Request for proposal for Selection of System Integrator for Implementation of ICT Solutions including Establishment of City Operations Centre in Belagavi

Volume 4: Annexures

Contents

Annexures

Annexure I: Smart Traffic

Details of Junctions

S. No.	Solution Requirement	Indicative Number
1	Total Number of existing Junctions with Signal	40
2	New junctions being proposed	23
3	Total no. of Junction proposed for ATMS	20

Proposed Junctions for ATMS (d): 20 Nos.

S. No	Junction Name	Signal Type (Fixed Time Traffic Signal / Pedestrian Signal)
1	CBT Circle	Fixed Time Traffic Signal
2	Ashoka Circle	Fixed Time Traffic Signal
3	RTO Circle	Fixed Time Traffic Signal
4	Rani Chennamma Circle	Fixed Time Traffic Signal
5	Samadevi Circle	Fixed Time Traffic Signal
6	Bogarvaes Ciecle	Fixed Time Traffic Signal
7	Basaweswar (Goaves) Circle	Fixed Time Traffic Signal
8	RPD Cross	Fixed Time Traffic Signal
9	Bank of India Circle	Fixed Time Traffic Signal
10	Kolhapur Circle (Krishnadevaraya Circle)	Fixed Time Traffic Signal
11	Seth Petrol Pump Circle	Fixed Time Traffic Signal
12	Dharamnath Circle	Fixed Time Traffic Signal
13	Nathpai Circle	Fixed Time Traffic Signal
14	KLE Junction	Fixed Time Traffic Signal
15	Surabhi Hotel Junction	Fixed Time Traffic Signal

16	Ganesh Circle (RT Nagar)	Fixed Time Traffic Signal
17	Srinagar Junction Underpass	Fixed Time Traffic Signal
18	Hanuman Nagar Junction	Fixed Time Traffic Signal
19	Gogte Circle	Fixed Time Traffic Signal
20	Ramling Khind & Patil Galli Junction	Fixed Time Traffic Signal

Annexure II: Smart Polls

S. No.	Solution Requirement	No.
1	Total Number of Smart Polls proposed	9

Identified Locations for Smart Poles

S. No.	Identified Location
1	Tilakwadi 1st railway Gate
2	Goaves Circle (Basaweswar Circle)
3	Sanman Hotel Circle (On College Road)
4	DC Office & Court complex
5	Kolhapur (krishnadevaraya) Circle
6	Heritage Park
7	Fort Area
8	KPTCL Road (Smart Road)
9	Mandoli Road (Smart Road)

Annexure III: Smart Transport

S. No.	Fleet Size	Indicative no.
1	Number of Buses Covering Inter City	67
2	Number of Buses Covering Suburban	115
3	Total Bus in City Having GPS System	50 (Purchased But GPS is not working)

S. No.	Bus Terminal Points (Existing)
1	Kittur Chanama Circle
2	Kakati
3	Azam Nagar
4	Dharamveer Sambaji Circle (Cantonment)
5	Union Jamkhana (Cantonment)
6	Goaves
7	Majagaon
8	Vantamuri
9	Airport (Airport Authority)
10	Kudachi
11	Kanbargi
12	Alarwad Cross
13	SuvarnaSoudha (PWD)
14	Vijayanagar
15	Sayadarinagar
16	Kuvemunagar
17	Guruprasad Colony
18	Angol
19	Vadagaon
20	Manickbag
21	Hindwadi (Gomatesh School)
	Proposed New Smart Bus Shelters – No 10

Annexure III (a): Proposed Smart Bus Shelters

S. No	Description	Nos	Remark
1	RPD Circle	2	
2	Gogte Cirlce	2	
3	Bogarves circle	1	
4	Opposite to Shivalay garden Ramteerth Nagar	1	
5	Opposite to hotel Surabhi on gogak road	2	
6	R T Nagar - Ganesh Circle	1	
7	On Sankam road near Ashok circle	1	
	Total	**10**	

Annexure III (b): Components of Smart Bus Shelters

S. No	Item	Nos	Remark
1	Wi-Fi Routers	7	*
2	VMS	10	
3	Digital Billboards	20	**
4	Surveillance Camera	10	

** One at each bus stop (wherever 2 bus stops are proposed only 1 Wi-Fi router is proposed to be installed at such locations)*

*** Two nos. at each bus stop (one on each side)*

Annexure III (C): Bus Having GPS Offline / Camera / Bus Destination Display System

Sl.No.	Vehicle No.		GPS	Camera	Display System
1	KA 22 F	2087	YES	YES	YES
2	KA 22 F	2088	YES	YES	YES
3	KA 22 F	2089	YES	YES	YES
4	KA 22 F	2090	YES	YES	YES
5	KA 22 F	2091	YES	YES	YES
6	KA 22 F	2092	YES	YES	YES
7	KA 22 F	2093	YES	YES	YES
8	KA 22 F	2094	YES	YES	YES
9	KA 22 F	2095	YES	YES	YES
10	KA 22 F	2096	YES	YES	YES
11	KA 22 F	2121	YES	YES	YES
12	KA 22 F	2122	YES	YES	YES
13	KA 22 F	2123	YES	YES	YES
14	KA 22 F	2124	YES	YES	YES
15	KA 22 F	2125	YES	YES	YES
16	KA 22 F	2126	YES	YES	YES
17	KA 22 F	2127	YES	YES	YES
18	KA 22 F	2128	YES	YES	YES
19	KA 22 F	2129	YES	YES	YES
20	KA 22 F	2130	YES	YES	YES
21	KA 22 F	2141	YES	YES	YES
22	KA 22 F	2142	YES	YES	YES
23	KA 22 F	2143	YES	YES	YES
24	KA 22 F	2144	YES	YES	YES

25	KA 22 F	2145	YES	YES	YES
26	KA 22 F	2146	YES	YES	YES
27	KA 22 F	2155	YES	YES	YES
28	KA 25 F	3196	YES	YES	YES
29	KA 25 F	3229	YES	YES	YES
30	KA 25 F	3254	YES	YES	YES
31	KA 22 F	2131	YES	YES	YES
32	KA 22 F	2132	YES	YES	YES
33	KA 22 F	2133	YES	YES	YES
34	KA 22 F	2134	YES	YES	YES
35	KA 22 F	2135	YES	YES	YES
36	KA 22 F	2136	YES	YES	YES
37	KA 22 F	2137	YES	YES	YES
38	KA 22 F	2138	YES	YES	YES
39	KA 22 F	2139	YES	YES	YES
40	KA 22 F	2140	YES	YES	YES
41	KA 22 F	2147	YES	YES	YES
42	KA 22 F	2148	YES	YES	YES
43	KA 22 F	2149	YES	YES	YES
44	KA 22 F	2150	YES	YES	YES
45	KA 22 F	2153	YES	YES	YES
46	KA 22 F	2154	YES	YES	YES
47	KA 25 F	3250	YES	YES	YES
48	KA 25 F	3251	YES	YES	YES
49	KA25 F	3252	YES	YES	YES
50	KA25 F	3253	YES	YES	YES

Annexure IV: ICT based Solid Waste Management System

Number of wards and details of the same handled by the Corporation: 10 Wards

Number of wards and details of the same handled by the Concessionaire: 48 Wards

A. Category wise fleet size for Solid Waste Collection and Transportation

Fleet Size	
Type of vehicle	**Number**
Corporation:	
Auto Tipper (Primary Collection)	8
Push Carts + Tricycle (Primary Collection)	21
Twin Dumpers (Secondary Collection)	2
Tipper (Secondary Collection)	5
Tractor (Secondary Collection)	0
Concessionaire	
Auto Tipper (Primary Collection)	42
Push Carts + Tricycle (Primary Collection)	13
Twin Dumpers (Secondary Collection)	0
Tipper (Secondary Collection)	45
Tractor (Secondary Collection)	0

B. Surveillance for Commercial Areas for Waste Monitoring / Waste Treatment Site

Sl. #	Location Type	No of Cameras
1	Land Fill Site + internal Garbage Sorting	6
2	Weigh Bridge	2
Sl. #	**Commercial Area**	**No of Cameras**
1	Market	10
2	Function Halls& other commercial Areas	10

C. Black Spot Locations in which cameras need to be installed: 20 nos.

S. No.	Ward No.	Name & No. of Black spots	Stage
1	7	Dhanshree Garden cross No 3 & 4 Bhagya Nagar	P
2	8	Deshmukh Road Near Belgaum Club	P
3	8	Khanapur road, near Indian oil corporation Ltd.,	p
4	23	Old P B Road Joshi Mal Corner Khasbag Belagavi	P
5	25	Near Beat Office Kacheri Galli Shahpur Belagavi	P
6	26	Kapileshwar main road, Near Bhatkande School, nala side	P
7	26	Renuka Hotel Container, 1.1 mt.sq.	P
8	28	Ramlingkhind, Near Hotel Raj mahal	P
9	28	Hotel Lalit bar, Mujawar galli	P
10	29	Near Ushatai School, patil galli	P
11	29	Trunk road, Dumper placer, 3.5 sq.ft.	P
12	30	Sheri galli	P
13	31	Ginde B.P. Kelkar bag	P
14	32	Kaveri cold drinks, Naragundkar bhave circle	P
15	32	Naragundkar Bhave Circle	P
16	40	Kakatives, Infront mahila aghadi biriyani hotel	p
17	40	Kakatives road near Govt. School	p
18	44	KP TCL Road	P
19	44	Sukh Sagar Opp	P
20	51	KEB Road, Azad nagar	P

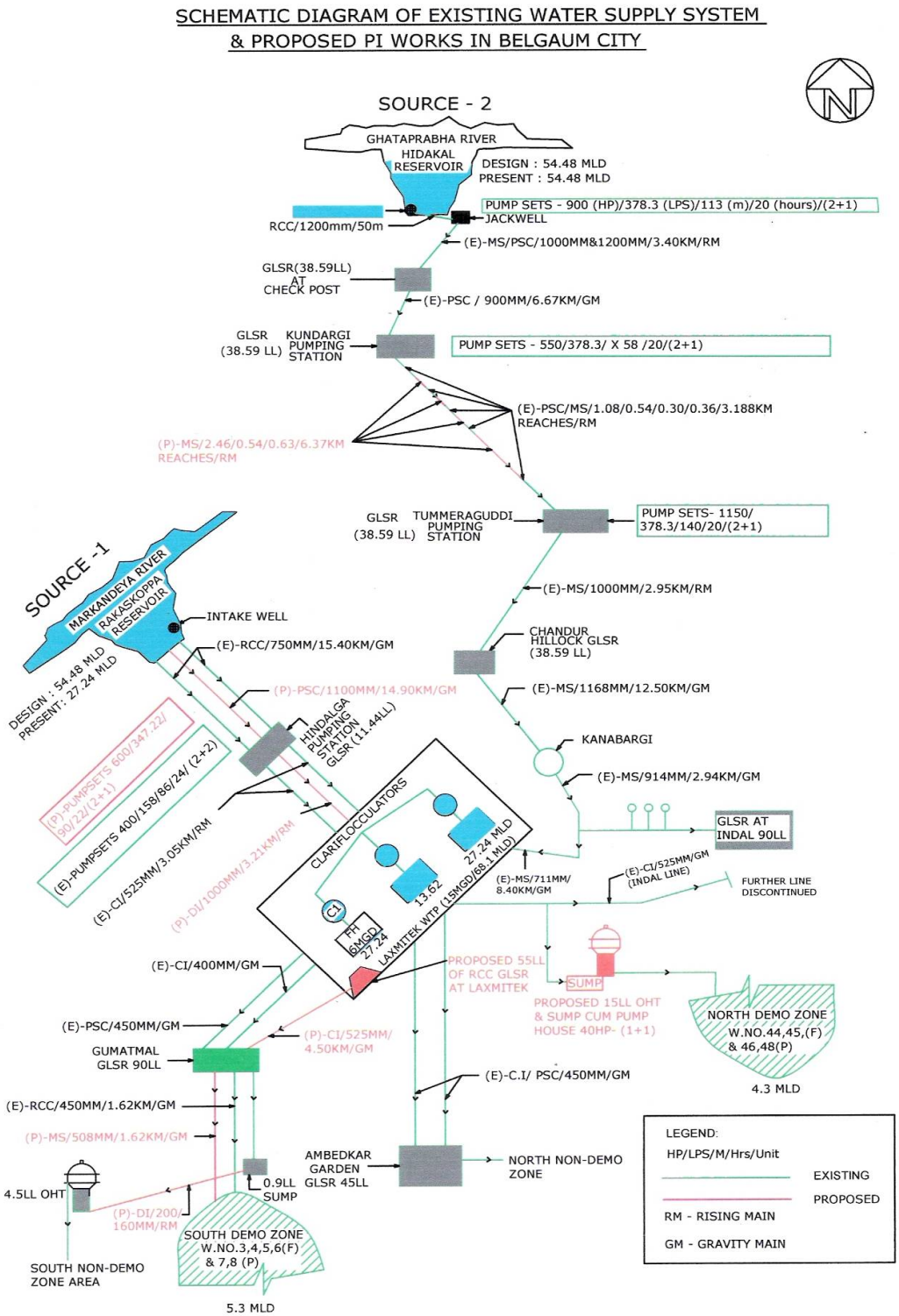
Note: P- Primary Collection

D. Location of the Waste treatment and Disposal Facility

	Details of Load cell
Waste Collection Point	Sy. No. 19, 40 and 42 of Turamuri village, Belgaum Taluk

Annexure V: ICT based Smart Water:

Schematic diagram of the entire Water Supply scheme from the Source to WTP to the GLSRs to be provided .Mapping of the entire existing assets like existing Bulk Flow meters, Pressure sensors, Quality Sensors needs to be provided on the schematic diagram



Details of Existing Assets (Bulk Meters)

No	Details of Location	Make/Type	Functional/ Non functional	AMR Ready/ Not Ready
Existing Bulk Flow Meters				
1	Main Bulk Water Meter (400 mm) at Node no 0002 Gummmatmal GLSR Hindwadi	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
2	Bulk Water Meter (160 mm) at Node no 0005 Adarsh Nagar	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
3	Bulk Water Meter (110 mm) at Node no 0019 Adarsh Nagar	ABB WaterMaster Electromagnetic Flowmeter	Functional	AMR Not Ready
4	Bulk Water Meter (160 mm) and PCV at Node no 1704, 4th cross Bhagya Nagar	ABB WaterMaster Electromagnetic Flow meter	Functional	AMR Not Ready
5	Bulk Water Meter (200 mm) and PCV at Node no 0017, Angol Main Road	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
6	Bulk Water Meter (150 mm) and PCV at Node no 3804, Annapurnawadi	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
7	Main Bulk Water Meter (400 mm) at Node no 0001 TB Ward OHT	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
8	Bulk Water Meter (150 mm) and PCV at Node no 0021 , Near BSNL office	ABB Water Master Electromagnetic Flow meter	Transmitter Not Working	AMR Not Ready
9	Bulk Water Meter (200 mm) and PCV at Node no 0022 , Near Akshay Cafe	ABB Water Master Electromagnetic Flow meter	Transmitter Not Working	AMR Not Ready
10	Bulk Water Meter (150 mm) and PCV at Node no 0028, Near KSRP Qtrs	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready
11	Bulk Water Meter (150 mm) and PCV at Node no 0016, Vaibhav Nagar	ABB Water Master Electromagnetic Flow meter	Functional	AMR Not Ready

Details of Bulk Flow Meters: 14Nos.

S. No	Location	Inlet	Outlet
1	WTP Laxmitek	1) Filter House No. 1 – Pump Line a) 600 HP Pump Line b) 400 HP Pump Line 2) Filter House No. 2 3) Filter House No. 3	1)District A Old Line 2) District B Old Line 3) District A New Line 4) District B New Line 5) MES Colony 6) VTU Colony 7) Cantonment 8) 24/7 – TB Ward 9) 24/7 - TB Ward 10) Sambra Line 11) Buda 12) Hindalga 13) Hindalga 14) Freedom Fighter colony

Details of New Assets

No	Type	Quantity
1	AMR Bulk Flow meters	14
2	Pressure Sensors	Not required
3	Quality Sensors (Turbidity, Ph& Chlorine)	6

Annexure V: Smart Parking (Future Solutions to come in as a Service to City Operation Center/Common Command Center):

Type of vehicle	Number
Closed Parking	1 (Central Bus Terminal)

Annexure VI: City Surveillance (Future Solutions to come in as a Service to City Operation Center/Common Command Center):

Indicative List of City Surveillance Locations which are being monitored at Police Surveillance Center and it has to come as live feed into CCC/CoC

	List of Camera Given by Police Department Belagavi	
Sr. No.	**Department**	**Qty**
1	Market Sub Division	49
2	Law & Order Point of View Khadebazar Sub -Division	37
3	Traffic Point of view South Camp	60
4	Khade Bazar Sub Division Hyper Sensitive Places	396
5	Khade Bazar Sub Division Sensitive Place	270
6	Khade Bazar Sub Division Normal Place	30
7	Traffic Point of view South Camp	137
8	**Market PS**	
	Hyper Sensitive Area	140
	Sensitive Area	138
	Normal Area	70
9	**Shahapur PS**	
	Hyper Sensitive Area	72
	Sensitive Area	54
	Normal Area	38
10	**APCMPS**	
	Hyper Sensitive Area	84
	Senstive Area	60
	Normal Area	38
11	**Malmaruti PS**	
	Hyper Sensitive Area	120
	Senstive Area	75
	Normal Area	40
	Total Cameras	**1908**

Annexure VII : Ambulance (108) & Fire engines (102) Details in which GPS device have to be installed

S.No	Description	Nos.
1	No .of Ambulances	97
2	No. of Fire engines	05

Annex-A (BioMetrics Standard)

1. BioMetrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

2. Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt ISO /IEC 19794-5:2005(E). While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

3. <u>Fingerprint Image and Minutiae Data Standard</u>

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.

It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

4. <u>Iris Image Data Standard</u>

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.

In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre-processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of both eyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

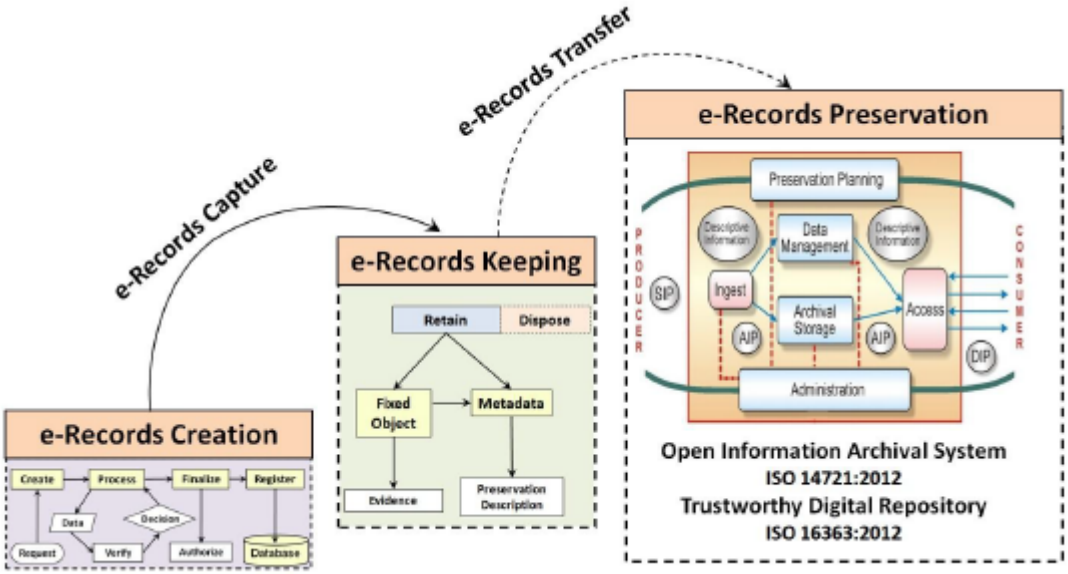
Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available.

	○ Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: ○ Support for JPEG2000 image compression ○ Support for transparency effects and layers ○ Embedding of OpenType fonts ○ Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard ○ Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

Annex-C (Localisation and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardization is one of the baselines to be followed in localization. Standardization means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardization becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

2. Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard. The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

3. **Unicode shall be the storage-encoding standard for all constitutionally recognized Indian Languages including English and other global languages as follows:**

Specification Area	Standard Name	Owner	Nature of Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future up gradation as reported by Unicode consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

- **Character**: Character is the smallest component of any written language that has semantic value.
- **ISCII**: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages. Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.
- **Unicode**: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

4. **Unicode vis-à-vis ISO10646**

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognized Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardization (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

1. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible with each other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font): A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format): OFF fonts allow the handling of large glyph sets using Unicode encoding. Such encoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

Annex-D (Metadata and Data Standards)

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

Rerefrence Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. **Creation of Mobile Services Delivery Gateway (MSDG)**

   MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

   Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

   To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

   a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

   b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to

the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. Guidelines to deliver public services round-the-clock to the users using m-Governance
b. Guidelines to develop standard based mobile solutions
c. Guidelines to integrate mobile applications with common e-Governance infrastructure

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILE SEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

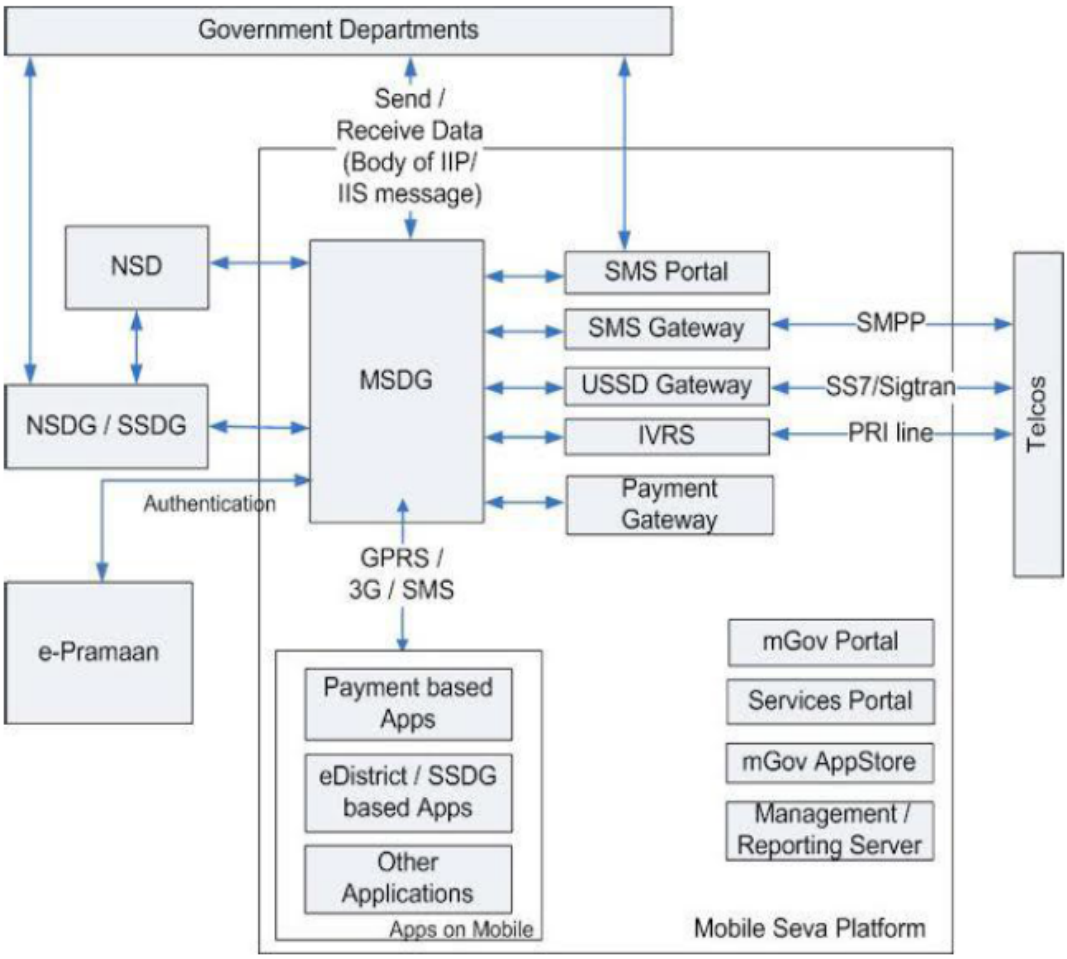


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

Mobile Application (m-Apps)

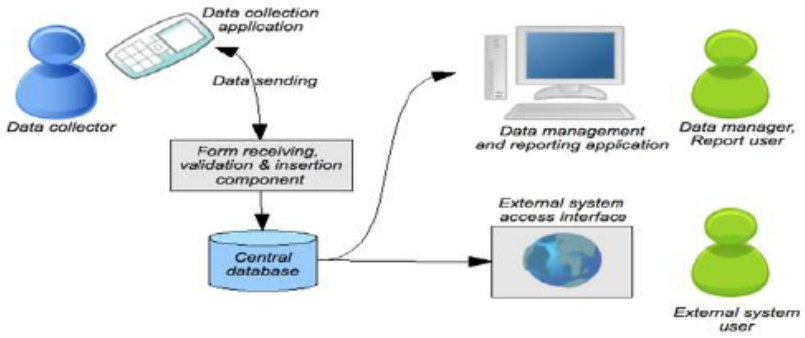
Mobile application software is applications software developed for handheld devices, such as mobile phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**

   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**

   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:



The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

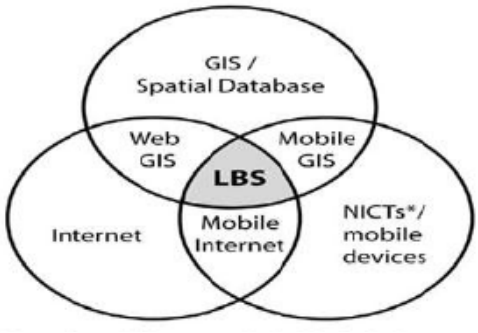
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.

It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.

A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

- **Text entry standards (i.e. keypad)**
- **Encoding standards to support all the major Indian languages**
- **Font support standardization for handsets to send & receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**

b. **Screen-assisted text inputting mechanisms available from few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Although efforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver's mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver's mobile number and MMID, and transfer the funds to the receiver's account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone's screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

Annexure-F (GIGW) Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarized form. Further, the search engines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official

government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.

b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any

changes, updates / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those

who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the "Policy on Open Standards for e-Governance" and "Technical Standards on Interoperability Framework for e-Governance".

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India" (hereinafter referred to as the "Policy") will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government's approach on the use of "Open APIs" to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.

ii. Enable quick and transparent integration with other e-Governance applications and systems.

iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.

iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.

v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.

ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.

iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.

iv. The Government organizations shall make sure that the Open APIs are stable and scalable.

v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organization shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.

vi. A Government organization consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorization through a process as defined by the API publishing Organization.

vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.

viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.

ix. The life-cycle of the Open API shall be made available by the API publishing Government organization. The API shall be backward compatible with at least two earlier versions.

x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organizations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

Annex-H (Internet of Things)

1. **Sensor & Actuators**
    a. **IEEE 1451:** IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.
    b. **Identification Technology: ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques.** It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.
    c. **Domain Specific Compliance:** Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. **Communication Technology**
    a. **Thread:** Networking protocol called Thread that aims to create a standard for communication between connected household devices.
    b. **AllJoyn:** Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.
    c. **IEEE 802.15.4:** It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs). IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006
    d. **IETF IPv6 over Low power WPAN (6LoWPAN):** It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
    6LoWPAN Frame Format
    Fragmentation and Reassembly
    Header Compression
    Support for security mechanisms
    e. **IETF "Routing Over Low power and Lossy (ROLL):**
    IPv6 Routing Protocol for Low power and Lossy Networks (LLNs)

(RPL) RPL Topology Formation
(Destination Oriented Directed Acyclic Graphs - DODAGs)
RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):** It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. Use Case/ Application Specific:

i. **Industrial IoT (IIoT):** Object Modeling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modeling
- Structured Assurance Case Metamodel
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modeling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. **Consortia**

   a. **Open Interconnect Consortium:**

   OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

   b. **Industrial Internet Consortium:**

   It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. **Architecture Technology**

   a. **IEEE P2413: Standard for Architectural Framework for Internet of Things**

   The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

   The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. **Further Readings for Standards**

   a. **ITU Standardization Roadmap**

   This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities.It includes Standards/ITU-T Recommendations relatedto Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

   b. **IERC Position Paper on IoT Standardization:**

   It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

Annex-I (Smart Parking)

The following standards and certifications need to be followed:

1. **Entry Device**
    i. Communication protocol should be TCP/IP
    ii. Conform ISO 9001 Quality Assurance Standard
    iii. CE, FCC, IC, CNRTLUS certified
    iv. Degree of protection based on IEC 60529: IP43
2. **Exit Device**
    i. Conform ISO 9001 Quality Assurance Standard
3. **Entry/Exit Barrier**
    i. The Barrier unit must conform to ISO 9001 Quality Assurance standards
    ii. CE, Ukr-Sepro certified
    iii. Degree of protection: IP34D
4. **Sensors**
    i. Conform ISO 9001 Quality Assurance Standard
    ii. Protection Level: IP67
5. **Parking light aisle indicators**
    i. Conform ISO 9001 Quality Assurance Standard
    ii. Protection Level: IP55
6. **Indoor LED indicators**
    i. Conform ISO 9001 Quality Assurance Standard
    ii. Protection Level: IP33
    iii. Communications: Bus RS-485
7. **Other Technical Specifications**

Annex-J (Public WI-FI)

1. **All equipment must support the following standards/capabilities:**
    i. 802.11n
    ii. 802.11ac
    iii. 802.11e Quality of Service (QoS)
    iv. WMM Wireless Multimedia Extensions
    v. WMM Power save
    vi. 802.11h Dynamic Frequency Selection and Transmit Power Control
    vii. 802.11i Security, including AES
    viii. 802.1X with dynamic VLAN policies
    ix. WPA2-Enterprise certification
    x. 802.11r Roaming
    xi. preferred: 3X3 MIMO
    xii. preferred: Polycom/SpectraLink VIEW Certification, SpectraLink Voice Priority
    xiii. preferred: Wi-Fi Certified Voice-Enterprise

2. **Wireless Access points specs**
    i. Shall be IEEE 802.11ac compliant concurrent dual radio access point.
    ii. Shall feature a three spatial-stream 802.11ac (3x3 MIMO) integrated or external dual band (2.4GHz & 5GHz) antenna.
    iii. Shall have 802.3af or 802.3at compliant Gigabit PoE UTP port and a console port.
    iv. Shall be IEEE 802.3af PoE compliant and both the radios shall operate at full power and full performance on 802.3af PoE/Gigabit Ethernet.
    v. Shall be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g/n/ac client devices.
    vi. Shall support up to 16 SSID/VSC profiles.

vii. Shall support simultaneous detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.

viii. Shall support both centrally managed mode (configured and updated via a controller) and autonomous mode (standalone in the absence of a controller).

ix. Shall support auto-selection of RF channel and transmit power.

x. Shall support enforcement of client authorization based on user credentials (802.1X/EAP), and hardware identifiers (MAC address, WEP key).

xi. Shall support ACS or similar feature to reduce co-channel interference (CCI) by automatically selecting an unoccupied radio channel.

xii. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

xiii. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services

xiv. Must support up to 23dbm of transmit power in both 2.4 GHz and 5 GHz radios.

xv. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

Annex-H (Disaster Management)

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 - *Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

Annex-I (Cyber Security)

All the solutions proposed shall follow the cyber security model frame work prepared by national Security Council secretariat. Please refer MoUD OM K-15016/61/2016-SE-1 dated 20th May 2016