) conceptual model (OGC Observations and Measurements v2.0 also published as ISO/DIS 19156), including a schema for Sampling Features. This encoding is an essential dependency for the OGC Sensor Observation Service (SOS) Interface Standard. More specifically, this standard defines XML schemas for observations, and for features involved in sampling when making observations. These provide document models for the exchange of information describing observation acts and their results, both within and between different scientific and technical communities.<br>http://www.opengeospatial.org/standards/om | OGC | Implementation Standard | 2011-03-22 | | SWE | | | | 550. |
| OGC Abstract Specification, Topic 2: Spatial Referencing by Coordinates<br>Version 4.0,<br>OGC Document 08-015r2<br>Also published as ISO 19111:2007 | This Abstract Specification defines the conceptual schema for the description of spatial referencing by coordinates, optionally extended to spatio-temporal referencing. It describes the minimum data required to define one-, two- and three-dimensional spatial coordinate reference systems with an extension to merged spatial-temporal reference systems. It allows additional descriptive information to be provided. It also describes the information required to change coordinates from one coordinate reference system to another.<br>http://www.opengeospatial.org/standards/as | OGC | Abstract Specification. | 2010-04-27 | | Geospatial Information | | | | 551. |
| OGC Abstract Specification, Topic 20: Observations and Measurements<br>Version 2.0<br>Document 10-004r3<br>Also published as ISO 19156:2010 | This International Standard defines a conceptual schema for observations, and for features involved in sampling when making observations. These provide models for the exchange of information describing observation acts and their results, both within and between different scientific and technical communities.<br>http://www.opengeospatial.org/standards/as | OGC | Approved Abstract Specification | 2010-11-10 | | SWE | | | | 552. |
| OGC Filter Encoding Encoding Standard<br>Version 2.0<br>Document 09-026r1<br>Also published as ISO 19143 | This International Standard describes an XML and KVP encoding of a system neutral syntax for expressing projections, selection and sorting clauses collectively called a query expression. These components are modular and intended to be used together or individually by other standards which reference this International Standard.<br>http://www.opengeospatial.org/standards/filter | OGC | Implementation Standard | 2010-11-22 | | Geospatial Information | | | | 553. |
| Open GeoSMS | The OpenGIS Open GeoSMS standard defines an encoding for location enabling the Short Message Service. SMS is a communication service for phone, web or mobile communication systems, that provides exchange of short text messages between fixed line or mobile phone devices. The OGC Open GeoSMS encoding standard facilitates communication of location content using the extended SMS devices or applications for achieving interoperable communications while still maintaining human readability of the content.<br>http://www.opengeospatial.org/projects/groups/opengeosmsswg | OGC | Standards Working Group | 2011 | | LBS | | | 2010/01/05 | 554. |
| OpenGIS Location Service (OpenLS) Implementation Specification: Core Services<br>OGC Document 07-074 | The five Core OpenLS services are defined in a single document:<br>1. Directory Service. Provides access to an online directory enabling an application to find the location of a specific or nearest place, product, or service.<br>2. Gateway Service. Retrieves the position of a known Mobile Terminal from the network. This interface is modelled after the | OGC | Implementation Standard | 9 September 2008 | | LBS | | | | 555. |

|  |  |  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|
|  | LIF/OMA Mobile Location Protocol (MLP), Standard Location Immediate Service, specified in Open Mobile Alliance MLP.<br>3. Location Utility Service (Geocoder/Reverse Geocoder) Geocoding converts a text description of a location, such as a place name, street address, or postal code to a position structured as Point geometry. Reverse Geocoding converts a position into a feature (Address with Point), where the address may be a street address, intersection address, place name, or postal code.<br>4. Presentation Service. Creates maps and other graphic depictions of selected geospatial data, with a set of ADTs as logical layers.<br>5. Route Service. Determines travel routes and navigation information between two or more points<br>http://www.opengeospatial.org/standards/ols |  |  |  |  |  |  |  |  |  |
| OpenLS Tracking Service Interface Standard<br>OGC Document 06-024r4 | The OpenLS Tracking Service Interface Standard supports a very simple functionality allowing a collection of movable objects to be tracked as they move and change orientation.<br>http://www.opengeospatial.org/standards/ols | OGC | Implementation Standard | 2008 |  | LBS |  |  |  | 556. |
| OpenLS: Part 6-Navigation Service Implementation Standard<br>OGC Document 08-028r7 | The OpenLS: Part 6-Navigation Service Implementation Standard is an enhanced version of the Route Service, that determines travel routes and navigation information between two or more points.<br>http://www.opengeospatial.org/standards/ols | OGC | Implementation Standard | 2008 |  | LBS |  |  |  | 557. |
| Sensor Model Language (SensorML)<br>OGC Document 07-000 | The Sensor Model Language Encoding Standard (SensorML) specifies models and XML encoding that provide a framework within which the geometric, dynamic, and observational characteristics of sensors and sensor systems can be defined. There are many different sensor types, from simple visual thermometers to complex electron microscopes and earth observing satellites. These can all be supported through the definition of atomic process models and process chains.<br>http://www.opengeospatial.org/standards/sensorml | OGC | Implementation Standard | 2007-07-17 |  | SWE |  |  |  | 558. |
| Sensor Observation Service<br>OGD Document 06-009r6 | The Sensor Observation Service Interface Standard (SOS) provides an API for managing deployed sensors and retrieving sensor data and specifically “observation” data. Whether from in-situ sensors (e.g., water monitoring) or dynamic sensors (e.g., satellite imaging), measurements made from sensor systems contribute most of the geospatial data by volume used in geospatial systems today.<br>http://www.opengeospatial.org/standards/sos | OGC | Implementation Standard | 2007-10-26 |  | SWE |  |  |  | 559. |
| Sensor Planning Service<br>OGC Document 09-000 | The Sensor Planning Service Interface Standard (SPS) defines interfaces for queries that provide information about the capabilities of a sensor and how to task the sensor. The standard is designed to support queries that have the following purposes: to determine the feasibility of a sensor planning request; to submit and reserve/commit such a request; to inquire about the status of such a request; to update or cancel such a request; and to request information about other OGC Web services that provide access to the data collected by the requested task.<br>http://www.opengeospatial.org/standards/sps | OGC | Implementation Standard | 2011-03-28 |  | SWE |  |  |  | 560. |
| Sensor Web Enablement Architecture<br>OGC Document | This document describes the architecture implemented by OGC’s Sensor Web Enablement (SWE). In much the same way that HTML and HTTP standards enabled the exchange of any type of information on the Web, the SWE initiative is focused on | OGC | Best Practice | 2008-08-20 |  | SWE |  |  |  | 561. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 06-021r4 | developing standards to enable the discovery of sensors and corresponding observations, exchange, and processing of sensor observations, as well as the tasking of sensors and sensor systems.<br>http://portal.opengeospatial.org/files/?artifact_id=29405 | | | | | | | | | |
| Web Feature Service<br>OGC Document 09-025r1<br>also ISO 19142 | This International Standard specifies the behaviour of a service that provides transactions on and access to geographic features in a manner independent of the underlying data store. It specifies discovery operations, query operations, locking operations, transaction operations and operations to manage stored parameterized query expressions.<br>http://www.opengeospatial.org/standards/wfs | OGC | Implementation Standard | 2010-11-02 | | Geospatial Information | | | | 562. |
| Web Map Service (WMS)<br>OGC Document<br>06-042<br>Also published as ISO 19128 | The Web Map Service Interface Standard provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images (returned as JPEG, PNG, etc) that can be displayed in a browser application.<br>http://www.opengeospatial.org/standards/wms | OGC | Implementation Standard | 2006-03-15 | | Geospatial Information | | | | 563. |
| OMA Global Permissions Management | The GPM enabler consists of the Permission Checking and Management component, which provides the following main functions:<br>- The Permissions Checking function which processes Permissions Rules, and is exposed by a derivative of the PEM-1 interface.<br>- The Permissions Rules management function for creating, reading, deleting, modifying of Permissions Rules, which is exposed by a derivative of the PEM-2 interface.<br>- Consent interaction function, which uses the Interfaces to other resources to asks Ask Targets for consent on Permissions Checking decisions (e.g. send Ask Request to Ask Target). This may be performed during processing of Permissions Rules. | OMA | Candidate Enabler | 2009-07-10 | | Identity management | | | | 564. |
| OMA Identity Management Framework Requirements | The intention of this Requirements Document is to tie together all existing efforts relating to Identity within the OMA in order to create a single Identity Management (IdM) enabler to be used by all OMA enablers. This document sets requirements for all technical working groups of OMA, and all Identity Management related functions should be satisfied according to the resulting enabler. | OMA | Candidate Enabler | 2005-02-02 | | Identity management | | | | 565. |
| OMA Web Services Network Identity | The 'OMA Web Services Enabler (OWSER): Network Identity Specifications' provides the specifications of the components needed to provide aspects of the Network Identity related capabilities of the OWSER. | OMA | Approved Enabler | 2006-03-28 | | Identity management | | | | 566. |
| The Real-Time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification Version 2.1, OMG Document Number: formal/2009-01-05 | | OMG | V2.0 adopted<br>V2.1 adopted | April 2008<br>January 2009 | Interoperability | Communications and Networking | Data Distribution Service for Device to Device (D2D) , or Machine to Machine (M2M), or Device to Cloud real-time data sharing | DDS is already deployed in many IoT application domains, including Industrial Control, Healthcare, Aerospace, Telecommunications, Defense, Energy, Smart Cities and Transportation | | 567. |
| IEC 61334-4-61, Distribution automation using distribution line carrier systems - Part 4-61: Data communication protocols - Network layer - Connectionless protocol | Covers the services required by the data communication protocol (DCP) network layer (N) sublayer entity at the logical interfaces with the N user layer and the LLC sublayer, using the connectionless N procedures. | TC/SC 57 | | | | network level | | | | 568. |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| IEC 62457, Multimedia home networks - Home network communication protocol over IP for multimedia household appliances | specifies the requirements for the interface between the Home Network Lower Layer for a country's home network of standalone-type household appliances and the TCP/IP Layer for cases where it is intended to introduce a TCP/IP Layer to each of the nodes comprising such home network of standalone-type household appliances. The specified interface in the Home Network Lower Layer consists of 2 portions, the TCP/IP Interface and the lower medium-specific Interface. Figure 3 shows the composition of the Home Network Layer and the standardized portions. In Annex C, this standard specifies the requirements for the lower medium-specific Interface One of these layers shall be IEEE 802.15.1, short-distance radio standard additional layers can be added in the future | TS/SC 100 | | | | network level | | | | 569. |
| ZigBee Document 053474r20: ZigBee Specification | The ZigBee Specification describes the infrastructure and services available to applications operating on the ZigBee platform | ZigBee Alliance | Accepted | | | network level | ZigBee IP | | | 570. |
| ZigBee Document 094945r00ZB: ZigBee RF4CE Specification Version 1.01 | The ZigBee RF4CE specification describes the protocol infrastructure and services available to applications operating on the ZigBee RF4CE platform | ZigBee Alliance | Accepted | | | network level | ZigBee IP | | | 571. |
| ZigBee Document 095023r34: ZigBee IP Specification | The ZigBee IP Specification describes the infrastructure and services available to applications operating on the ZigBee IP platform | ZigBee Alliance | Accepted | | | network level | ZigBee IP | | | 572. |
| | | | | | | | | | | 573. |