Document No: IFEG: 01
Version: 1.0
May 2012

Technical Standards for

Interoperability Framework for E-Governance in India

Government of India
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

Metadata of Document **IFEG: Technical Standards**

S. No.	Data elements	Values
1.	**Title**	Technical Standards for Interoperability Framework for E-Governance (IFEG) in India
2.	**Title Alternative**	IFEG: Technical Standards
3.	**Document Identifier**	IFEG: 01
4.	**Document Version, month, year of release**	Version: 1.0 May, 2012
5.	**Present Status**	Approved and notified
6.	**Publisher**	Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT), Government of India (GoI)
7.	**Date of Publishing**	May 10, 2012
8.	**Type of Standard Document**	Technical Specification
9.	**Enforcement Category**	Mandatory
10.	**Creator**	Expert Committee for Mapping Open Standards Principles to Technical Standards of IFEG under the Chairmanship of Prof. G. Sivakumar, Department of Computer Science & Engineering, IIT-B, Mumbai
11.	**Contributor**	• DeitY • NIC
12.	**Brief Description**	IFEG is essential to enable e-Governance Applications to inter-operate. For this purpose, technical standards need to be identified in Interoperability Areas within various Domains of e-Governance. This document focuses on the Interoperability Areas prioritised by DeitY, in view of the interoperability requirements in e-Governance systems. Further, in each of the Interoperability Area, technical Standards have been identified, on the basis of the 'Policy on Open Standards', their maturity and industry preparedness for their

S. No.	Data elements	Values
		adoption.
13.	**Target Audience**	-Project Teams of e-Governance applications in all Departments at Central / State Government level -Contractual Policy framing agencies for development of e-Governance Applications -All integrators / service providers for Indian e-Governance Applications
14.	**Owner of approved standard**	DietY, MCIT, New Delhi
15.	**Subject**	Interoperability Framework for e-Governance
16.	**Subject. Category**	Domain-wise List of Technical Standards
17.	**Coverage. Spatial**	INDIA
18.	**Format**	PDF
19.	**Language**	English
20.	**Copyrights**	DietY, MCIT, New Delhi
21.	**Source**	Different resources, as indicated in the document
22.	**Relation**	This would be referred in IFEG Main Document, which is in the initial draft stage, and being created by the same Expert Committee.

Table of Contents

Technical Standards for

Interoperability Framework for E-Governance in India

1. BACKGROUND

Providing integrated citizen centric services at different levels of Central, State and grass root level Governance bodies is key objective of e-Governance initiatives. Current e-Governance solutions are usually based on different technology platforms, and most of them work in silos. For the purpose of Integrated Services Delivery, the data from various applications distributed logically as well as physically needs to be seamlessly exchanged/integrated in a secure way by following Open Standards for data interchange / exchange and archival. An Interoperability Framework for e-Governance is essential to support flow of information, through which two or more e-Governance applications can inter-operate. Open standards are also important to ensure long-term access and retrieval of important data, preventing vendor and technology lock-in. Considering such factors, Government of India (GoI) has decided to use Open Standards. “Policy on Open Standards for e-Governance ” (Version 1.0) (hereinafter referred to as 'Policy') was announced by GoI in November 2010 to provide a framework for selection of technical standards in identified Interoperability Areas.

Interoperability Framework for E-Governance (IFEG) in India addresses three aspects of Interoperability viz. Organizational Interoperability, Semantic Interoperability and Technical Interoperability. The present document addresses, Technical Interoperability requirements. It identifies domains for interoperability and each domain is further sub-divided into Interoperability Areas (hereinafter referred to as “Areas”), for which Technical Standards need to be identified as per Policy.

1.1 Scope

This document describes technical standards to be adopted for e-Governance application in the areas covered under IFEG, as per the Policy. Since technical standards are globally evolving, this document will be periodically reviewed and updated by considering the reasons like new Areas/Domains, standards, versions, etc.

This document should be read in conjunction with the Policy and an Enforcement Process Guideline document (to be prepared by GoI) which outlines when and how to use the Technical Standards in e-Governance applications.

1.2 Objective/Purpose

Refer to *section 1. Objective* of the Policy.

1.3 Applicability

Refer *section 3.Applicability* of the Policy.

1.4 Description

This section describes how this document is organised.

Section 1 provides the background information.
Section 2 describes the target audience for this document.
Section 3 describes type of document and enforcement category.

Section 4 describes definitions of terms and acronyms used in this document.
Section 5 describes the list of Technical Standards along with additional information about them.

2. TARGET AUDIENCE

The Technical Standards listed in this document shall be used in all e-Governance applications by

- Project Teams of e-Governance applications in all Departments at Central / State Government level
- Contractual Policy framing agencies for e-Governance Applications
- All integrators / service providers of Indian e-Governance Applications

3. TYPE OF DOCUMENT

Type of Document	:	**Technical Standards**
Enforcement Category	:	**Mandatory**

4. DEFINITIONS AND ACRONYMS

Refer Annexure-I

5. LIST OF TECHNICAL STANDARDS FOR E-GOVERNANCE

In IFEG , the 'Areas' for e-Governance applications have been categorized under 7 broad Domains viz.

Presentation and Archival

Process

Data Integration

Meta-data

Data Interchange

Network Access and Application

Security.

The Technical Standards are tabulated for each Area within a Domain. The description of columns of the tables under '5.1 Domain-wise List of Technical Standards' section is given below:

Interoperability Area	Name of the interoperability area in a Domain, which serves a specific purpose within the domain.		
Standard/Specification	Name of the standard/specification with its version number with hyper-link to the respective sites, if any.		
Standards Body	Name of the Standards Body which published the standard/specification.		
Status of Standard as per "Policy"	This can have any of the following values		
	O	Open Standard: Which meets the Mandatory Characteristics of the Policy	
	I	Interim Standard: As per section 4.3 & 4.4 of Policy	
	A	Additional Open Standard: As per section 5 of Policy	
Maturity level	This can have any of the following values		
	MC	Matured and Current Matured: As per definition of "Maturity" in the Policy	
	MD	Matured but Declining	
	E	Evolving: A standard, which meets the maximal functional requirements and progressing towards Maturity	
*Enforcement Category**	This can have any of the following values		
	M	Mandatory /MUST	Matured & Current Standards (To be reviewed periodically)
	MW	Mandatory – Watch-list	Interim Standard / Open, Matured & Declining Standard / Open & Evolving Standard. (It is also Mandatory/Must, but it will be reviewed more frequently to explore *if a better candidate standard has become available*)
	O	Optional	Additional Open Standard (Either of the Recommended / Additional standard to be mandatory with preference to Recommended standard)
Other version(s), if any, which can also be considered through a Version Management Mechanism.	Each version of a standard has its own life cycle period (evolve, effective, retire and removal). In this document, the recommended version of the standard is the one which has broader usage and also well supported. The 'other version' (new or evolving or old version) of the same standard can also be considered through a version management mechanism in certain situations as explained in the paragraph "**Version Management Mechanism**" below this table. It is also to be noted that multiple versions of a standard do not mean "multiple standards" or "additional standard" for that Area.		
For additional information, refer the Table No. under this column	For additional information, refer the Table Numbers indicated in this column. These tables are available under section "5.2 Additional Information on Technical Standards"		

**For every Area where no Additional Standard has been recommended, the single identified standard is the one that MUST be used; All listed standards in this document need to be reviewed periodically. However, the standards which are categorized as Evolving (E) or Matured but Declining (MD) or Interim (I) need to be reviewed more frequently to explore if a better candidate has become available; Enforcement Category for such standards has been recorded as Mandatory - Watch-list (MW). Here Watch list is only to alert the users that the mandated standard for this Area will be reviewed more frequently. Other standards have been marked as Mandatory/MUST (M).*

Version Management Mechanism

In this document, most stable versions of the technical standards are mandated for adoption. However, in few cases, other version(s), if any, are also included for consideration on case to case basis through a 'Version Management Mechanism'.

The purpose of version management mechanism is to ensure that e-Governance systems do not get precluded from leveraging the added features of the evolving / new version, due to guideline by GoI for adoption of stable version of a standard, even if it is lower version.

Other version(s) of the same standard, if any may be considered for adoption due to any specific constraints / reasons like :

- the recommended version does not have the additional features of new version, essentially required for development of e-Governance applications / the new version overcomes the limitations of the previous version
- resource constraints preclude wide deployment or adoption of the recommended version; whereas other version may not have such constraints
- the project development life cycle is considerably big and by the time the application would be rolled out the new version would have been stabilized.

In such cases, the versions listed in the 'Other Versions' column may be considered by following the Version Management Mechanism, which would be in place to issue updates and guidelines from time to time on controlling the versions in use at different stages (RFP, Implementation, Upgrade, Migration, etc.) of any e-Governance project. The Mechanism will also guide stake-holders of e-Governance applications to choose the appropriate version (from the “recommended version” and “other versions”) depending on the Area under considerations. It will be done by involving the domain-experts on **case to case basis** as no general guideline can be applied across all Areas or all applications..

5.1 Domain-wise List of Technical Standards

5.1.1 Presentation And Archival Domain

The Presentation part of this Domain provides the interface to the user for accessing information. The Archival part of this Domain provides interface for storing and retrieving the data.

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy"	Maturity Level	Enforcement Category	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
				O-Open	MC-Matured & Current	M-Mandatory		
				I-Interim	MD-Matured but Declining	MW-Mandatory - Watch-list		
				A-Additional	E-Evolving			
1	Document type for Simple Hypertext Web Content	ISO/IEC 15445:2000 (HTML 4.01)	ISO/IEC W3C	O	MC	M	HTML 5	5.2.6
2	Document type for Complex, Strict Hypertext Web Content (XML or non-XML)	XHTML v1.1	W3C	O	MC	M	HTML5	5.2.31
3	Style Sheets (to define Look & Feel of Web-page)	CSS 2	W3C	O	MC	M	CSS3	5.2.1
4	Extensible Style Sheets (to transform format and addressing parts of documents)	XSL 1.1	W3C	O	MC	M	--	5.2.38
5	Document Type for Editable documents (with formatting)	ISO/IEC 26300:2006 (ODF - OpenDocument v1.0)	ISO/IEC OASIS	O	MC	M	ODF – OpenDocument 1.2	5.2.16
6	Document Type for Presentation	ISO/IEC 26300:2006 (ODF - OpenDocument v1.0)	ISO/IEC OASIS	O	MC	M	ODF – OpenDocument 1.2	5.2.16
7	Document Type for Spreadsheet	ISO/IEC 26300:2006 (ODF - OpenDocument v1.0)	ISO/IEC OASIS	O	MC	M	ODF – OpenDocument 1.2	5.2.16
8	Document type for Non-editable documents	ISO 32000-1:2008 (PDF 1.7)	ISO/IEC	I	MC	MW	--	5.2.17
9	**Graphics –** Raster Image (Lossy Compression) – Exchange Format for Restricted Memory Device cases (like Smart Cards)	JPEG2000 Part 1	ISO/JPEG Committee	I	MC	MW	--	5.2.14
10	**Graphics –** Raster Image (Lossy Compression) – Exchange Format for	JPEG	ISO/JPEG Committee	I	MC	MW	--	5.2.13

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy"	Maturity Level	Enforcement Category	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
				O-Open	MC-Matured & Current	M-Mandatory		
				I-Interim	MD-Matured but Declining	MW-Mandatory - Watch-list		
				A-Additional	E-Evolving			
	Normal cases (like Web, Desktop applications)							
11	**Graphics –** Raster Image (Lossless Compression)	ISO/IEC 15948:2004 (PNG)	ISO/IEC W3C	O	MC	M	--	5.2.19
12	Image Storage/Archival	ISO/IEC 15948:2004 (PNG)	ISO/IEC W3C	O	MC	M	--	5.2.19
13	Scanned Document Storage/Archival	ISO 19005-1:2005 (PDF/A)	ISO/IEC	O	MC	M	--	5.2.18
14	Animation (Raster image graphics format)	GIF89a	CompuServe	I	MC	MW	--	5.2.5
15	Relational Database Query Language	Core SQL 2008	ISO/IEC	O	MC	M	--	5.2.25
16	Content for Mobile Devices – Hypertext Markup Language	XHTML Basic v1.1	W3C	O	MC	M	HTML 5	5.2.32

5.1.2 Data Integration Domain

This domain covers standards that allow data exchange between homogeneous and heterogeneous systems.

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy" O-Open I-Interim A-Additional	Maturity Level MC-Matured & Current MD-Matured but Declining E-Evolving	Enforcement Category M-Mandatory MW-Mandatory - Watch-list	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
1	Data Description Language (for exchange of data)	XML 1.0	W3C	O	MC	M	--	5.2.33
2	Data Schema Definition	XML Schema (XSD) 1.0 Part 1: Structures, XML Schema Part 2:Datatypes	W3C	O	MC	M	--	5.2.35
3	Data Transformation for Presentation	XSL 1.1	W3C	O	MC	M	--	5.2.38
4	Data Transformation for conversion from XML schema format to another format	XSLT 2.0	W3C	O	MC	M	--	5.2.39
5	Content searching and navigation in an XML document.	Xpath 2.0	W3C	O	MC	M	--	5.2.37
6	XML vocabulary for specifying formatting semantics	XSL 1.1	W3C	O	MC	M	--	5.2.38
7	Meta-data elements for content	ISO 15836:2009 (Dublin Core Metadata Element set)	ISO/IEC	O	MC	M	--	5.2.2

5.1.3 Data Interchange Domain

This domain covers standards that allow data interchange services support the exchange of data between homogeneous and heterogeneous systems.

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy" O-Open I-Interim A-Additional	Maturity Level MC-Matured & Current MD-Matured but Declining E-Evolving	Enforcement Category M-Mandatory MW-Mandatory - Watch-list	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
1	Web Services Description Language	WSDL 2.0	W3C	O	MC	M	--	5.2.29
2	Web service request delivery	SOAP 1.2	W3C	O	MC	M	--	5.2.23
3	Web Services Security - Basic Security Profile	Basic Security Profile V1.1	WS-I (Part of OASIS)	O	MC	M	--	5.2.28
4	Web Services Security – SOAP message security	SOAP Message security V1.1	OASIS	I	MC	MW	--	5.2.24
5	Web Services Security – Username Token Profile	Username Token Profile V 1.1	OASIS	I	MC	MW	--	5.2.28
6	Web Services Security - X.509 Certificate Token Profile	X.509 Certificate Token Profile V 1.1	OASIS	I	MC	MW	--	5.2.30

5.1.4 Network Access and Application

The Network layer of this domain specifies how information-processing resources are interconnected, and documents the standards for protocols (for network access and communication), topology (design of how devices are connected together), and wiring (physical medium or wireless assignments). The Network layer encompasses the interoperability components that facilitate the communication and exchange of information within the distributed information-processing environment. The Information Access layer covers the technical specifications required for achieving interoperability between different access medium and application. The Communication domain deals with the intra process communication within application systems as well as the intercommunication between systems.

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy" O-Open I-Interim A-Additional	Maturity Level MC-Matured & Current MD-Matured but Declining E-Evolving	Enforcement Category (M-Mandatory MW-Mandatory - Watch-list))	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
1	Internet Protocol – 32 bit	IPv4	IANA	O	MC	M	--	5.2.11
2	Internet Protocol – 128 bit	IPv6	IETF	O	MC	M	--	5.2.12
3	Wireless LAN - Implementation	IEEE 802.11n-2009	IEEE	I	MC	MW	--	5.2.9
4	Authentication and Authorisation Data Exchange	SAML 2.0	OASIS	I	MC	MW	--	5.2.21
5	Hypertext Transfer	HTTP v1.1	IETF, W3C	O	MC	M	--	5.2.7
6	E-mail Transport	SMTP	IETF	O	MC	M	--	5.2.22
7	Mailbox Access	IMAP4	IETF	O	MC	M	--	5.2.10
8	Directory Access	LDAP V3	IETF	O	MC	M	--	5.2.15
9	Domain Name services	DNS	IETF	O	MC	M	--	5.2.3

5.1.5 Security

This domain deals with the defined security services that are required at each domain of e-Government Architecture model and wherever the components communicate with each other.

Sl. No.	Interoperability Area	Standard / Specification	Standards Body	Status of Standard as per "Policy" O-Open I-Interim A-Additional	Maturity Level MC-Matured & Current MD-Matured but Declining E-Evolving	Enforcement Category (M-Mandatory MW-Mandatory - Watch-list))	*Other version(s), if any, which can also be considered through a Version Management Mechanism*	For additional information, refer the Table No. in this column
1	Secure Electronic mail	S/MIME 3.1	IETF	O	MC	M	S/MIME 3.2	5.2.20
2	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL	HTTPS	IETF	O	MC	M	--	5.2.8
3	Secure Socket Layer	SSL 3.0	IETF	I	MC	MW	--	5.2.26
4	Transport Layer Security for Server	TLS 1.2	IETF	I	MC	MW	--	5.2.27
5	Transport Layer Security for Web Browser	TLS 1.0	IETF	I	MC	MW	--	5.2.27
6	Digital Signature Algorithms	DSA(FIPS 186-3)	NIST	O	MC	M	--	5.2.4
7	XML Signature for XML Message signing	XML Signature	W3C	O	MC	M	--	5.2.36
8	XML Encryption for XML Message encryption	XML Encryption	W3C	O	MC	M	--	5.2.34
9	Wireless LAN security	IEEE 802.11n-2009	IEEE	I	MC	MW	--	5.2.9

5.2 Additional Information on Technical Standards

This section documents additional information on each of the recommended standard for IFEG arranged in alphabetical order in tabulated format with the following columns:

Interoperability Area	*Name of the interoperability area.*	
Standard/Specification with Version and Publication Date (if applicable)	*Name of the Standard/specification with version, where ever applicable (eg. HTML v4.01). Publication date (Month & Year) of the Standard/specification, if applicable (eg. Dec 1999).*	
Description	*Brief description of the Standard/Specification. Largely based on the description in the official specification of the standard.*	
Reference	*Reference or the links to the official specification of the standard.*	
Standards Body	*Name of the Standard Body which published the standard/specification with links to the respective sites (if any).*	
Status of standard as per Policy on open standards	*Open Standard* *Interim Standard* *Additional Standard*	
Maturity Level	*Matured & Current* *Matured but Declining* *Evolving*	
Enforcement Category[1]	*Mandatory/MUST*	*Matured & Current Standards*
	Mandatory – Watch-list	*Interim Standards, Matured & Declining and Evolving Standards* *(It is also Must, but it will be reviewed periodically for revision)*
	Optional	*Additional Standards* *(Either of the Recommended / Additional standard to be mandatory with preference to Recommended standard)*
Other version(s), if any, which can also be considered through a Version Management Mechanism.	Each version of a standard has its own life cycle period (evolve, effective, retire and removal). In this document, the recommended version of the standard is the one which has broader usage and also well supported. The 'other version' (new or evolving or old version)of the same standard can also be considered through a version management mechanism in certain situations as explained in the paragraph "**Version Management Mechanism**" It is also to be noted that multiple versions of a standard do not mean "multiple standards" or "additional standard" for that Area.	
Applicability/Scope	*Basis for selection, applicability and scope.*	
Additional remarks	*Additional remarks such as limitations, specific recommendation / remarks if any.*	
For Interim Standard, the clauses of Policy it violates	*If the Standards is 'Interim', the list of Mandatory Characteristics which it violates.*	
History of revision with dates	*History of the Standards recommended under this Area in earlier Committee's reports, if any.*	

1 *For every Area where no Additional Standard has been recommended, the single identified standard is the one that MUST be used; All listed standards in this document need to be reviewed periodically. However, the standards which are categorized as Evolving (E) or Matured but Declining (MD) or Interim (I) need to be reviewed more frequently to explore if a better candidate has become available; Enforcement Category for such standards has been recorded as Mandatory - Watch-list (MW). Here Watch list is only to alert the users that the mandated standard for this Area will be reviewed more frequently. Other standards have been marked as Mandatory/MUST (M).*

5.2.1 CSS

Interoperability Area	Style Sheets (to define Look & Feel of Web Page)
Standard/Specification with Version and Publication Date (if applicable)	**CSS2** **May 1998 (Revised Apr 2008)**
Description	Cascading Style Sheets, level 2 (CSS2) is a style sheet language that allows authors and users to attach style (e.g., fonts, spacing, and aural cues) to structured documents (e.g., HTML documents and XML including SVG and XUL applications). By separating the presentation style of documents from the content of documents, CSS2 simplifies Web authoring and site maintenance.
Reference	http://www.w3.org/TR/2008/REC-CSS2-20080411/
Owner	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	CSS is designed primarily to enable the separation of document content (written in HTML or a similar markup language) from document presentation, including elements such as the layout, colours, and fonts.
Additional remarks	CSS2 builds on CSS1 and, with very few exceptions, all valid CSS1 style sheets are valid CSS2 style sheets. CSS2 supports media-specific style sheets so that authors may tailor the presentation of their documents to visual browsers, aural devices, printers, Braille devices, hand-held devices, etc. Though CSS3 is not yet a W3C recommended standard, but all the major browsers are already supporting many of the new features. CSS3 is divided into several separate documents called "modules". Each module adds new capabilities or extends features defined in CSS 2, over preserving backward compatibility. Different modules are in different levels of W3C recommendations.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.2 ISO15836 (Dublin Core Metadata Element set)

Interoperability Area	Meta-data elements for Content
Standard/Specification with Version and Publication Date (if applicable)	**ISO15836:2009** **(Dublin Core Metadata Element set)**
Description	The Dublin Core Metadata Element Set is a vocabulary of fifteen properties for use in resource description. The fifteen-element "Dublin Core" described in this International Standard is part of a larger set of metadata vocabularies and technical specifications maintained by the Dublin Core Metadata Initiative (DCMI).
Reference	http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=52142 http://dublincore.org/
Owner	ISO/IEC; DCMI
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	This International Standard establishes a standard for cross-domain resource description. Like RFC 3986, this International Standard does not limit what might be a resource. This International Standard defines the elements typically used in the context of an application profile which constrains or specifies their use in accordance with local or community-based requirements and policies. However, it is does not define implementation detail, which is outside the scope of this International Standard.
Additional remarks	The name "Dublin" comes from its original 1995 invitational workshop, which took place in Dublin, Ohio; "core" because its elements are broad and generic, usable for describing a wide range of resources. Dublin Core consists set of small fundamental metadata fields to describe and catalogue almost all resources from various disciplines. The set contains 15 fields to describe resources like books, video, sound, images, text files and composite media like web pages. Initially these metadata informations intended to provide a solution to interaction between cross-platform resources. Later it was promoted as standard in the fields of library science and computer science.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.3 DNS

Interoperability Area	Domain Name Services
Standard/Specification with Version and Publication Date (if applicable)	**DNS November 1987**
Description	The Domain Name System (DNS) is a nomenclature for computers, services, or any resource connected to the Internet or a private network. It translates human understandable Internet domain and host names to numerical identifiers (Internet Protocol addresses) associated with networking equipments for the purpose of addressing.
Reference	http://www.ietf.org/rfc/rfc1034.txt http://www.ietf.org/rfc/rfc1035.txt
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internet, and administrative organizations.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.4 DSA

Interoperability Area	Digital Signature Algorithms
Standard/Specification with Version and Publication Date (if applicable)	**DSA (FIPS 186-3), June 2009**
Description	This Standard specifies algorithms for applications requiring a digital signature, rather than a written signature. A digital signature is represented in a computer as a string of bits. A digital signature is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data. The Digital Signature Algorithm (DSA) is a United States Federal Government standard for Digital Signatures. For their purpose in Digital Signature Standard (DSS), DSA was proposed by NIST (National Institute of Standards and Technology) in Aug 1991. This initial specification mentioned in FIFS 186. In 1996 a minor revision was released as FIPS 186-1. Then it was expanded further in 2000 as FIPS 186-2 and again in 2009 as FIPS 186-3.
Reference	http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
Standards Body	NIST (National Institute of Standards and Technology)
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	This scope of this Standard is for the protection of binary data (commonly called a message), and for the verification and validation of those digital signatures. Three techniques are approved.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.5 GIF

Interoperability Area	Animation
Standard/Specification with Version and Publication Date (if applicable)	**GIF89a 1989**
Description	Initial version of GIF format was called as 87a. Then the enhanced version 89a came with features like animation delay support, transparent background colours and storage of application-specific metadata. It also supports incorporating of text labels as text instead of embedding them into images.
Reference	http://www.w3.org/Graphics/GIF/spec-gif89a.txt
Standards Body	CompuServe
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	CompuServe introduced the Graphics Interchange Format (GIF) in 1987 and now its used wildly because of its support and portability. It was introduced to provide small size colour images for their downloading areas. It replaced the existing run-length encoding to store black and white images. It was more efficient when compare to run-length encoding. It uses up to 8 bits to represent each pixel. It is not suitable for photographs and colour images with continuous colours because of its colour limitation. But it is well-suited for reproducing solid colour images and photos.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.6 ISO/IEC 15445 (HTML)

Interoperability Area	Document type for Simple Hypertext Web Content
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC 15445:2000 May 2000** **(HTML 4.01 Dec 1999)**
Description	Hyper Text Markup Language (HTML) is the encoding scheme used to create and format a web document. HTML 4 extends HTML with mechanisms for style sheets, scripting, frames, embedding objects, improved support for right to left and mixed direction text, richer tables, and enhancements to forms, offering improved accessibility for people with disabilities.
Reference	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=27688 http://www.w3.org/TR/html401/
Standards Body	ISO/IEC , W3C,
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	HTML 5
Applicability/Scope	HTML is widely adopted global standard for simple hypertext web content (See also XHTML). HTML 4.01 is the latest version. The scope of HTML is to: •Publish online static documents with headings, text, tables, lists, photos, etc. •Retrieve online information via hypertext links, at the click of a button. •Design forms for conducting transactions with remote services, for use in searching for information, making reservations, ordering products, etc. •Include spread-sheets, video clips, sound clips, and other applications directly in the documents. And not recommended for complex/dynamic web pages.
Additional remarks	The popular browsers implement HTML 4.01 differently with non-standard extensions. The e-Governance web content authors are strongly recommended to consult the appropriate browser vendor's documentation and test the compatibility of their content with respective browsers in popular Operating System configurations. HTML 5.0 is W3C's proposed next standard for HTML 4.01, XHTML 1.0 and DOM level 2 HTML .
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.7 HTTP

Interoperability Area	Hypertext Transfer
Standard/Specification with Version and Publication Date (if applicable)	**HTTP 1.1 June 1999**
Description	Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems.
Reference	http://www.ietf.org/rfc/rfc2616.txt
Standards Body	IETF, W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	HTTP is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers. HTTP has been in use by the World-Wide Web global information initiative since 1990.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.8 HTTPS

Interoperability Area	Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL
Standard/Specification with Version and Publication Date (if applicable)	**HTTPS, May 2000**
Description	Hypertext Transfer Protocol Secure (HTTPS) is a web protocol based on Hype Text Transfer Protocol (HTTP) and SSL/TLS protocol to provide encrypted communication and secure identification of a network web server.
Reference	http://www.ietf.org/rfc/rfc2818.txt
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	HTTP functions as a request-response protocol in the client-server computing model. HTTPS is designed to withstand such attacks and is considered secure against attacks and vulnerability. HTTPS is not a separate protocol, but refers to the use of ordinary HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.9 IEEE 802.11n-2009

Interoperability Area	Wireless LAN
Standard/Specification with Version and Publication Date (if applicable)	**IEEE 802.11n-2009**
Description	The purpose of this standard is to provide wireless connectivity to automatic machinery, equipment, or STAs that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area. This standard also offers regulatory bodies as a means of standardizing access to one or more frequency bands for the purpose of local area communication.
Reference	*http://standards.ieee.org/findstds/standard/802.11n-2009.html* *http://standards.ieee.org/getieee802/download/802.11n-2009.pdf*
Standards Body	IEEE STANDARDS ASSOCIATION
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The scope of this standard is to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations (STAs) within a local area.
Additional remarks	The 802.11n amendment defines modifications to both the IEEE 802.11 physical layer (PHY) and the IEEE 802.11 medium access control (MAC) sub-layer so that modes of operation can be enabled that are capable of much higher throughputs, with a maximum throughput of at least 100 Mb/s, as measured at the MAC data service access point (SAP).
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.10 IMAP

Interoperability Area	Mailbox Access
Standard/Specification with Version and Publication Date (if applicable)	**IMAP 4rev1, March 2003**
Description	The Internet Message Access Protocol (IMAP) is an Application Layer Internet protocol. IMAP allows a client to access and manipulate electronic mail messages on a server. This permits manipulation of mailboxes (remote message folders) in a way that is functionally equivalent to local folders. IMAP also provides the capability for an off-line client to resynchronize with the server.
Reference	http://tools.ietf.org/html/rfc3501
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The Internet Message Access Protocol (IMAP) is a standard mail protocol used to receive emails from a remote server to a local email client. IMAP supports both on-line and off-line modes of operation.
Additional remarks	Email clients using IMAP generally leave messages on the server until the user explicitly deletes them. Email clients can use SMTP for sending emails and IMAP for retrieving emails.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.11 IPv4

Interoperability Area	Internet Protocol – 32 bit
Standard/Specification with Version and Publication Date (if applicable)	**IP v4 , Sep 1981**
Description	Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. It provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses (IP addresses). In addition to inter network routing, IP provides error reporting and fragmentation and reassembly of information units called datagrams for transmission over networks with different maximum data unit sizes. Internet Protocol version 4 is the fourth revision of Internet Protocol used in Internet Layer and it is the widely deployed version compared to other revisions. IPv4 is defined in IETF with RFC 791 which replacing the previous version of RFC 760. Ipv4/8 allocations are maintained by IANA.
Reference	http://www.rfc-editor.org/rfc/rfc791.txt
Standards Body	IANA
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	IP v4 is a connectionless protocol used in packet-switched link layer networks. It works on best effort delivery model, in that it assures proper sequencing or duplicate avoiding. It means that it doesn't assure the time of delivery or guarantee delivery of data packets. It will reach the hosts depending on the network traffic loads.
Additional remarks	Although the 32-bit address space of IPv4 allows for 4,294,967,296 addresses, the allocation practices limit the number of public IPv4 addresses to a few hundred million. The rising prominence of Internet-connected devices and appliances ensures that the public IPv4 address space will eventually be depleted. Due to impending exhaustion of the IPv4 address space, migration from IPv4 to IPv6 should be evaluated periodically and implemented gradually.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.12 IPv6

Interoperability Area	Internet Protocol – 128 bit
Standard/Specification with Version and Publication Date (if applicable)	**IPv6, Dec 1998**
Description	Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. It provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses (IP addresses). In addition to inter network routing, IP provides error reporting and fragmentation and reassembly of information units called datagrams for transmission over networks with different maximum data unit sizes. IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4) [RFC-791]. The changes from IPv4 to IPv6 fall primarily into the following categories: • Expanded Addressing Capabilities • Header Format Simplification • Improved Support for Extensions and Options • Flow Labelling Capability
Reference	http://www.rfc-editor.org/rfc/rfc2460.txt
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	IPv6 mainly concentrate areas such like IPv4 address exhaustion, Multicast, Stateless address auto-configuration (SLAAC), IPSec, Simplified processing by routers, Mobility and Jumbograms. IPv6 uses 128 bit for addressing where as IPv4 uses 32 bit. So its allows wide range of addresses to identify devices on the network. In IPv4 limits the payload packets to 65535 (2^{16}-1) octets. Instead IPv6 allows (2^{32}-1) octets per payload which will increase the performance of network connections.
Additional remarks	To meet the exponential growth of the Internet and the impending exhaustion of the IPv4 address space, it is advised that any new procurement of hardware should support IPv6.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.13 ISO/IEC IS 10918-1:1994 (JPEG)

Interoperability Area	Graphics - Raster (Lossy Compression) – Exchange Format for Normal Cases (like Web, Desktop Applications)
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC IS 10918-1:1994 (JPEG)**
Description	JPEG is an image coding system with digital compression for continuous-tone grayscale or colour digital still image data. Its architecture should lend itself to a wide range of uses from portable digital cameras through to advanced pre-press, medical imaging and other key sectors. JPEG refers to all parts of the standard; Part 1 is The basic JPEG standard, which defines many options and alternatives for the coding of still images of photographic quality.
Reference	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18902
Standards Body	ISO/IEC
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	As lossy method can produce a much smaller compressed file than any lossless method, it can be used for low bandwidth transmission, etc. Only for such situations, this should be used.
Additional remarks	There is no eligible standard (as per the Policy on Open Standards for e-Governance) currently available for using image with high compression ratios by compromising the quality; the current recommendation that JPEG Part-1 may be used where high compression ratios are required, with loss in quality. This decision should be reviewed regularly (at least once in two years) keeping in mind the following: *i. If JPEG Committee/Consortium's intent to make it royalty free with no submarine patents is achieved then no further reviews will be necessary* ii. Otherwise, if evolving open standards achieved the required high compression, migration away from JPEG Part-1 may be undertaken.
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.14 ISO/IEC 15444-1:2004 (JPEG2000 Part 1)

Interoperability Area	Graphics - Raster (Lossy Compression) - Exchange Format for Restricted Memory Device cases (like Smart Cards)
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC 15444-1:2004 (JPEG2000 Part 1)** **Second Edition Sep 2004**
Description	JPEG 2000 is an image coding system that uses compression techniques based on wavelet technology. Its architecture should lend itself to a wide range of uses from portable digital cameras through to advanced pre-press, medical imaging and other key sectors. JPEG 2000 refers to all parts of the standard; Part 1 is the Core coding system. JPEG 2000 Part 1 supports both lossless and lossy compressions.
Reference	http://www.iso.org/iso/search.htm?qt=15444&searchSubmit=Search&sort=rel&type=simple&published=on
Standards Body	ISO/IEC
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	As lossy method can produce a much smaller compressed file than any lossless method, it can be used for low bandwidth transmission, storing in limited storage size like smart cards, etc. Only for such situations, this should be used.
Additional remarks	There is no eligible standard (as per the Policy on Open Standards for e-Governance) currently available for using image with high compression ratios by compromising the quality; the current recommendation that JPEG 2000 Part-1 may be used where high compression ratios are required, with loss in quality. This decision should be reviewed regularly (at least once in two years) keeping in mind the following: *i. If JPEG Committee/Consortium's intent to make it royalty free with no submarine patents is achieved then no further reviews will be necessary* *ii. Otherwise, if evolving open standards achieved the required high compression, migration away from JPEG 2000 Part-1 may be undertaken.* JPEG 2000 has poor support in popular web browsers especially in Linux.
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.15 LDAP

Interoperability Area	Directory Access
Standard/Specification with Version and Publication Date (if applicable)	**LDAP v3- June 2006**
Description	The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.
Reference	http://tools.ietf.org/html/rfc4510
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	LDAP is an application protocol used to read as well as to update remote directory contents over an IP network. Here a directory means a set of records with hierarchically structured and stored globally for purpose of distributed access over network. Its mainly used to store login informations where the details can be accessed from heterogeneous applications or platforms.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.16 ISO/IEC 26300 (ODF)

Interoperability Area(s)	Document Type for Editable documents (with formatting), Spreadsheet, Presentation.
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC 26300:2006 (ODF v1.0 Dec 2006)**
Description	The OpenDocument Format (ODF) is an XML-based file format for representing electronic documents such as spreadsheets, charts, presentations and word processing documents.
Reference	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office
Standards Body	ISO/IEC; OASIS
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	This is the specification of the Open Document Format for Office Applications (OpenDocument) format, an open, XML-based file format for office applications. The most common filename extensions used for OpenDocument documents are: • .odt for word processing (text) documents • .ods for spreadsheet • .odp for presentation • .odg for graphics • .odf for formulae, mathematical equations There are many free and proprietary implementations that support the OpenDocument format including office suites (both stand-alone and web-based) and individual applications such as word-processors, spreadsheets, presentation, and data management applications. Few of the office suites supporting OpenDocument fully or partially include: AbiWord, Adobe Buzzword, Atlantis Word Processor, Aspose.Words, Google Docs, IBM Lotus Symphony, Koffice, Microsoft Office 2010/Office 2007 SP2, NeoOffice, OpenOffice.org, Sun Microsystems StarOffice, SoftMaker Office, WordPad 6.1, Corel WordPerfect Office X4, Zoho Office Suite, Evince, Inkscape exports, Okular, Scribus imports, etc.
Additional remarks	OpenDocument 1.1 was approved as an OASIS Standard during Feb 2007. This version was not submitted to ISO/IEC, because it is considered to be a minor update to ODF 1.0 OpenDocument 1.2 is currently OASIS recommendation.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.17 ISO 32000-1 (PDF)

Interoperability Area	Document type for Non-editable documents
Standard/Specification with Version and Publication Date (if applicable)	**ISO 32000-1:2008** **(PDF 1.7 Jul 2008)**
Description	Portable Document Format (PDF) is a file format for document exchange. PDF is used for representing two-dimensional documents in a manner independent of the application software, hardware, and operating system. Each PDF file encapsulates a complete description of a fixed-layout 2D document that includes the text, fonts, images, and 2D vector graphics which compose the documents
Reference	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502
Standards Body	ISO/IEC
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	PDF files are viewable and printable on virtually any platform — Mac OS, Microsoft® Windows®, UNIX®, Linux and many mobile platforms. PDF files look like original documents and preserve source file information — text, drawings, video, 3D, maps, full-colour graphics, photos, and even business logic — regardless of the application used to create them.
Additional remarks	There is no eligible standard (as per the Policy) currently available for Non-editable documents and Scanned Document Storage/Archival ; the Committee recommends that PDF 1.7 (ISO/IEC 32000-1:2008) may be used as an interim standard. This decision should be reviewed regularly (at least once in two years) keeping in mind the following: *i. If Adobe Systems Incorporateds intent to make it royalty free is achieved then no further reviews will be necessary* *ii. Otherwise, if evolving open standards achieved the functional requirements, migration away from PDF 1.7 (ISO/IEC 32000-1:2008) may be undertaken.*
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.18 ISO 19005-1:2005 (PDF/A)

Interoperability Area	Scanned Document Storage/Archival
Standard/Specification with Version and Publication Date (if applicable)	**ISO 19005-1:2005 (PDF/A-1 Oct 2005)**
Description	PDF/A is a standard which turns Portable Document Format (PDF) into a "electronic document file format for long-term preservation". PDF/A-1 is the first part of the standard. It is based on PDF 1.4 It is published as an ISO Standard under ISO 19005-1:2005 on 1st Oct 2005 (Document Management - Electronic document file format for long term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)). ISO 32000-1, which is based on PDF 1.7 is under development (ISO/DIS 19005-2).
Reference	http://www.iso.org/iso/catalogue_detail?csnumber=38920
Standards Body	ISO/IEC
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	PDF/A, an electronic document, can be used for long-term preservation of documents. PDF/A is a subset of PDF and are viewable and printable on virtually any platform — Mac OS, Microsoft® Windows®, UNIX®, Linux and many mobile platforms. Many document handling software support PDF/A: ABBYY FineReader, Adlib Software, Adobe Acrobat, ghostscript, Kofax Express, Microsoft Office 2007, Open Office 2.4 and above, PDF/A Manager, etc.
Additional remarks	The reproducibility requirement for PDF/A documents is to be 100% self-contained. All of the information necessary for displaying the document in the same manner every time is embedded in the file. A PDF/A document is not permitted to be reliant on information from external sources (e.g. font programs and hyper-links). Other key elements to PDF/A compatibility include: • Executable file launches, Sound, Movie, Reset Form, Import Data and JavaScript are forbidden. • All fonts must be embedded and also must be legally embeddable for unlimited, universal rendering. • Colour-spaces specified in a device-independent manner. • Encryption is disallowed. • Use of standards-based metadata is mandated.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.19 ISO/IEC 15948:2004 (PNG)

Interoperability Area	Graphics – Raster Image (Lossless Compression)
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC 15948:2004** **(PNG Nov 2003)**
Description	Portable Network Graphics (PNG) is an extensible file format for lossless, portable, well-compressed storage of raster images. PNG provides a patent-free replacement for GIF and can also replace many common uses of TIFF. Indexed-colour, grayscale, and true-colour images are supported, plus an optional alpha channel for transparency.
Reference	http://www.w3.org/TR/PNG/
Standards Body	W3C, ISO/IEC
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	The Portable Network Graphics (PNG) format was designed as an image-file format not requiring a patent license to replace the older and simpler GIF format and, to some extent, the much more complex TIFF format. PNG supports palette-based (palettes of 24-bit RGB or 32-bit RGBA colours), grayscale, RGB, or RGBA images. PNG can be used for image archival in systems having normal storage size and also for transmission through high bandwidth networks. PNG can also used in areas where repeated editing involved, since there will not be any quality degradation.
Additional remarks	Animated PNG (APNG) is an unofficial extension to PNG. APNG files works similarly to animated GIF files, while supporting 24-bit images and 8-bit transparency not available for GIFs. It also retains backward compatibility with non-animated PNG files. APNG has web-browser support for Firefox, SeaMonkey and Opera; image processing applications like GIMP, ImageJ also support APNG. PNG in combination with SVG and SMIL can be used to animate images.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.20 S/MIME

Interoperability Area	Secure Electronic Mail
Standard/Specification with Version and Publication Date (if applicable)	S/MIME **3.1 July 2004**
Description	Secure/Multi-purpose Internet Mail Extensions (S/MIME) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures), and data confidentiality (using encryption).
Reference	http://www.ietf.org/rfc/rfc3851.txt
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	3.2
Applicability/Scope	S/MIME was created on the existing MIME protocol standard and it can be integrated easily into the existing email and messaging products. As S/MIME was designed on the existing popular supported standards, it became quite popular and was implemented across a wide range of operating systems and email clients. The users do not have to install any additional program or software to utilize this facility.
Additional remarks	S/MIME 3.2 – was published by IETF during January 2010. (http://tools.ietf.org/html/rfc5751)
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.21 SAML

Interoperability Area	Authentication and Authorisation Data Exchange
Standard/Specification with Version and Publication Date (if applicable)	**SAML 2.0 March 2005**
Description	Security Assertion Markup Language (SAML) defines an XML-based framework for communicating security and identity (e.g., authentication, entitlements, and attribute) information between computing entities. SAML promotes interoperability between disparate security systems, providing the framework for secure e-business transactions across company boundaries.
Reference	http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
Standards Body	OASIS
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	SAML does not require user information to be maintained and synchronized between directories. SAML V2.0 permits attribute statements, name identifiers, or entire assertions to be encrypted. SAML V2.0 includes mechanisms that allow providers to communicate privacy policy and settings. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.22 SMTP

Interoperability Area	E-mail Transport
Standard/Specification with Version and Publication Date (if applicable)	**SMTP, October 2008**
Description	Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
Reference	http://tools.ietf.org/html/rfc5321
Standards Body	IETF
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. Simple Mail Transport Protocol (SMTP) enables the standardized exchange of electronic mail. Between a client and the mail server, SMTP is only used for sending messages to the server. The client relies on another protocol to retrieve messages and manage mailboxes.
Additional remarks	This specification also contains information that is important to its use as a "mail submission" protocol, as recommended for Post Office Protocol (POP).
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.23 SOAP

Interoperability Area	Web Services Request Delivery
Standard/Specification with Version and Publication Date (if applicable)	**SOAP 1.2 – Part 1 (Second Edition)** **Apr 2007**
Description	SOAP stands for Simple Object Access Protocol. SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information among machines in a decentralized, distributed network environment. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.
Reference	http://www.w3.org/TR/soap12-part1/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks using XML as its message format. This XML based protocol consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined data-types, and a convention for representing procedure calls and responses.
Additional remarks	Limitations •The limitations of SOAP arise from its adherence to the client server model.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.24 SOAP Message Security

Interoperability Area	Web Services Security - SOAP Message Security
Standard/Specification with Version and Publication Date (if applicable)	**SOAP Message Security 1.1 - 2006**
Description	This specification proposes a standard set of SOAP [SOAP11, SOAP12] extensions that can be used when building secure Web services to implement message content integrity and confidentiality. This specification refers to this set of extensions and modules as the "Web Services Security: SOAP Message Security" or "WSS: SOAP Message Security". This specification is flexible and is designed to be used as the basis for securing Web services within a wide variety of security models including PKI, Kerberos, and SSL. Specifically, this specification provides support for multiple security token formats, multiple trust domains, multiple signature formats, and multiple encryption technologies. The token formats and semantics for using these are defined in the associated profile documents. This specification provides three main mechanisms: ability to send security tokens as part of a message, message integrity, and message confidentiality. These mechanisms by themselves do not provide a complete security solution for Web services. Instead, this specification is a building block that can be used in conjunction with other Web service extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies. These mechanisms can be used independently (e.g., to pass a security token) or in a tightly coupled manner (e.g., signing and encrypting a message or part of a message and providing a security token or token path associated with the keys used for signing and encryption).
Reference	http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
Standards Body	Web Service Security (WSS) - OASIS
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The goal of this specification is to enable applications to conduct secure SOAP message exchanges. This specification is intended to provide a flexible set of mechanisms that can be used to construct a range of

	security protocols; in other words this specification intentionally does not describe explicit fixed security protocols.
Additional remarks	The following topics are outside the scope of this specification: • Establishing a security context or authentication mechanisms. • Key derivation. • Advertisement and exchange of security policy. • How trust is established or determined. • Non-repudiation. For erratas, refer http://www.oasis-open.org/standards#wssv1.1
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.25 ISO/IEC 9075:2008 (SQL:2008)

Interoperability Area(s)	Relational Database Query Language
Standard/Specification with Version and Publication Date (if applicable)	**ISO/IEC 9075:2008 (SQL:2008) – July 2008** **(Core SQL : Conformance to Part 2 & Part 11)**
Description	SQL initially developed by IBM and then formalized by ANSI in 1987. Then its further updated and made as ISO 9075 standard in 1982. Latest version released in 2008 with the name SQL:2008 with update. ISO 9075 consist the following parts. * ISO/IEC 9075-1:2008 Framework (SQL/Framework) * ISO/IEC 9075-2:2008 Foundation (SQL/Foundation) * ISO/IEC 9075-3:2008 Call-Level Interface (SQL/CLI) * ISO/IEC 9075-4:2008 Persistent Stored Modules (SQL/PSM) * ISO/IEC 9075-9:2008 Management of External Data (SQL/MED) * ISO/IEC 9075-10:2008 Object Language Bindings (SQL/OLB) * ISO/IEC 9075-11:2008 Information and Definition Schemas (SQL/Schemata) * ISO/IEC 9075-13:2008 SQL Routines and Types Using the Java TM Programming Language (SQL/JRT) * ISO/IEC 9075-14:2008 XML-Related Specifications (SQL/XML) Every claim of conformance shall include a claim of minimum conformance, which is defined as a claim to meet the conformance requirements specified in [ISO9075-2] and [ISO9075-11]. SQL language that does not require more than a claim of minimum conformance is called **Core SQL**.
Reference	http://www.iso.org/iso/catalogue_detail.htm?csnumber=45498 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38640 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38641 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38642 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38643 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38644 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38645 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38646 http://www.iso.org/iso/catalogue_detail.htm?csnumber=45499
Standards Body	ISO/IEC
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	SQL is designed to manage data in Relational Database Management Systems using the functionalities like data insertion, querying, data update, deletion, schema creation and modification, and data access control. Some of the additional features supported are: regular expression matching, object-oriented

	features, recursive queries, triggers, procedural and control-of-flow statements, XML related features, auto generated values, enabling applications to integration of XQuery with SQL, etc.
Additional remarks	Some of the major implementations that follow the Core SQL:2008 compliance are: Oracle (http://download.oracle.com/docs/cd/E14072_01/server.112/e10592/ap_standard_sql003.htm), MS SQL 2008 (http://download.microsoft.com/download/C/6/C/C6C3C6F1-E84A-44EF-82A9-49BD3AAD8F58/%5BMS-TSQLISO02%5D.PDF, http://download.microsoft.com/download/C/6/C/C6C3C6F1-E84A-44EF-82A9-49BD3AAD8F58/%5BMS-TSQLISO11%5D.PDF), PostgreSQL (http://developer.postgresql.org/pgdocs/postgres/features.html), etc. Some of the implementations are inconsistent with the standard and, usually, incompatible between vendors.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.26 SSL

Interoperability Area	Secure Socket Layer
Standard/Specification with Version and Publication Date (if applicable)	**SSL 3.0-1996**
Description	The Secure Sockets Layer (SSL) is a commonly-used cryptographic protocol for managing the security of a message transmission on the Internet. It has been succeeded by Transport Layer Security TLS 1.0 (RFC 2246), which is based on SSL 3.0. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. The SSL protocol was developed by Netscape. Version 1.0 was not released publicly. Version 2.0 was released in February 1995 with number of security flaws. This led to the design of SSL version 3.0 and was released in 1996.
Reference	http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
Standards Body	IETF, Netscape
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	SSL protocol relies on the use of public key encryption technology for authentication and encryption. The intent was to be a “security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.” The goals included cryptographic security, interoperability, extensibility, and relative efficiency.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.27 TLS

Interoperability Area	Transport Security Layer for Web Browser Transport Security Layer for Server
Standard/Specification with Version and Publication Date (if applicable)	**TLS 1.0- January 1999 (**for Transport Security Layer for Web Browser) **TLS 1.2- August 2008 (**for Transport Security Layer for Server)
Description	Transport Layer Service Protocol (TLS) is a cryptographic protocol for managing communication security of a message transmission on the Internet. It was based on Secure Sockets Layer (SSL). The protocol allows “server to server” and “web-browser to server” applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Reference	http://www.ietf.org/rfc/rfc5246.txt
Standards Body	IETF
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications apart from cryptographic security, interoperability, extensibility, and relative efficiency.
Additional remarks	TLS v 1.2 is SSL v 3.3
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.28 Username Token Profile

Interoperability Area	Web Services Security - User name Token Profile
Standard/Specification with Version and Publication Date (if applicable)	**Username Token Profile V 1.1 – Feb 2006**
Description	This specification describes how to use the UsernameToken with the WSS: SOAP Message Security specification [WSS]. More specifically, it describes how a web service consumer can supply a UsernameToken as a means of identifying the requester by “username”, and optionally using a password (or shared secret, or password equivalent) to authenticate that identity to the web service producer.
Reference	http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-UsernameTokenProfile.pdf
Standards Body	OASIS
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	This specification is designed to work with the general SOAP [SOAP11, SOAP12] message structure and message processing model, and should be applicable to any version of SOAP. All compliant implementations MUST be able to process the <wsse:UsernameToken> element. For erratas, refer http://www.oasis-open.org/standards#wssv1.1
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.28 WS-I Basic Security Profile

Interoperability Area	Web Services Security - Basic Security Profile
Standard/Specification with Version and Publication Date (if applicable)	**Basic Security Profile V 1.1 – Jan 2010**
Description	Basic Security Profile standard consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability. Basically it is intended to provide secure and reliable messaging service for web services.
Reference	http://www.ws-i.org/profiles/basicsecurityprofile-1.1.html
Standards Body	WS-I
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	The Profile was developed according to a set of principles that, together, form the philosophy of the Basic Security Profile 1.1, as it relates to bringing about interoperability.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.29 WSDL

Interoperability Area	Web Services Description Language
Standard/Specification with Version and Publication Date (if applicable)	**WSDL 2.0** **June 2007**
Description	Web Services Description Language Version 2.0 (WSDL 2.0) provides a model and an XML format for describing Web services. WSDL 2.0 enables one to separate the description of the abstract functionality offered by a service from concrete details of a service description such as “how” and “where” that functionality is offered.
Reference	http://www.w3.org/TR/wsdl20/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	WSDL is used to provide web services over Internet in combination with SOAP and XML Schema. The operations available on the server can be determined by a client program connecting to a web service by reading the WSDL file on the server. Using XML Schema, special data-types are embedded in the WSDL file. The client can then use SOAP to actually call one of the operations listed in the WSDL file. By accepting binding to all the HTTP request methods, WSDL 2.0 specification offers better support for RESTful web services, and is much simpler to implement.
Additional remarks	WSDL 2.0 became a W3C recommendation on June 2007. WSDL 1.2 was renamed to WSDL 2.0 because it has substantial differences from WSDL 1.1.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.30 X.509 Certificate Token Profile

Interoperability Area	Web Services Security - X.509 Certificate Token Profile
Standard/Specification with Version and Publication Date (if applicable)	**X.509 Certificate Token Profile V 1.1 – February 2004**
Description	This specification describes the use of the X.509 authentication framework with the Web Services Security: SOAP Message Security specification. An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number and validity interval. This binding may be subject to subsequent revocation advertised by mechanisms that include issuance of CRLs, OCSP tokens or mechanisms that are outside the X.509 framework, such as XKMS. An X.509 certificate may be used to validate a public key that may be used to authenticate a SOAP message or to identify the public key with SOAP message that has been encrypted.
Reference	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0
Standards Body	OASIS
Status of recommendation as per Policy	Interim Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory - Watch-list
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	This specification describes the syntax and processing rules for the use of the X.509 authentication framework with the Web Services Security: SOAP Message Security specification [WS-Security]. When using X.509 certificates, the error codes defined in the WSS: SOAP Message Security specification [WS- Security] MUST be used. If an implementation requires the use of a custom error it is recommended that a sub-code be defined as an extension of one of the codes defined in the WSS: SOAP Message Security specification [WS-Security]. For erratas, refer http://www.oasis-open.org/standards#wssv1.1
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	4.1.2 - The Patent claims necessary to implement the Identified Standard shall be made available on a Royalty-Free basis for the life time of the Standard.
History of revision with dates	-

5.2.31 XHTML

Interoperability Area	Document type for Complex Hypertext Web Content
Standard/Specification with Version and Publication Date (if applicable)	**XHTML 1.1 Module-based XHTML** **May 2001**
Description	XHTML is a XML based stricter and cleaner markup language.
Reference	http://www.w3.org/TR/xhtml11/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	HTML 5 (XML serialisation XHTML5)
Applicability/Scope	XHTML offers freedom of introducing new elements or additional element attributes to express developers/designers discovering ideas through markup. XHTML is widely adopted global standard for complex hypertext web content, including Content Management System.
Additional remarks	As the XHTML family evolves, documents conforming to XHTML 1.1 will be more likely to inter operate within and among various XHTML environments. XHTML content can be parsed using standard XML parsers. XHTML content can also be transformed to other XML formats by using XSLT. HTML 5.0 is W3C's proposed next standard for HTML 4.01, XHTML 1.1 and DOM level 2 HTML, and is expected to replace XHTML in the future.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.32 XHTML Basic

Interoperability Area	Content for Mobile Devices
Standard/Specification with Version and Publication Date (if applicable)	**XTML Basic v1.1 Second Edition – November 2010**
Description	The XHTML Basic document type includes the minimal set of modules required to be an XHTML host language document type, and in addition it includes images, forms, basic tables, and object support. It is designed for Web clients that do not support the full set of XHTML features; for example, Web clients such as mobile phones, PDAs, pagers, and set top boxes. The document type is rich enough for content authoring. XHTML Basic is designed as a common base that may be extended. The goal of XHTML Basic is to serve as a common language supported by various kinds of user agents.
Reference	http://www.w3.org/TR/xhtml-basic/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	HTML 5
Applicability/Scope	The motivation for XHTML Basic is to provide an XHTML document type that can be shared across communities (e.g. desktop, TV, and mobile phones), and that is rich enough to be used for simple content authoring. New community-wide document types can be defined by extending XHTML Basic in such a way that XHTML Basic documents are in the set of valid documents of the new document type. Thus an XHTML Basic document can be presented on the maximum number of Web clients.
Additional remarks	XHTML Basic is designed as a common base that may be extended. The goal of XHTML Basic is to serve as a common language supported by various kinds of user agents. Compared to the rich functionality of HTML 4, XHTML Basic may look like one step back, but in fact, it is two steps forward for clients that do not need what is in HTML 4 and for content developers who get one XHTML subset instead of many. HTML 5.0 is W3C's proposed next standard for HTML 4.01, XHTML 1.x and DOM level 2 HTML
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.33 XML

Interoperability Area	Data Description Language for exchange of Data
Standard/Specification with Version and Publication Date (if applicable)	**XML 1.0 (Fifth Edition)** **Nov 2008**
Description	Extensible Markup Language (XML) is a simple, very flexible text format with a set of rules for encoding documents electronically. It is derived from SGML (ISO 8879), the Standard Generalized Markup Language.
Reference	http://www.w3.org/TR/xml/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	XML's design goals emphasize simplicity, generality, and usability over the Internet. It is a textual data format, with strong support via Unicode for the languages of the world. It is also widely used for the representation of arbitrary data structures, like in Web Services.
Additional remarks	XML is currently having 2 versions, viz. XML 1.0 and XML 1.1. XML 1.0 was initially defined in 1998 and currently in Fifth Edition published during Nov 2008. It is widely used and hence recommended for general use. *XML 1.1*, was initially published during Feb, 2004. The features of XML 1.1 are intended to make XML easier in cases like enabling the use of line-editing characters used on EBCDIC platforms, and the use of scripts and characters absent from Unicode 3.2. XML 1.1 is not widely implemented.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.34 XML Encryption

Interoperability Area	XML Signature for XML Message signing
Standard/Specification with Version and Publication Date (if applicable)	**XML Encryption, December 2002**
Description	This specification specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption element which contains or references the cipher data.
Reference	http://www.w3.org/TR/xmlenc-core/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	XML Encryption, also known as XML-Enc, is a specification, that defines how to encrypt the contents of an XML element.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.35 XML Schema

Interoperability Area	Data Schema Definition
Standard/Specification with Version and Publication Date (if applicable)	**XML Schema Part 1: Structures (Second Edition),** **XML Schema Part 2:Datatypes (Second Edition)** **Oct 2004**
Description	*XML Schema: Structures* specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on *XML Schema Part 2: Datatypes*. *XML Schema: Datatypes* is part 2 of the specification of the XML Schema language. It defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.
Reference	http://www.w3.org/TR/xmlschema-1/ http://www.w3.org/TR/xmlschema-2/ http://www.w3.org/XML/Schema
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	
Applicability/Scope	The scope of *XML Schema: Structures* is to define the nature of XML schemas and their component parts, provide an inventory of XML markup constructs with which to represent schemas, and define the application of schemas to XML documents. The scope of *XML Schema: Datatypes is to* discuss datatypes that can be used in an XML Schema. These datatypes can be specified for element content that would be specified as #PCDATA and attribute values of various types in a DTD. It is the intention of this specification that it be usable outside of the context of XML Schemas for a wide range of other XML-related activities such as [XSL] and [RDF Schema].
Additional remarks	The technical benefits of using XML Schemas (also called as XSD-

	XML Schema Document or WXL – W3C XML Schema) over other languages, though not exhaustive, are listed below: •XML Schemas are themselves XML documents •Refers XML Schema namespaces •Provides more powerful means to define XML documents structure and limitations •Support for primitive (built-in) data types (eg: xsd:integer, xsd:string, xsd:date, and so on), which facilitates using XML in conjunction with other typed-data, including relational data. •The ability to define custom data types, using object-oriented data modelling principles: encapsulation, inheritance, and substitution. •Compatibility other XML technologies, for example, Web services, XQuery, XSLT, XForms and other technologies can optionally be schema-aware.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.36 XML Signature

Interoperability Area	XML Signature for XML Message signing
Standard/Specification with Version and Publication Date (if applicable)	**XML Signature, 10th June 2008**
Description	XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.
Reference	http://www.w3.org/TR/xmldsig-core/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	XML signatures is used to sign any data of any type, typically XML documents which are accessible via a URL can be signed. An XML signature used to sign a resource outside its containing XML document is called a detached signature. If it is used to sign some part of its containing document, it is called an enveloped signature. If it contains the signed data within itself it is called an enveloping signature.
Additional remarks	-
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.37 XPath

Interoperability Area	Content searching and navigation in an XML document.
Standard/Specification with Version and Publication Date (if applicable)	**Xpath 2.0** **23 January 2007**
Description	XML Path Language (XPath) is a query language for selecting nodes from an XML document and also can be used to compute values (eg. Strings, numbers or Boolean) from the content of an XML document.
Reference	http://www.w3.org/TR/xpath20/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	XPath 2.0 is an expression language that allows the processing of values conforming to the data model defined in **[XQuery/XPath Data Model (XDM)]**. The data model provides a tree representation of XML documents as well as atomic values such as integers, strings, and booleans, and sequences that may contain both references to nodes in an XML document and atomic values. The result of an XPath expression may be a selection of nodes from the input documents, or an atomic value, or more generally, any sequence allowed by the data model.
Additional remarks	The name of the language derives from its most distinctive feature, the path expression, which provides a means of hierarchic addressing of the nodes in an XML tree. XPath 2.0 is a superset of **[XPath 1.0]**, with the added capability to support a richer set of data types, and to take advantage of the type information that becomes available when documents are validated using XML Schema. A backwards compatibility mode is provided to ensure that nearly all XPath 1.0 expressions continue to deliver the same result with XPath 2.0.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.38 XSL

Interoperability Area	Data Transformation for Presentation
Standard/Specification with Version and Publication Date (if applicable)	**XSL 1.1** **5th Dec 2006**
Description	Extensible Stylesheet Language (XSL) is a language for expressing stylesheets. It consists of two parts: 1. a language for transforming XML documents (XSLT), and 2. an XML vocabulary for specifying formatting semantics. An XSL stylesheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses the formatting vocabulary.
Reference	http://www.w3.org/TR/xsl11/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	With XML we can use any tags we want, and the meaning of these tags are not automatically understood by the browser: <table> could mean a HTML table or maybe a piece of furniture. Because of the nature of XML, there is no standard way to display an XML document. In order to display XML documents, it is necessary to have a mechanism to describe how the document should be displayed. One of these mechanisms is Cascading Style Sheets (CSS), but XSL (eXtensible Stylesheet Language) is the preferred style sheet language of XML, and XSL is far more sophisticated than the CSS used by HTML.
Additional remarks	XSL Formatting Objects (XSL-FO) is part of XSL.
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

5.2.39 XSLT

Interoperability Area	Data Transformation for conversion from XML format to another format
Standard/Specification with Version and Publication Date (if applicable)	**XSLT 2.0** **Jan 2007**
Description	XSLT is a language for transforming XML documents into other XML documents.
Reference	http://www.w3.org/TR/xslt20/
Standards Body	W3C
Status of recommendation as per Policy	Open Standard
Maturity Level	Matured & Current
Enforcement Category	Mandatory
Other version(s), if any, which can also be considered through a Version Management Mechanism.	--
Applicability/Scope	XSLT is designed for use as part of XSL, which is a stylesheet language for XML. In addition to XSLT, XSL includes an XML vocabulary for specifying formatting. XSL specifies the styling of an XML document by using XSLT to describe how the document is transformed into another XML document that uses the formatting vocabulary. XSLT is also designed to be used independently of XSL. However, XSLT is not intended as a completely general-purpose XML transformation language. Rather it is designed primarily for the kinds of transformations that are needed when XSLT is used as part of XSL.
Additional remarks	XSLT 2.0 is a revised version of the XSLT 1.0 Recommendation [XSLT 1.0] published on 16 November 1999. XSLT 2.0 is designed to be used in conjunction with XPath 2.0, which is defined in [XPath 2.0]. XSLT shares the same data model as XPath 2.0, which is defined in [Data Model], and it uses the library of functions and operators defined in [Functions and Operators]. XSLT 2.0 also includes optional facilities to serialize the results of a transformation, by means of an interface to the serialization component described in [XSLT and XQuery Serialization].
For Interim Standard, the clauses of Policy it violates	-
History of revision with dates	-

6. Steps / Best practices for implementation of Technical standards

1. For new e-Governance projects, right from the conceptualization and design stage, the usage of listed Technical Standards in this document, and other e-Governance standards published by GoI from time to time, must be adhered to. For this purpose, , all Interoperability Areas covered under applicability of Policy on Open Standards requiring use of Standards must be identified. For the Areas covered by this document, the listed standards must be used. If any Area is not covered in this document, it should be flagged and communicated to GoI at the earliest for evaluation.
2. The project proposals /Request For Proposals (RFP) should ensure compliance to technical standards published this standard document.
3. Conformance to the identified standards in the specified Areas should be ensured during the e-Governance project life cycle using suitable mechanism in consultation with DeitY.
4. In case of Interim or Matured but Declining or Evolving standards, one should look for updates, if any from time to time.
5. New versions of legacy applications should ensure adherence to the standard specifications .

7. ANNEXURES

Annexure-I: Definitions and Acronyms

GoI's Policy on Open Standards for e-Governance' (Version 1.0 November 2010) can be referred for the definitions of the following terms:

- Designated Body
- Domain
- Interim Standard
- Maturity
- Not-for-profit
- Open Standard
- Standard

GoI's 'Manual on Implementation of Policy on Open Standards for e-Governance' (Version 1.0 November 2010) can be referred for the definition of the following terms:

- Interoperable

Definitions of other terms used in this document are as follows:

Definitions	
Matured & Current Standard	A standard which is matured and have strong ongoing support at the time of consideration.
Matured but Declining Standard	A standard which is matured and still used but receiving less support or are being superseded by an evolving standard.
Evolving Standard	A standard, which meets the maximal functional requirements and progressing towards Maturity
Mandatory Standard	The standard which is Matured and Current.
Mandatory-Watch-list Standard	The standard which is Interim or Evolving or Matured but Declining will be in watch-list and need to be reviewed periodically (at least once a year) to explore if a better candidate has become available.
Additional Open Standard	GoI shall endeavour to adopt Single and Royalty-Free (RF) Open Standard for an Area. However, in view of the sufficient technical justification and in the wider public interest, additional Open Standard(s) in the same Area may be considered by GoI based on the recommendations of the Designated Body. Such standard shall be compatible and bi-directionally interoperable with the already existing selected Open Standard.

Acronyms	
DeitY	Department of Electronics and Information Technology
GoI	Government of India
IFEG	Interoperability Framework for E-Governance
NeGP	National e-Governance Plan

8. References

This document builds on the Areas identified in 'Interoperability Framework for e-Governance' Version 2.4 prepared by working group on Technical Standards & e-Governance Architecture.

This document vets the Technical Standards for their openness as per the procedure laid down in 'Policy on Open Standards for e-Governance' (GoI notification, Version-1.0, Nov., 2010 http://egovstandards.gov.in/).

Specific references for individual standards are listed in respective tables. Some useful general references are listed below:

1.International Standards Organisation (ISO) (http://www.iso.org)

2.World Wide Web Consortium (W3C0 (http://www.w3c.org)

3.Internet Engineering Task Force (IETF) (http://www.ietf.org)

4.Object Management Group (OMG) (http://www.omg.org)

5.Xiph.org Foundation (http://www.xiph.org)

6.Unicode Consortium (http://unicode.org/)

7. OASIS (http://www.oasis-open.org/)

9. List of Contributors

Expert Committee Members

1	Prof G. Sivakumar, Dept. of CSE, IIT-B, Mumbai	Chairman of Expert Committee
2	Dr. M. Sasikumar, Director (R&D) - Corporate, C-DAC	Member of Expert Committee
3	Dr. P. Balasubramanian, Scientist-G, NIC-OTC, Chennai	Member of Expert Committee
4	Mr. T. Manisekaran, Scientist-E, NIC-OTC, Chennai	Member of Expert Committee

Other Reviewers / Contributors

1	Mrs. Renu Budhiraja, Senior Director, DeitY, New Delhi
2	Mrs. Kavita Bhatia, Scientist-E, DeitY, New Delhi
3	Mrs. Anita Mittal, Senior Consultant, DeitY, New Delhi
4	Mrs. Aruna Chaba, Senior Consultant, NICSI, New Delhi
5	Dr. V.S.R. Krishnaiah, Scientist-F, Head, e-GSD, NIC, New Delhi
6	Dr. (Mrs) Meenakshi Mahajan, Scientist-E, e-GSD, NIC, New Delhi
7	Mr. C. Senthil Kumar, RS-I, NIC-OTC, Chennai

Acknowledgements:

The contributions received from various reviewers through closed group reviews and public reviews are greatly acknowledged.