Interoperability Framework for e-Governance (IFEG)

Version 1.0

October 2015

Government of India

Department of Electronics and Information Technology

Ministry of Communications and Information Technology

New Delhi – 110 003

Metadata of a Document

S. No.	Data elements	Values
1.	**Title**	Interoperability Framework for e-Governance (IFEG)
2.	**Title Alternative**	Interoperability Framework for e-Governance (IFEG)
3.	**Document Identifier**	IFEG
4.	**Document Version, month, year of release**	Version 1.0, Oct, 2015
5.	**Present Status**	Draft.
6.	**Publisher**	Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT), Government of India (GoI)
7.	**Date of Publishing**	October, 2015
8.	**Type of Standard Document** *(Policy / Framework / Technical Specification/ Best Practice /Guideline/ Process)*	Framework
9.	**Enforcement Category** *(Mandatory/ Recommended / Advisory)*	Advisory (for all public agencies)
10.	**Creator**	Department of Electronics and Information Technology (DeitY)
11.	**Contributor**	DeitY, NIC.
12.	**Brief Description**	Purpose of Interoperability Framework for e-Governance (IFEG) is: • To provide background on issues and challenges in establishing interoperability and information sharing amongst e-Governance systems. • To describe an approach to overcome these challenges; the approach specifies a set of commonly agreed concepts to be understood uniformly across all e-Governance systems. • To offer a set of specific recommendations that can be adopted by various stake-holders to pro-actively address the challenges in interoperability.

S. No.	Data elements	Values
13.	**Target Audience** *(Who would be referring / using the document)*	◦ Public agencies (including policy decision-makers and governing bodies of IFEG) ◦ Providers of e-Services ◦ Citizens ◦ ICT industry (playing the roles of suppliers, developers, implementers and maintainers) ◦ Academia and Research Institutes ◦ Standards Bodies (including Apex Body for e-Governance, Expert Committees, Working Groups, Task Forces, Specialist Committees at the National level and also International Organisations)
14.	**Owner of approved Framework**	DeitY, MCIT, New Delhi
15.	**Subject**	Interoperability Framework
16.	**Subject. Category**	Adoption Framework
17.	**Coverage. Spatial**	INDIA
18.	**Format**	PDF
19.	**Language**	English
20.	**Rights. Copyrights**	DeitY, MCIT, New Delhi
21.	**Source** *(Reference to the resource from which present resource is derived)*	Different resources, as indicated in the document
22.	**Relation**	NIL

Preamble

Government of India is rapidly advancing in e-Governance through various Mission Mode and other e-Governance Projects designed to efficiently deliver services to citizens. However, ensuring Interoperability amongst various e-Governance systems and applications is very important. Without the assurance of interoperability, citizens will have fragmented interactions with several agencies. These largely uncoordinated interactions with limited coherence will significantly degrade the quality and effectiveness of service delivery contrary to the Government of India's (GoI) vision and intent.

This document provides the overarching framework, IFEG, required to achieve interoperability amongst e-Governance applications. After a brief Introductory chapter setting the context, it addresses in detail the current scenario and challenges at each layer (organisational, semantic and technical) and makes specific recommendations in respective chapters on how to address them. It concludes by recommending an action plan and a way forward.

Content

1 Introduction

Government of India (GoI) is implementing the Digital India programme as an umbrella programme to prepare India for a knowledge based transformation into a digitally empowered society and knowledge economy. Under the over-arching vision of Digital 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 a 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. In this context, it is important to ensure interoperability amongst various e-Governance systems to upgrade the quality and effectiveness of service delivery.

The National e-Governance Plan (NeGP) of the Government of India takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is being developed, and large-scale digitization of records is taking place to enable easy and reliable access over the internet. Public Service is “any service or part thereof being provided to any person by the Central Government and the State Government or public authority either directly or through any service provider and includes the receipt of forms and applications, issue or grant of any license, permit, or certificate, sanction or approval and the receipt or payment of money by whatever name called in a particular manner”. The ultimate objective is to bring such public services closer to home; as articulated in the vision statement of NeGP: "Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man".

Currently, the citizen has to interact with more than one public agency to avail a service. Most of the e-Governance systems & databases are established in silos as per the specific requirements of the individual public agency. These public agencies have limited coherence and interactions remain largely uncoordinated. The projects often span the **three-tier** Indian administrative architecture of Central, State and Local-Body public agencies. The establishing of interoperability among these systems is one of the most urgent and important challenges.

Today there are increasing public expectations for transparency, openness, and communication. For many industries and government organizations, meeting these expectations means exploring new tools and practices that help foster innovation, drive efficiency, and create economic benefits—for end customers, constituents, and communities. Standards are one of the many tools that can be used to help foster interoperability among products or services within a market, and when they are responsive to real marketplace needs they can help promote innovation, fuel market growth, and protect investments in new technologies. ICT standards are tools that help vendors—including hardware and software providers—develop products and services that work together better for users, and enhance interoperability among different technologies and processes.

1.1 Purpose of IFEG

The purpose of Interoperability Framework for e-Governance (IFEG) in Indian context is

- To provide background on issues and challenges in establishing interoperability and information sharing among e-Governance systems.
- To describe an approach to overcome these challenges; the approach specifies a set of commonly agreed concepts to be understood uniformly across all e-Governance systems.
- To offer a set of specific recommendations that can be adopted by various stake-holders to pro-actively address the challenges in interoperability.

1.2 Expected Impact of IFEG:

- Enable systems to inter-operate efficiently and effectively with other systems across various domains of e-Governance.
- Ensuring Consistency that information exchanged is interpreted and processed unambiguously in all the interacting-systems at all the time.
- Ensuring better sharing of ICT infrastructure; reproducibility and reliability of the data collected or encoded at various sources.
- Compliance to the Policy on Open Standards by adopting the formats, standards and specifications as per policy for better interoperability.
- Enable autonomous development for systems within the principles of various levels of interoperability.
- Adoption of principles of Service Oriented Architecture (SOA) to enable integration of dissimilar technologies.
- Offer e-Services (including G2C, G2B, G2G, G2E) to concerned stake-holders through a single window (or one-stop delivery or one service window), but through multiple delivery channels like PC, Mobiles and Common Services Centres (CSC).

1.3 Applicability of IFEG

- Applicability of the IFEG shall include all planned e-Governance systems and Disaster Recovery (DR) Management systems from all the public agencies.
- When to comply
  - new implementation of e-Governance systems
  - up-gradation of existing e-Governance systems
  - release of new version of IFEG
  - change of overall technology strategy
  - All existing e-Governance systems after the transition period announced.
- Scope of Compliance

- Interface level where exchange of information occurs
- Data Archival / Storage level

- Nature of Compliance
  - Advisory (for all public agencies)

1.4 Targeted Stakeholders

- Public agencies (including policy decision-makers and governing bodies of IFEG)
- Providers of e-Services
- Citizens/Public at large which are users of e-Governance Services
- ICT industry (playing the roles of suppliers, developers, implementers and maintainers)
- Academia and Research Institutes
- Standards Bodies (including Apex Body for e-Governance, Expert Committees, Working Groups, Task Forces, Specialist Committees at the National level and also International Organisations)

1.5 Exemptions

- Any request for exemptions from IFEG can be granted if:
  - The current version of IFEG does not meet the requirements of the e-Governance system or
  - The reasons for the exemptions contribute to the revision of IFEG significantly.
- When an exemption is granted to any agency from confirming to IFEG, the exemption is not generic; the exemption is specific in reference to
  - A specific e-Governance system (not all systems of the agency/sector)
  - Specific e-Governance processes (not the entire ICT environment of the agency/sector)
  - Specific time period (temporarily, but not perpetual)

1.6 Outcomes of non-compliance of IFEG

The e-Governance systems that are, as whole or in part, non-compliant with IFEG are subject to the following restrictions:

- Interfaces with such systems may not be supported; i.e. e-Governance systems seeking to link to public information infrastructure facilities (like SWAN, SDC, NDC) will be refused connection.
- Use of core components will be restricted.

1.7 Challenges and Issues in the Current Situation for adopting IFEG

- Lack of a single centralised coordinating agency to manage the implementation of IFEG.
- Lack of enforcement policies and guidelines on the adoption of IFEG.
- Lack of awareness on complexity of IFEG implementation.
- Shared elements and common processes are not identified during the architecture stage and resolving these interoperability issues at later stage is very difficult.
- The incompatible e-Governance infrastructure (including wide-varying platforms and their frameworks & software, non-standard data formats for archiving & exchange, disparate hardware-systems and unreliable network-systems) may pose a great challenge.
- In most of the cases, the coordination among the concerned public agencies is very poor due to various reasons like wide-varying working nature, the lack of proper understandings (on Quality of Service, etc.) and mutual commitments.
- Accessibility of information syntactically and semantically from one e-Governance system to another e-Governance system is not easy due to the use of varying formats, structures and meanings. The wide use of different types of data-models, processes & rules, time-bases and user-interfaces in the e-Governance systems make interoperability a difficult task.
- The non-availability of adequate funding for efforts & facilities needed for adopting interoperability is one of the major constraints in public agencies. Thus an effort has to be made to make use of reusable components while designing the e-Governance systems so that the cost of software development can be reduced.
- **Process changes**, and extensive **staff and user trainings** needed for the adoption of interoperability are rarely considered.
- Addressing of contrasting-requirements like dissemination of information under legal requirements (like compliance to RTI) and rules related to data protection (like privacy, IPR) is yet another challenge.
- Sensitivity of data, differences in culture, working practices, issues of trust, timings, collaboration, work-flows, convincing stake-holders, legal issues, levels of political support and technical approach among public agencies may also pose problems for implementing interoperability.
- Cultural and linguistic diversity in India introduces additional administrative constraints like naming conventions, multiple local official languages, language-dependent format, etc.

2 Concepts, Principles and Structures

2.1 Interoperability

Interoperability in e-Governance is defined as "the ability of different systems from various stakeholders of e-Governance to work together, by communicating, interpreting and exchanging the information in a meaningful way". The interactions between all stake-holders are achieved, by sharing of information and knowledge through the business processes they support.

Inter/Intra organisational sharing of information is basic requirement of e-Services delivery in Federated Governance structure.

There are three primary goals associated with achieving interoperability in any system (computer or otherwise) i.e.

- Data exchange through Infrastructure and Software (Technical ability of software / hardware used by different systems to exchange data through common data exchange protocols, development of software necessary for management of data connections, creation of user interfaces in order to enable communication between different organisations).
- Meaning exchange (Ability of different systems / organisations to understand exchanged data in same way through a mechanism allowing the presentation of service data and data definitions).
- Process agreement (Ability of organisations to provide services to other organisations or their clients, It ensures services agreements and their legalisation).

2.2 Interoperability Framework for e-Governance

IFEG in Indian context would encompass agreed approach to be adopted by the public agencies that wish to work together towards the joint delivery of public services using ICT, to achieve above mentioned goals, namely exchange of data, meaning of exchanged data and agreed process.

An IFEG involves a common structure which comprises a set of standards and guidelines; the structure can be used by the public agencies to specify the preferred way that all stake-holders interact with each other to share the information. It is synonymous to speaking a common language.

2.2.1. Levels of Interoperability

The interoperability levels related to the sharing of information in IFEG are mainly classified into

- Organisational Interoperability (like process-re-engineering including Government-Orders, Process Changes, Organisational Structures),

- Semantic Interoperability (Enabling data to be interpreted & processed with the same meaning, etc.) and
- Technical Interoperability (like technical issues in interconnecting ICT systems and services, information storage and archival, protocols for information exchange and networking, security, etc.); in general, technical interoperability was considered for classifying the standards into various layers or domains (eg. Presentation domain, Network domain, Data Interchange domain, etc.) in earlier versions of IFEG/GIF documents from various countries.

Figure 1.2 provides an overall view of the levels of the interoperability system. This helps to define the way in which applications and re-usable services will be developed and their interaction with other ICT systems. As indicated in the Figure 1.2, Organisational Interoperability is supported by Semantic Interoperability, which in turn is supported by Technical Interoperability. Hence Technical Interoperability forms the basis for the IFEG. Governance facilitates and enforces the implementation of IFEG.

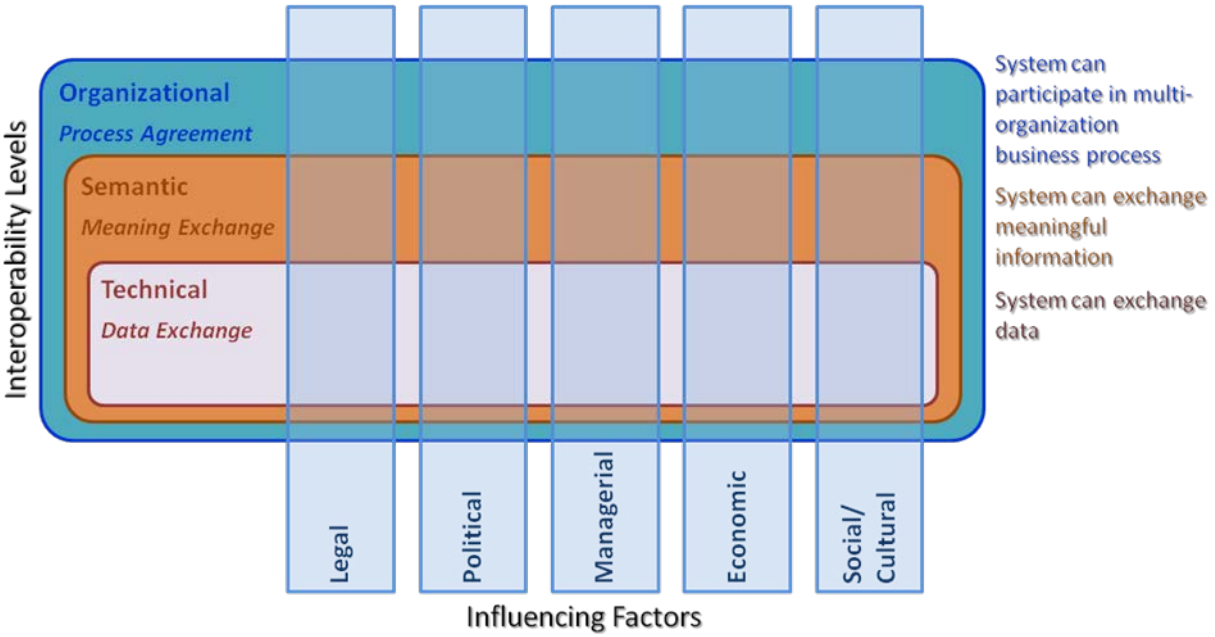

Figure 1.2: e-Governance Interoperability Model

The Multilateral mechanism for IFEG is influenced by the following key sub-areas:

- Political – For strategy related issues. In Political context, support and commitment from authority, provisioning of policies / guidelines, strategies over different levels of interoperability are expected.
- Legal – For issues like IPR / Copy Right, content regulation, privacy, freedom of information, electronic identities, etc; these are context-sensitive. Legal factors include legal-power assigned to system for data protection and privacy information of the citizen, governance issues related

to information management, executive orders and laws related to e-Governance services, citizen services driven by administrative procedures, enforcement, etc.

- Managerial – For issues like training, motivation, reorientation of concerned staff from public agencies.
- Economic – For funding related issues.
- Social/Cultural – For social/cultural characteristics of system stakeholders. Social / Cultural factors like differences in culture, working practices, issues of trust, timings, social exclusion issues have more influence. Cultural and linguistic diversity in India introduces additional administrative constraints like naming conventions, multiple local official languages, language-dependent format, etc.

This mechanism should be defined (i) with transparent, consensual, collaborative open-environments and (ii) also through the participation from all stakeholders.

When an e-Service initiative involves more than one public agency, there is a need for a commonly-agreed project plan before committing a budget for the initiative. Clear-cut roles, responsibilities and accountabilities of all stake-holders should be defined and maintained. Also adequate organisational resources should be provisioned and capabilities for implementing IFEG should be imparted through capacity building.

The e-Governance initiatives should be aligned with (i) e-Governance Strategy of the Government (ii) legal requirements (data protection and privacy information of the Citizen, etc.), (iii) administration & custodianship of public agencies with reference to information management, (iv) executive orders and laws related to e-Governance services, (v) Citizen Services driven Administrative Procedures Enforcement, etc.

3 Interoperability Levels:

3.1 Organisational Interoperability

Organizational Interoperability enables a multilateral mechanism to ensure proper management and implementation of IFEG by identifying and addressing any possible barriers (including legal, political, managerial and economic). Multilateral mechanism means organisational structures, appropriate processes, adequate resources, facilities, autonomy and authority.

For coordination and managing implementation of IFEG it is necessary to have a cross-departmental **organizational structure** which has clear set **processes**. By setting up these processes and activities, interoperability can be achieved both at strategic and technical level. The organisational structure widely used is established in two ways:

- **Inter-agency and inter-ministry committee:** This committee will be responsible for defining the enforcement policies for their department. This committee will ensure that the IFEG policy and standards are applied within the department/ministry.
- **Operational group:** This group will be responsible for executing and implementing IEFG and report to the concerned inter-ministry committee. The group will predominantly handle the technical adoption of IFEG. The group should be managed by persons with technical background of ICT and ICT project management methodologies. The group would also coordinate and provide support to ICT projects and agencies related to interoperability.

3.1.1 Steps for Achieving Organizational Interoperability

3.1.2.1. User identification standardisation

Today, one has to log in separately and get authenticated separately for each service provided by different agencies. Every portal and every agency follows their own local methods for these. Authorisation to perform specific task is an even more complex hurdle even if one shares log-in; because each agency have their roles and access management structure. In a sense, it is almost like visiting a number of independent offices, except for the travel in cyberspace.

Addressing the challenge posed by use of different user identification is a major task in itself. Given the federated multi-tier structure with a fair degree of autonomy among the different public agencies, it may need to allow some flexibility in how the different entities function. This may affect the set of roles and their inter-dependencies. For the general problem of multiple user profiles for multiple services, broadly there are two solutions.

1. One is to use a global identification scheme, as proposed by the UIDAI of the Government of India. All agencies can either use this as their primary identification, or minimally accept this as an alternate identification. This would depend on the availability of such a globally accepted scheme and effective delivery of such a scheme to all relevant services. Where this is possible, this would enable a single sign-on for a given user, to any chosen service. This is the most preferred option for addressing the multiple profile issue. Frameworks to support

single sign-on are commonly available today, so that, this is more a matter of organisational policy, than a technical challenge.

2. Another approach is to provide a registry service providing mapping among the different known schemes. This is harder to implement and scale up in the longer run; but has the advantage that individual applications do not need major modifications.

3.1.2.2. Standardisation of Processes

- One of the ways to bring Interoperability is to standardise processes; each public agency will identify the list of unique processes for their activities for standardisation.
- The standardised processes should be made as e-Processes or e-Services and shared with other stakeholders by the respective public agency through a Process Agreement.
- List of information on input, output and internal operations of each process/service will be shared with others.
- Providing sub-level processes for each of the "constituents of the IFEG" (Standards, Protocols, Policies, Guidelines and Technologies) including ownership, definition, development, maintenance, monitor, promotion, implementation, periodical review, support (RFP level, technical, etc.), changes in management life cycle required in IFEG, audit, compliance, issue resolution (including disputes, legal, political)
- Providing compliance guidelines and check-list.

3.1.2.3. Information ownership matrix

One of the major factors hindering Interoperability among public agencies is the ownership of data. When a specific piece of data – say date of birth, medical record, land ownership, income information, etc – is shared with another application, one could lose control on the data. To avoid and minimise such concerns, it is useful to publish a public document, assigning ownership and modification rights to various types of information data that one deals with in governance. Such a matrix may list these data types and assign the ownership and modification rights to specific departments, under specified conditions. The conditions may include taking concurrence from other stake-holders, and filing a copy for information in specified places.

3.1.2.4. Process Agreement

It is important to have Process Agreement, similar to SLA, by concerned public agency with key stakeholders to establish a common understanding on reviews, artefacts, Do's & Don'ts, templates and conformance conditions of the e-Governance system. The approved Process Agreement can be provided to concerned stakeholders as part of a request for proposal (RFP). As an input to the proposal, the Process Agreement helps to scope the expected work and

also the time-frame for completion. Generally, Process Agreement is to be completed during the initial phases of Project Planning and Monitoring Life Cycle. Views of various stakeholders, including ICT Industry can be considered at this stage.

Process Agreement can deliver a number of benefits including faster decision-making, transparency in decision-making, easy prediction of the timing of key stages, clearer lines of communication between authority and applicant and effective & earlier engagement of key stakeholders.

3.1.2 Challenges in achieving Organizational Interoperability

1. The Interoperability of e-Governance systems involves much more than technical specifications of data formats and protocols. In most cases, the systems belong to different organisational entity, developed using different process models, and may be positioned in different cultures. Ensuring Interoperability in such a scenario, need to consider organisational issues. Organisational Interoperability is generated by many factors, which can be grouped into:
    - Non-transparent work-flows within each agency.
    - Non-transparent processes within each agency.
    - Local design and implementation of filing and tracking methods: Usually, each agency has their own file-number, application number and even user identification which do not have any utility for other agencies.
2. Addressing such Organisational Interoperability issues is more challenging compared to the case of Technical Interoperability; this is due to difficulties in addressing its concepts which have large scope for interpretation in multiple ways:
    - Resistance & reluctant to change to new process & data from the existing process & data due to the fear of loss of control.
    - Lack of additional incentives to the particular individual-involved in order to cooperate with other stake-holders.
    - Lack of additional budget allocation to introduce new activities which are outside the conventional program.
3. In general, Organisational Interoperability includes a number of dimensions
    - Political and human issues.
    - Legal matters.

3.2 Semantic Interoperability

Semantic Interoperability addresses the requirement of understanding the meaning of data by different stakeholders in same way, while exchanging data.

The purpose of Semantic Interoperability is to build the capability of all stakeholders involved in the delivery of e-Services, with the following functionalities:

a. Discover information-requirements for the delivery of quality e-Services.

b. Explicitly describe the meaning of data to be shared multilaterally among the stakeholders.

c. Process the received-information in a manner consistent with its intended-purpose.

Basic elements of Semantic Interoperability are:

- Semantic description of data, which may have contextual meaning
- Semantic Mediation to resolve conceptual meanings differences, while exchanging data
- Semantic discovery of desired assets for seamless exchange of data

Semantic interoperability will require an agreement on the precise meaning of exchanged information among the e-Governance systems for the delivery of integrated e-Services. For this purpose, there is a need for building centralised repository of Semantic Interoperability Assets like:

- XML schema for meta-data of data elements for uniformity in data storage formats of common generic data elements.
- Code lists for controlled values.
- Ontology of common generic data elements in corresponding applications along with its contextual meaning (precise meaning, concept, attributes, constraints, restrictions, business rules, etc.)
- Taxonomies for classification of data.
- These assets would be built by identified domains within application-sectors. To ensure uniform mechanism for creation of the repository of the above assets, a prescribed structure should be in place. Further, due to dynamic nature of these assets there should be mechanisms for:
- Version controls of data elements in the repository.
- Maintenance of history of changes in values with time.
- Registration of users of the repository, and also process of issuing automatic alerts to the applications, using the repository.

3.2.1 Steps for Achieving Semantic Interoperability

3.2.1.1 Semantic Interoperability Framework (SIF)

Need to address above through SIF, which should be subset of IFEG, and its purpose should be as described in section 3.1

The scope of SIF should include policies, mechanisms, and best practices for:

- Data accessibility, authentication, authorisation, security, transparency, accountability and privacy that constrain semantic interoperability.
- Building and maintenance of Repository of Semantic Interoperability Assets by addressing various aspects like precise meaning, consistency in values, understandability, and reproducibility of exchanged data / web services.
- Mapping the assets with e-Governance systems delivering e-Services.
- Maintenance of controlled data values, and history of the changes in assets common across the applications, for backward traceability.
- Issuing alerts to the applications, whenever there are changes in meta-data / values or conflicts during inter/intra organisation data exchanges.
- Addressing legal issues related to authentication / access / privacy rights, ownership / update rights etc., as data to be shared would be owned by heterogeneous agencies, using heterogeneous platforms and covered under heterogeneous legal systems.
- Policies regarding open data management.

3.2.1.2 Domain Specific Metadata Standards.

The Meta-data is an abstraction layer that makes the underlying information of a domain of an application-sector, which can be seamlessly accessed by the users of other application-sectors / domains. Thus the interoperability can be increased by the way of defining domain specific Meta Data Standards. This will bring semantic compatibility across various application-sectors / domains like Finance, Health, Education, Land resources, Panchayati Raj, Drinking Water & Sanitation, Food & Public Distribution, Agriculture, Justice, Road & Transport, Urban Development, Commerce, Police (Home Affairs) and Labour & Employment.

3.2.2 Challenges in achieving Semantic Interoperability

a) Issues like different ways of representations; context based reasoning, inconsistency in data etc.

b) No common understanding of information in terms of:

- Information Heterogeneity : Semantic, structural, representational, syntactic and format Heterogeneity
- Information Systems Heterogeneity: Heterogeneity of Digital Media Repository

Management Systems, Database Management Systems, data models and system capabilities such as concurrency control, recovery etc.

- Platform Heterogeneity: Heterogeneity of Operating Systems, Hardware / System
- Heterogeneous legacy systems
- Different cultural backgrounds
- Varied legal systems

c) Lack of bilateral or multilateral agreements for information exchange. In communication for information exchange between the systems, there are usually three participants like:

- System, that provides Information
- System that receives information
- System (optional) that monitors information-exchanged between provider(s) and recipient(s), for audit logging or any other reason

There is no implicit guarantee that all participants may understand the meaning of exchanged-data precisely, as context is associated with it.

d) The conflicts in the contextual meaning like:

- Data value conflicts
- Precision conflicts
- Labelling conflicts
- Integrity conflicts
- Conflicts of description of an entity by different attributes
- Conflicts in mandatory / optional nature of data in applications
- Ownership conflicts
- Conflicts in categorisation of data etc.

3.3 Technical Interoperability

To knit different kinds of e-Governance infrastructure and their services together through a catalogue of technical standards and specifications for the purpose of achieving interoperability in e-Governance systems; this is done by exchanging information across various boundaries (applications, interfaces, libraries, levels of administration including vertical and horizontal, etc.) and storage/archival of the information.

3.3.1 Levels of offer for e-Services

The levels of offer of e-Services may vary from one public agency to another based on factors like available resources, capability of human resources. In the initial level, the public agencies may have only online information for sharing; sometimes, they may have online downloadable eForms in addition to the online information; then, they may move to next level of offering online services. However, the ultimate objective is to offer online-integrated e-Services in the advanced level to the users.

3.3.2 Layers of Technical Interoperability

Technical interoperability addresses various layers/domains as indicated in Figure 4.2.

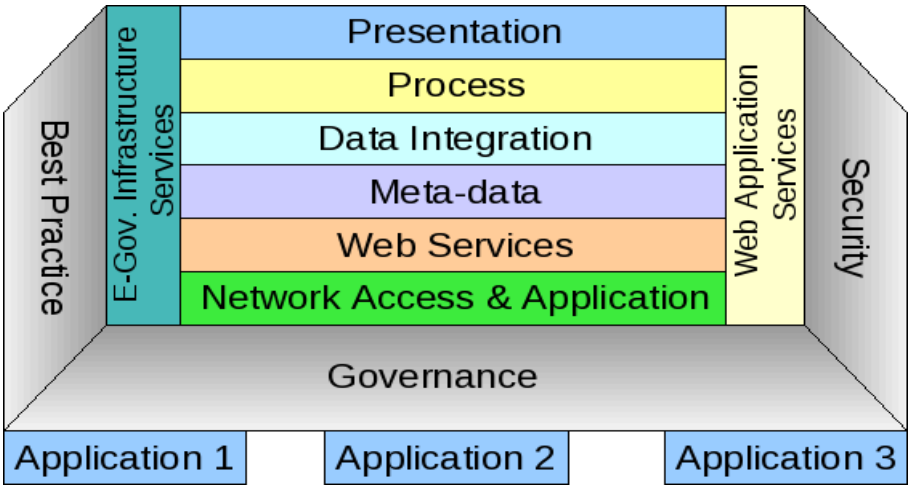

Figure 4.2 Layers/Domains of Interoperability

1. **Presentation and Archival:** 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. This concerns most of the user interface aspects relating to presentation of information in various formats. This includes standards and technologies related to the presentation of data to the user in the various means of access (personal computers, smart cards, mobile phones, PDA hand-held devices, digital televisions, etc.) to e-Services. The Archival part of this layer provides interface for storing and retrieving the data.

This layer is further divided according to the mode of service delivery and the corresponding standards on how the documents are presented (ODF, PDF, JPEG, etc.). The common standards found in this domain include: HTML, XHTML, WML, etc.

2. **Process:** This domain deals with standardisation of business and software processes. It is necessary that the business processes of the Government are aligned with the overall objectives of ICT based good governance. At the same time the technological (software) solutions also need to be developed with a view to promote integration and inter-operation among processes. This consists of set of processes followed to get desired output from given inputs. For example, a process describing how to file income tax return in batch processing using web services provided by income tax department website. The common standard found in this domain is BPMN

3. **Data Integration:** This domain covers standards that allow data exchange between homogeneous and heterogeneous systems. This relates to integrating data from different systems to provide consolidated view of the data. Data integrity and consistency is to be maintained. It includes standards and technologies for storage, retrieval, the discovery & location of resources and management government information. The common standards found in this domain include: XML, UML.

4. **Meta Data:** This domain deals with the core standards required for describing the data structures and their mapping to real-world entities, relational database table structures, XML schema used in the systems. The common standard(s) found in this domain include: Dublin Core Meta-data Initiative (DCMI)

5. **Web Services (Data Interchange):** This domain covers standards that allow data interchange services which support the exchange of data between homogeneous and heterogeneous systems. This concerns standards that allow data interchange services and that support the exchange of data between homogeneous and heterogeneous systems.

6. **Network Access & Application:** The Network layer of this domain specifies how information-processing resources are interconnected, and document 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. Network part of this layer consists of network protocols, messaging protocols, etc; it encompasses the interoperability components that facilitate the communication and exchange of information within the distributed information-processing environment. The Access part of this layer covers the technical specifications required for achieving interoperability between different access medium and application. The Application part of this layer includes standards for identifying communication partners, determining resource availability, and synchronising communication.

7. **Security:** This domain deals with the defined security services that are required at each domain of e-Governance Architecture model and wherever the components communicate with each other. This deals with security issues like encryption, decryption, passwords, digital signatures, etc. The security layer cuts across all technical interoperability layers. It includes standards and technologies needed to enable secure exchange of information as well as secure access to public sector information and services; includes encryption of data, public key infrastructure standards supporting the use of public and private encryption and decryption keys, digital signatures, and secure transmission protocols; also includes storing, using, and safekeeping identity information for users, citizens, employees, and resources. All other layers/domains to reflect the fact that security needs to be designed into a system, not added as a layer on top. Underpinning all these layers/domains is Governance which refers to ensuring the adoption of IFEG by public agencies with adequate resources, facilities, autonomy and authority. This is further described in detail in the next chapter.

3.3.3 Steps for Achieving Technical Interoperability

3.3.3.1 Standards to Enable Technical Interoperability

The layers/domains of Technical Interoperability are further sub-divided as Interoperability Areas (hereinafter referred to as “Areas”), for which Technical Standards are identified and vetted for openness as per the Policy.

3.3.3.2 Integration with Legacy Applications:

Encapsulation, such as web service which is a part of technical interoperability aspect, can be considered to share legacy applications as reusable components & services; it is relatively easy, cost-effective and less-risky compared to alternative methods; it is the best strategy if the legacy applications are fulfilling the e-Governance requirements.

3.3.3.3 Service-Oriented Architecture:

Many governments are moving toward adopting a service-oriented approach for their activities. This aligns with the fast growing solution architecture – namely, Service Oriented Architecture (SOA) – often adopted when implementing ICT solution. Service-Oriented Architecture (SOA) can be defined as a system design of loosely coupled and reusable software components called “services”; these services can be recombined into different solutions and scenarios, as determined by the e-Governance requirements. SOA has been identified as a best mechanism to enable the roll out of interoperable e-Governance services with appropriate access control (like Policy Based Access Control) that can be used among wide varying platforms with heterogeneous technology environments.

Adoption of a service as the unit of interaction for a department with citizens and other departments, provide an effective approach that promotes loose coupling among the various

stakeholders. Such a loose coupling is needed in a multi-tier administrative set-up as in India. At the same time, service is an appropriate and powerful unit for reuse and Interoperability between systems. It breaks down processes and applications into discrete parts – called services –, and then develops solutions for these parts which can then be used and shared widely. A service orientation defines the needs and outcomes of the department in terms of services, independent of the technology that implements them.

With respect to the administrative aspect of the approach, one can use services provided by different vendors, and integrate them suitably to realise what one is looking for. Therefore, it is recommended that all departments and agencies adopt a service based approach to their functioning, clearly defining the services they offer to other stakeholders. This would also include the assumptions under which the service will be offered, and the inputs required for delivering the service. This would enable a public agency to handle changes in input sources or the manner of collection of the inputs, seamlessly, since the service framework can be defined independent of these issues. This is the essence of the service model.

3.3.4 Challenges in achieving Technical Interoperability:

a) The non-availability of ICT infrastructure to support technical interoperability at the data/component/service level is one of the major challenges; different kinds of platforms and their frameworks of the e-Governance systems may conflict with each other to disturb the enablement of interoperability.

b) The interoperability among legacy systems with disparate technology, process and data may pose a great challenge. The development of mechanism to perform the technical reconciliation among legacy systems may also create obstacles.

c) Many public-agencies have their own web-sites in silos to offer web services.

d) Unavailability of adequate resources, facilities, and autonomy to monitor the compliance with IFEG from the stage of Request for Proposal (RFP).

e) Conflicting requirements due to national security, IPR and privacy.

4 Summary and Recommendations

4.1 Organisational Interoperability:

1. All agencies could use UIDAI for user authentication/identification.
2. While adopting the BPR for policy and standardization the autonomy of public agencies should be ensured for required data protection and security purpose.
3. Interoperability for most applications requiring interactions among several public agencies should not need any special agreements.
4. Private sector bodies and non-governmental organisations participating in the IFEG should own only the information and/or data pertaining to them. The use of nested e-Services should be agreed amongst various public agencies.
5. Each public agency should determine access restrictions within its own information system.
6. The differences among e-Governance systems should not pose an obstacle to tasks which span those systems; the agreements should be signed by all stake-holders to accommodate & resolve differences and to support shared information architecture.
7. Each public agency should identify the list of processes belonging to it for standardisation. The standardised processes should be made as e-Processes or e-Services; these should be shared with other stakeholders by the respective public agency through a Process Agreement. List of information on input, output and internal operations of each process/service should be shared with others.
8. Management and Governance recommendations;
9. e-Services should be exchanged free or at a nominal charge among public-agencies with mutually agreed terms/SLAs.
10. Each e-Service should be offered with appropriate Service Level Agreement (SLA).
11. The interoperability issues should be emphasised right from the RFP stage.
12. The capacity building should be incorporated to educate and train government personnel on IFEG and ICT skills
13. Appropriate metrics should be defined and used at regular interval to measure the success of interoperability.
14. The integrated common front-office should be established through a common service delivery mechanism like a Portal.
15. Sharing of ICT infrastructure should be preferred through mechanisms like virtual-instance/cloud-computing, enhanced reuse of service-components & libraries.

4.2 Semantic Interoperability:

1. Need to have processes in place to create quick repository of semantic interoperability assets
2. While identifying stakeholders for various mechanisms, the following roles & responsibilities should be clearly defined and agreed upon:
    - Ownership rights
    - Assurance about correctness and integrity
    - Assurance about making the data available for sharing within stipulated time period
    - Addition of data in centralize repository
    - Updating, auditing, compliance review rights and corresponding stipulated processes and discharge legal obligations etc.
3. Mapping the standardised data elements with data elements in legacy systems, which are not standards based.
4. To increase interoperability, it is required to define domain specific Meta Data Standards to bring semantic compatibility across various domains of application-sectors.

4.3 Technical Interoperability

1. The technical interoperability across various boundaries (applications, interfaces, libraries, etc.) and storage/archival of the systems should be ensured.
2. The representation of information should be based on open standard and formats. The mandatory adoption of notified standards will help public agencies to avoid vendor lock-in.
3. The technology-neutral or technology-independent frameworks/formats should be used to ensure long term preservation of information.
4. Technologies and Frameworks used in e-Governance should be selected to address Inclusion and Accessibility requirements of the disabled, the illiterate segment of the population.
5. Multilingualism/Localisation should be considered at all levels from the design stage itself in e-Governance so that there is minimum efforts required whenever website or system is to be made available in multiple Indian languages.
6. Security and privacy should be ensured in e-Governance systems.
7. The technology which enables the scalability of e-Governance systems should be preferred to handle change or fluctuation in demand and volume of transactions, considering the size of Indian population.
8. The standards and technologies selected should reduce costs (total cost including the transition cost to avoid vendor lock-in) and risks to all stake-holders of e-Governance.
9. Compatibility with Internet and World-Wide Web specifications should be ensured.

10. Standards-based Web-browser should be preferred to access and deliver e-Services through multiple channels and devices.
11. Adoption of XML Technologies should be preferred for integration of information-system and presentation of data.
12. Component-based e-Services model should be created by public agencies so that existing components can be reused as much as possible.
13. Higher-level e-Service should be preferably composed from various lower-level e-Service components offered by various public agencies.
14. Solutions (proprietary/open source) based on Open Standards should be preferred.

5 Way Forward

This document provides the overarching framework for interoperability. It addresses in detail the current scenario and challenges at each layer (Organisational, Semantic and Technical) and makes specific recommendations in the respective chapters on how to address them. However, a bottom-up approach towards addressing these recommendations separately at each layer and in a theoretical or abstract manner is unlikely to be very effective. A top-down integrated action plan is suggested which is expected to contribute valuable learning and propel interoperability of GoI e-Governance initiatives to the next level.

IFEG recognises that the interoperability is a continuous task among the public agencies since interoperability can be disrupted by changes to the environments like:

- Legislation
- Needs & their priorities of citizens and businesses
- The organisation of public administrations
- Business processes
- Technologies.

And hence the framework needs to be periodically revised taking into consideration the above influencing factor.

6 Annexure

Annexure I: Global Scenario

IFEG is the core component to achieve interoperability in e-Governance. An IFEG is simply defined as a common structure which comprises a set of standards and guidelines; the structure can be used by the public agencies to specify the preferred way that all stake-holders interact with each other to share the information. It is synonymous to speaking a common language. IFEG is also known as 'Government Interoperability Framework' (GIF) in some countries.

Federated Enterprise Architecture (FEA) is one of the ways to build further on IFEG by classifying standards for interoperability based on services and life-time events. FEA is adopted in European Union, Germany, etc. Additional details are described in FAQ (Annexure VIII).

This document customises the IFEG approach for the Indian context, for enabling interoperability between e-Governance projects for the seamless flow of information between different administrations in the delivery of e-Services.

Organisational Interoperability finds a mention in most of the frameworks for Interoperability published by different countries. Organisational Interoperability is a growing concern in most of the countries dealing with Interoperability. However, of the many challenges in effectively realising Interoperability, Organisational Interoperability is being seen as the biggest challenge, with very little formalisation so far.

In general, there are three strategies for achieving Organisational Interoperability with respect to the organisational issues.

1. Centralisation of tasks – make the different applications involved to be owned and run by a single agency. This may raise issues of change of jurisdiction and authority, and hence, in turn, requires strong political intervention.
2. Standardisation of processes – all external interfaces and processes at the boundary are standardised. All entities requiring that interface or process, agrees to adhere to this standard specification.
3. Introduce clearing houses – often used as a temporary solution, these provide conversion service, to bring in Interoperability among two interfaces, by converting information in one interface to the form requires for the other interface. This may include form conversions, data formats, etc.

The exchange of services through multilateral agreements among many public agencies is preferred compared to bilateral agreements. Orientation of the activities as services brings the focus to the end users. Process changes are introduced to make the accessibility of all e-Services from anywhere, any-time.

Internationally Governments are also taking initiatives to address **Semantic Interoperability** requirements either in their Interoperability Frameworks or their Enterprise Architecture.

In USA, Data Reference Model (DRM) serves as means for identifying, what data the Government has, and how such data can be shared for business requirements. It addresses three areas for standardisation like:

data description, data context, and data sharing

Interoperability Framework for European Union (EU) addresses strategy about content interoperability. The **Semantic Interoperability Centre Europe (SEMIC.EU)** is an eGovernment service initiated by the European Commission and managed by the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) Unit. It is a service for the exchange of solutions to semantic interoperability, with a focus on demands of eGovernment in Europe.

In UK Interoperability Framework, Meta-data standard addresses requirement of data interoperability to ensure maximum consistency of meta-data across public sectors.

Information Interoperability Framework of Australian Government aims to assist agencies in their capacity for information management to support seamless information exchange.

Service Oriented Architecture (SOA) is used to exchange e-Services from widely disparate e-Governance systems; SOA defines the loosely coupled interface in terms of protocols and functionality. Web Services implement SOA in web-based environment. REST, Mashups and Cloud Computing are considered as recent extensions of SOA; they are progressively adopted for the exchange of web-based e-Services.

All e-Services are offered through web-browser interfaces available in different kinds of systems like desktop, laptop, tablet, mobile, etc.

The e-Services from various public agencies under a state and its local-bodies are initiated / offered through a common multi-lingual State Portal where a set of eForms are made accessible; eForms can be downloaded for filling and submitting (with or without payments) through online / off-line processes. The use of multiple Indian languages is also allowed to fill multi-lingual forms.

Annexure II: GoI Initiatives

- Many government policies and guidelines, including the 'Policy on Open Standards for e-Governance', are aimed at ensuring Openness and Transparency. GoI has decided to use Open Standards for e-Governance projects in India. “Policy on Open Standards for e-Governance” was announced by GoI in November 2010 to provide a framework for selection of technical standards in identified areas, within interoperability layers/domains. All standards, specifications, protocols, shall align with the Policy.
- GoI has brought out “Guidelines for Indian Government Websites” which addresses the various accessibility issues of government websites.
- GoI has brought out a set of guidelines for information security.
- E-Governance Infrastructure Services include Wide Area Network (like SWAN, NICNET, NKN), Government Data Centres (like SDC, NDC), e-Governance citizen service centres (like CSC, e-Seva); these are implemented by public agencies (like DeitY, NIC, CDAC, etc) for the use of stake-holders of e-Governance. Detailed reference in Annexure

  A set of standardised applications (like National & State Portals, NSDG, SSDG) to connect and integrate web-based applications over the Internet. “Technical Standards for Interoperability Framework for e-Governance (IFEG) in India” is hosted at the following link: https://egovstandards.gov.in/sites/default/files/Published_Standards/Technical%20Standards%20for%20IFEG/Technical_Standards_for_IFEG_Ver1.0.pdf
- Preparation of Institutional Mechanism for building Domain specific Meta Data and Data Standards (MDDS) for generic data elements common across the domains and common within domains. Meta Data and Data Standards for Person Identification and Land Region codification already notified, and action initiated for the domains Panchayat Raj, and Land records Management. Repository of code directories of generic data elements identified so far and having controlled values already published for use by e-Governance applications developers.
- The report on **Technical Standards on Interoperability Framework** for e-Governance which contains 47 Technical Standards for the identified Interoperability Areas was notified by GoI in June, 2012. The following standards were also notified:
    - MDDS – Demographic – Ver 1.1
    - Biometric Standards
    - Quality Assurance Framework (QAF)
    - Font Standard
    - Character Encoding Standard

  Other activities include notification of **Institutional Mechanism for e-Governance Standards Formulation** and set of standards and guidelines as indicated at http://egovstandards.gov.in/

Annexure III: e-Governance Infrastructure in India

State Data Centre (SDC) was identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of NeGP. SDC provides many functionalities like Central Repository of the State, Secure Data Storage, On-line Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. SDCs also provides better operation & management control and minimise overall cost of Data Management, IT Resource Management, Deployment and other costs.

National Portal of India and **State Portal** projects have been formulated under the NeGP to act as a single front-end interface (a single window or one-stop delivery or one service window) to the national and state level e-Governance initiatives and services. GoI has developed the Portal Framework which inculcates certain degree of standardisation, interoperability & exchange of Information & Services among the websites of public agencies.

The e-Services are rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as **State Wide Area Network (SWAN)**.

GoI initiated **State Service Delivery Gateway (SSDG)** at the state level to integrate e-Services, eForms and CSCs with the State Portal (SP) by leveraging the common infrastructure (SWAN, SDC etc.). Similarly **National e-Governance Service Delivery Gateway (NSDG)** was launched at the national level to integrate e-Services with the National Portal and other SSDGs by utilising the common infrastructure (national networks and national data centres). Both SSDG and NSDG are realised under the NeGP.

GoI has initiated Public Information Infrastructure and Innovations (**PIII**) with the planned tasks like

- Operationalising the National Knowledge Network (NKN) to interconnect all educational and research institutions
- Overseeing broadband connectivity to Panchayats and enabling citizen interface to improve delivery of public services and citizen empowerment
- Promoting greater use of ICT in Public Transport Systems
- Promoting greater use of ICT in the Justice System
- Developing an Action Plan for a Decade of Innovation

Annexure IV: Definitions

Apex Body (Refer Policy)

Area (Refer Policy)

Common Services Centre (CSC) is a centre at the citizen's locality meant for providing integrated e-Governance service from multiple public agencies. It may be established through Public-Private-Partnership; or it may be established at other public agencies like Post Office, Village Panchayat Office, etc.

Enterprise is a company, an institution, or a department within a company or an institution.

e-Service: Any service offered by a public agency through Information & Communication Technology (ICT) to other stake-holders like citizen, other public agency, business, public-servant / people's representative, etc. is known as e-Service or E-Governance Service. e-Services are classified into G2G, G2C, G2B and G2E. However, e-Service in Indian Context doesn't cover G2OG and G2Org.

G2G in IFEG includes interoperability among various federated structures of the Indian Government;

- Central government agency to central government agency
- Central government agency to state government agency
- State government agency to state government agency
- State government agency to local government agency of the state.
- Local government agency to local government agency (within the state)

G2C includes interoperability between any public agency in the federated structure of the Indian Government and the citizen; similarly, G2B includes interoperability between any public agency in the federated structure of the Indian Government and the business and G2E includes interoperability between a public agency in the federated structure of the Indian Government and its employee.

e-Seva is a set of e-Governance services provided by public agencies.

ICT resources are data, network equipment, software components, business locations, human resources, etc.

ICT Infrastructure means the computer and communication hardware, software, services, networks, physical assets (such as highly specialised buildings and equipments including for power, air-conditioning, and safety), people & policies supporting ICT information management functions.

Interoperability Framework is simply defined as a common structure which comprises of a set of common elements: vocabulary, concepts, principles, policies, guidelines, recommendations, standards and practices; the structure can be used by the public agencies to specify the preferred way that all stake-holders interact with each other to share the information. It is synonym to speaking a common language.

Layer/Domain (Refer Policy)

Meta-Data means 'data about data'. It is defined as the data that provides information about or documentation of other data managed within an application or environment.

Multilateral Mechanism is a process to facilitate multiple public agencies to work together to offer agreed public services.

National e-Governance Plan (NeGP) The National e-Governance Plan (NeGP) of the Govt. of India aims to make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man. The Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 8 components, on May 18, 2006. The Government has accorded approval to the vision, approach, strategy, key components, implementation methodology, and management structure for NeGP.

(Reference: http://www.mit.gov.in/content/national-e-governance-plan)

National e-Governance Service Delivery Gateway (NSDG) In order for the Government to realise the NeGP vision, it is imperative that the different departments in the Centre, States and Local Government cooperate, collaborate and integrate information across the various levels, domains and geographies. Government systems characterised by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation, make this task very challenging. The National e-Governance Service Delivery Gateway (NSDG), a MMP under the NeGP, can simplify this task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across.

The emergence of many e-Governance systems for different departments to provide on-line services to citizens, businesses and government would require increasing interactions amongst departments and with external agencies at various levels in Government. Departments would need to develop connectors/adaptors for point to point connections between departments creating a mesh as shown in figure and also tight coupling between applications. This would lead to applications that are difficult to maintain and upgrade in case of version change and change in government policies and business rules. The NSDG is an attempt to reduce such point to point connections between departments and provide a standardised interfacing, messaging and routing switch through which various players such as departments, front-end service access providers and back-end service providers can make their applications and data inter-operable. The NSDG aims to achieve a high order of interoperability among autonomous and heterogeneous entities of the Government (in the Centre, States or Local bodies), based on a framework of e-Governance Standards.

(Reference: http://www.mit.gov.in/content/about-nsdg)

The **One-Stop delivery** system is a system under which public agencies collaborate to create a seamless system of service delivery that will enhance access to the e-Governance service.

Ontology formally represents knowledge as a set of concepts within a domain (system or application) and the relationships among those concepts. That is, ontologies provide meanings to concepts; most ontologies describe individuals (instances), classes (concepts), properties & relations (attributes of concepts) and constraints & restrictions (axioms & rules).

Public Agency: A government or quasi-government organisation as a part of vertical and horizontal three-tier federal administrative structure that serves the community is called as Public Agency. The Public Agencies in Indian scenario includes the agencies from: Central Government (including cabinet secretariat, ministries, departments, and public sectors), Constitutional Bodies, State Governments (including state secretariat, ministries, departments, public sectors, and district administration), Local Bodies (including Corporation, Municipalities, Town Panchayat, Village Panchayat, Block Panchayat, District Panchayat).

Semantics is the study of the meaning or an interpretation of the meaning of a word, data, sign, or sentence. It is expected to give same understanding when the data is exchanged.

Service Level Agreements referred to as SLA is a contract of "level of service" between service provider and a customer. SLA may specify the availability, performance, problem management, legal compliance, resolution of disputes, customer duties & responsibilities, security, IPR & confidential information, termination, etc. for each level of the service.

Service Oriented Architecture (SOA) is a collection of loosely coupled distributed services which communicates and interoperates via agreed standards, the combination of a service and standards based approach can result a directory of reusable service components which together can be employed to enhance the existing applications or build new applications. Some means of connecting services to each other is needed. The technology of Web services is the most likely connection technology of service-oriented architectures. Web services essentially use XML to create a robust connection.

Syntactic means systematic orderly arrangement of words, data, signs or sentences. But there is no guarantee for the exchanged data to give same understanding.

State Service Delivery Gateway (SSDG) The GoI desires to create an integrated information infrastructure that will expand, integrate and enhance the utility and reach of the services provided by the Government by utilising the network of the CSCs. This project aims to enhance the services provided to the citizens through CSCs. It is envisaged that State Portal (SP) along with SSDG will be developed and implemented so that citizens are provided with outlets where they can access the services under a single interface mechanism in the form of the Portal. Also the project entails delivery of the services through CSCs)\ by leveraging the common infrastructure (SWAN, SDC etc.) and develop the applications and infrastructure required for deployment of SP and SSDG for the State. This will enable citizens to download forms and submit their applications electronically through a common gateway. This important initiative facilitating Electronic Service Delivery will provide significant benefits to the citizens especially in the form of a single gateway to citizen for service delivery. Thus holistic and harmonious use of the CSCs along with the common infrastructure (SWAN, SDC) and technology across the state for all application and services shall be achieved.

(Reference: http://www.mit.gov.in/content/introduction-ssdg)

Annexure V: Acronyms & Abbreviations

List of Acronyms:

API	Application Programming Interface
BPMN	Business Process Model & Notation
CDAC	Centre for Development of Advanced Computing
CSC	Common Services Centre
DeitY	Department of Electronics and Information Technology
DCMI	Dublin Core Meta-data Initiative
DR	Disaster Recovery
DRM	Data Reference Model
EA	Enterprise Architecture
EU	European Union
FEA	Federated Enterprise Architecture
G2B	Government-to-Business and vice versa
G2C	Government-to-Citizen and vice versa
G2E	Government-to-Employee and vice versa
G2G	Government-to-Government and vice versa
G2OG	Government-to-Other-Government and vice versa
G2Org	Government-to-Organisations and vice versa
GIF	Government Interoperability Framework
GoI	Government of India
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communication Technology
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IFEG	Interoperability Frameworks for e-Governance
IPR	Intellectual Property Rights
IT	Information Technology
JPEG	Joint Photographic Experts Group
MDDS	Meta Data and Data Standards
MMP	Mission Mode Projects
NDC	National Data Centre
NeGP	National e-Governance Plan
NIC	National Informatics Centre
NICNET	National Informatics Centre Network
NKN	National Knowledge Network
NSDG	National Service Delivery Gateway
ODF	Open Document Format
OSS	Open Source Software
PC	Personal Computer
PDA	Personal Digital Assistance
PDF	Portable Document format
PIII	Public Information Infrastructure and Innovations
REST	REpresentational State Transfer
RFP	Request For Proposal
RTI	Right to Information
SAGA	Standards and Architectures for e-Government Applications

SDC	State Data Centre
SEMIC-EU	Semantic Interoperability Centre Europe
SIF	Semantic Interoperability Framework
SLA	Service Level Agreement
SP	State Portal
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSDG	State Service Delivery Gateway
SWAN	State Wide Area Network
UDDI	Universal Description, Discovery and Integration
UIDAI	Unique Identification Authority of India
UK	United Kingdom
UML	Unified Modelling Language
WML	Wireless Markup Language
WS	Web Service
WSDL	Web Services Description Language
XHTML	eXtensible Hyper Text Markup Language
XML	Extensible Markup Language

List of Abbreviations:

Dept.	Department
Govt.	Government

Annexure VI: Benefits of IFEG

The impacts yield from IFEG are ultimately to serve Citizens, however, the derived impacts of IFEG which have indirect benefits to citizen are not explicitly marked.

	Expected Impact	Public agencies	Providers of eServices/ depts	Citizens	Public servants	Public Representatives	ICT Industries	Academia & Research Institutes	Standards Bodies
	Introduction								
1.1	Avail eServices (including G2C, G2B, G2G, G2E) through a single window	☐	☐	☐	☐	☐	☐	☐	☐
1.2	Avail eServices through multiple delivery channels like PC, Mobiles, Common Services Centres	☐	☐	☐	☐	☐	☐	☐	☐
1.3	Enable a system to inter-operate efficiently and effectively with other systems from stake-holders of e-Governance	☐	☐				☐	☐	☐
1.4	Enable better coordinated cooperative decision-making among the stake-holders of e-Governance	☐	☐	☐	☐	☐			☐
1.5	ble autonomous development for systems within the principles of various levels of interoperability	☐	☐				☐	☐	☐
1.6	Enable better sharing of ICT infrastructure	☐	☐						
1.7	Enable (i) enhanced reuse of service-components & libraries, (ii) avoidance of duplication of service-components & libraries	☐	☐				☐	☐	☐
1.8	While procuring, create competition among various vendors which will lead to (i) cost-saving, (ii) reduction in the dependency on single vendors and (iii) provisioning of multiple choices for public agencies	☐	☐				☐	☐	
1.9	Facilitate smoother operations through e-Commerce/e-Trade activities to enable better trade among countries	☐							
1.10	Enable better Cyber Security.	☐	☐	☐	☐	☐	☐	☐	☐
1.11	itate availing of public services (i) through eServices from anywhere, at any-time, by anyhow and (ii) also through the conventional service-delivery channels like face-to-face meeting, postal, telephone, etc.	☐	☐						

	Expected Impact	Public agencies	Providers of eServices/ depts	Citizens	Public servants	Public Representatives	ICT Industries	Academia & Research Institutes	Standards Bodies
	Organisational Interoperability								
2.1	Easier integration of e-Governance systems across public agencies.	☐	☐						
2.2	A smoother experience for users and public agencies, as they work across organisational boundaries.	☐	☐	☐	☐	☐	☐	☐	☐
2.3	Enabling e-Services through "Single Window".	☐	☐				☐		
2.4	Enabling better readiness among public agencies to support and to facilitate Interoperability and e-Services.	☐							
2.5	Reduced efforts of development of systems for e-Services by reusing already standardised common processes	☐	☐				☐		
	Semantic Interoperability								
3.1	Ensuring Consistency that information exchanged is interpreted and processed unambiguously in all the interacting-systems at all the time.	☐	☐	☐	☐	☐	☐	☐	☐
3.2	Building trust that the communicated information from multiple sources is valid, and without any ambiguity.	☐	☐	☐	☐	☐	☐	☐	☐
3.3	Ensuring reproducibility and reliability of the data, which is collected or encoded at various sources and reproduced for the usage among the stakeholders. This holds both for individual and aggregated data at organisation level.	☐	☐	☐	☐	☐	☐	☐	☐
	Technical Interoperability								
4.1	Facilitation of availing e-Services from anywhere, at anytime, by anyhow (through multiple delivery channels like PC, Mobiles, CSCs) with the adoption of compatible ICT infrastructure.	☐	☐	☐	☐	☐	☐	☐	☐
4.2	Consolidation and preservation of data of each e-Governance application at a centralised location with appropriate backup and	☐	☐				☐		

	Expected Impact	Public agencies	Providers of eServices/ depts	Citizens	Public servants	Public Representatives	ICT Industries	Academia & Research Institutes	Standards Bodies
	disaster recovery mechanism at a remote location.								
4.3	Provision of integrated & shared e-Service, which may span multiple public agencies, through a single window to all its stake-holders.	☐	☐	☐	☐	☐	☐	☐	☐
4.4	Offer of integrated e-Service with appropriate Quality of Service (QoS), Service Level Agreement (SLA) and Security.	☐	☐				☐		
4.5	Avoidance of single point of failure for e-Governance system by establishing alternative mechanisms or fail-over (clustering) mechanisms at the critical portions.	☐	☐	☐	☐	☐	☐	☐	☐
4.6	Compliance to the Policy on Open Standards.	☐	☐	☐	☐	☐	☐	☐	☐
4.7	Establishment of common public e-Governance infrastructure at each State and National level to offer interoperability of e-Governance systems.	☐	☐				☐		
4.8	Adoption of principles of Service Oriented Architecture (SOA) to enable integration of dissimilar technologies.	☐	☐						

Annexure VII: A Typical Template on Performance & Evaluation of IFEG

Department / Organisation Name	
Ministry	
Project Name	

Sl. No (A)	Interoperability Level (B)	Total number of IFEG recommendations (C)	Applicable number of IFEG recommendations (D)	% of Applicability (D)/(C) (E)	Compliance Score (F)	% of Compliance (F)/[5*(D)] (G)
1	Organisational Interoperability	11	*		*	
2	Semantic Interoperability	8	**		**	
3	Technical Interoperability	21	***		***	
	TOTAL					

* - Values from 'Organisational Interoperability' Table

** - Values from 'Semantic Interoperability' Table

*** - Values from 'Technical Interoperability' Table

Column (E) & (G) are calculated columns.

Interoperability Level: Organisational Interoperability

Sl. No	IFEG Recommendations for Organisational Interoperability	Applicability of the Recommendation (1 for applicable, 0 for not applicable)	Compliance score (Scale 5 to 0, 5 for fully compliant and 0 for non-compliant)	Remarks
1	Use of UIDAI as an alternative mode for user authentication/identification.			
2	The autonomy of public agencies should be retained with appropriate Business Process Re-engineering (BPR) changes.			
3	Interoperability for most applications requiring interactions among several public agencies should not need any special agreements.			
4	Private sector bodies and non-governmental organisations participating in the IFEG own only the information and/or data pertaining to them. The use of nested e-Services is agreed on among various public agencies.			
5	Data in the state information system should be owned by the state.			
6	Responsibility for the structure and content of data should lie with the public agency administrating the respective data either as a chief or an authorised processor of data.			
7	Legal restrictions as well as organisational capacities should be taken into account during data exchange.			
8	Interoperable public agencies should exchange information by user authorisation.			
9	Each public agency should determine access restrictions within its own information system.			
10	The agreements should be signed by all stake-holders to accommodate & resolve differences and to support shared information architecture.			
11	It is important to have Process Agreement by concerned public agency with key stakeholders to establish a common understanding on reviews, artifacts, Do's & Don'ts, templates and conformance conditions of the e-Governance system.			
	Total			
	Percentage of Applicability of Recommendations Applicable No. of IFEG Recommendations ---------- X 100 Total No. of IFEG Recommendations			
	Percentage of Compliance Compliance Score ---------- X 100 (Applicable No. Of Recommendations) X 5			

Interoperability Level: Semantic Interoperability

Sl. No	IFEG Recommendations for Semantic Interoperability	Applicability of the Recommendation (1 for applicable, 0 for not applicable)	Compliance score (Scale 5 to 0, 5 for fully compliant and 0 for non-compliant)	Remarks
1	Need for strategic policies at GoI level for developing Semantic Interoperability capabilities.			
2	A centralised agency for Semantic Interoperability Centre may be created by GoI on the lines similar to Europe (SEMIC.EU), to manage Semantic Interoperability Assets; otherwise, these functions may be handled by the proposed central-agency for the implementation of IFEG as indicated in the chapter on Governance of IFEG, may be by establishing a central agency for management of Semantic Interoperability assets.			
3	While identifying stakeholders for various mechanisms, the following roles / specifics should be clearly defined and agreed upon: -Ownership rights -Assurance about correctness and integrity -Assurance about making the data available for sharing within stipulated time period -Addition of data in centralize repository updating, auditing, compliance review rights and corresponding stipulated processes and discharge legal obligations) etc.			
4	Special efforts may have to be put for mapping the standardised data elements with data elements in legacy systems, which are not standards based			
5	Conflicts resolution should be handled at senior management level, and should be resolved immediately			
6	Data sharing requirements in case of disasters are usually unplanned, and there is need to have processes in place to create quick repository of semantic interoperability assets by providing appropriate authority to the concerned agencies			
7	Accountability for correctness of the data by the owners of the shared data, and also accountability for seamless exchange of such data needs to be assured through audit processes			
8	To increase interoperability, it is required to define domain specific Meta Data Standards to bring semantic compatibility across various domains of application-sectors			
	Total			
	Percentage of Applicability of Recommendations Applicable No. of IFEG Recommendations			

	---------- X 100 Total No. of IFEG Recommendations			
	Percentage of Compliance Compliance Score ---------- X 100 (Applicable No. Of Recommendations) X 5			

Interoperability Level: Technical Interoperability

Sl. No	IFEG Recommendations for Technical Interoperability	Applicability of the Recommendation (1 for applicable, 0 for not applicable)	Compliance score (Scale 5 to 0, 5 for fully compliant and 0 for non-compliant)	Remarks
1	The technical interoperability across various boundaries (applications, interfaces, libraries, etc.) and storage/archival of the systems should be ensured.			
2	The representation of information should be based on open standard and formats. The mandatory adoption of notified standards will help public agencies to avoid vendor lock-in			
3	The technology-neutral or technology-independent frameworks/formats should be used to ensure long term preservation of information & freedom since most of the information in e-Governance need to be preserved for a long period, often running into several decades. Multiple platforms should be supported.			
4	Openness and transparency should be used in e-Governance.			
5	Technologies and Frameworks used in e-Governance should be selected to address Inclusion and Accessibility requirements of the disabled, the illiterate segment of the population.			
6	Multilingualism/Localisation should be considered at all levels from the design stage itself in e-Governance so that there is minimum efforts required whenever website or system is to be made available in multiple Indian languages.			
7	Security and privacy should be ensured in e-Governance systems.			
8	The technology which enables the scalability of e-Governance systems should be preferred to handle huge change or fluctuation in demand and volume of transactions, considering the size of Indian population.			
9	The standards and technologies selected should reduce costs (total cost including the transition cost to avoid vendor lock-in) and risks to all stake-holders of e-Governance.			
10	The Central government and State governments should establish common and secure ICT infrastructure which adopt notified standards.			

Sl. No	IFEG Recommendations for Technical Interoperability	Applicability of the Recommendation (1 for applicable, 0 for not applicable)	Compliance score (Scale 5 to 0, 5 for fully compliant and 0 for non-compliant)	Remarks
11	A common-portal with appropriate security mechanism should be established & used to submit requests to all public agencies and get responses by all users of e-Services.			
12	Alignment with Internet and World-Wide Web specifications should be ensured.			
13	Standards-based Web-browser should be preferred to access and deliver e-Services through multiple channels and devices.			
14	Adoption of XML Technologies should be preferred for integration of information-system and presentation of data.			
15	All data & information collected for e-Services at various public-agencies should be consolidated at State and National levels but at the same-time retaining the autonomy of the concerned public agencies. This should also facilitate backup & recovery mechanism for the e-Services offered at remote public-agencies.			
16	Information should be exchanged among different e-Governance systems at service-level but not at the database-level; however, the consolidation of information from remote locations to the common central location for a particular e-Governance application can be considered at the database-level.			
17	Component-based e-Services model should be created by public agencies so that existing components can be reused as much as possible.			
18	Higher-level e-Service should be preferably composed from various lower-level e-Service components offered by various public agencies.			
19	Solutions (proprietary / open source) based on Open Standards should be preferred.			
20	Wider adoption of Open Source Software (OSS) solutions should be considered alongside Proprietary Software Solutions. OSS should be preferred over Proprietary Software Solutions when both meet the requirements.			
21	Encapsulation, such as web services, should be considered to share legacy applications.			
	Total			
	Percentage of Applicability of Recommendations Applicable No. of IFEG Recommendations ---------- X 100 Total No. of IFEG Recommendations			
	Percentage of Compliance Compliance Score ---------- X 100			

Sl. No	IFEG Recommendations for Technical Interoperability	Applicability of the Recommendation (1 for applicable, 0 for not applicable)	Compliance score (Scale 5 to 0, 5 for fully compliant and 0 for non-compliant)	Remarks
	(Applicable No. Of Recommendations) X 5			

Annexure VIII: Frequently Asked Questions (FAQs)

1) In what ways a Service can be implemented?

Increasing applications are moving to a web environment from older client/server and stand-alone modes. We will, therefore, be focusing mostly on web based applications. There are two broad approaches for implementing web based applications – REST based and web service based. While more and more people are adopting to web service based implementations, this trend is currently in the early stages and is triggered by the service oriented approach to computing. This provides a simpler and cleaner abstraction for modularising large applications. Service also provides a natural unit/ primitive for interoperability. However, we observe that a lot of current and in-process applications still use REST based model, and hence this is covered within the scope of this document. A brief comparison of the two approaches is given below.

WS approach:

A Web service is any piece of software that makes itself available over the Internet and uses a standardised XML messaging system. XML is used to encode all communications to a Web service. For example, a client invokes a Web service by sending an XML message, and then waits for a corresponding XML response. Because all communication is in XML, Web services are not tied to any one operating system or programming language. It has an interface described in a machine-processable format (specifically Web Services Description Language WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialisation in conjunction with other Web-related standards.

REST approach:

REST is an acronym for “Representational State Transfer”. The Web is comprised of resources, such as HTML page giving information about a company, URL giving access to internet media file. Whenever a client accesses such a resource, its representation places the client in a state. The client application transfers this state with each resource representation. REST is intended to evoke an image of how a well-designed Web application behaves: a network of web pages (a virtual state-machine), where the user progresses through an application by selecting links (state transitions), resulting in the next page (representing the next state of the application) being transferred to the user for his/her use.

2) Compare Web Services and REST.

REST expose a simpler interface than WS. Development of REST is simpler and quicker and this is the reason why most popular APIs are REST-based. However, REST has some limitations which come from the HTTP protocol it uses. So to design application exclusively for web, REST is good option. For designing SOA applications that interconnect to multiple systems using multiple channels, WS approach is better choice. Given the higher modularity offered by the service level of abstraction, a service oriented structure of applications is more and more popular. Hence, a web service model is worth investigating for newer applications. Web services also provide a full framework for many-many interactions among the services with UDDI, WSDL, SOAP etc.

At present one may choose either of the approaches and the IFEG discussed here provides scope for both.

3) What are the differences between Interoperability and Intra-operability?

The collaboration and service sharing can be made available through intra-operability and interoperability environments.

In the intra-operability situation, one product is somehow central and dominant, either by market-share, attitude, or acquiescence. The nature of connectivity (including data formats, protocols, user-interface, etc.) is often prescribed and even controlled by the provider.

In the interoperability situation, one use standards that do not favour any one software provider. The interoperability environments strengthen the provision of integrated services to facilitate the electronic flow of information and transactions seamlessly across government to all its stakeholders.

4) How the interoperability is enabled?

Though it is possible to achieve interoperability technically, government's strategy & leadership to deliver effective e-Governance services to other stake-holders are more crucial. To enable interoperability across e-Governance projects from public agencies, one does not start with technology. One has to start with the government's strategy, the vision and goals to deliver effective e-Governance services to Citizens and Businesses in the short term as well as in the medium term.

5) What are the factors for the success of IFEG?

The success of the IFEG approach for the interoperability is not only based on how strong it is as a technical document, but also how well it supports the overall goals of a flexible public service and good e-Governance. The IFEG approach must demand and create interoperability focused on obtaining more efficient, effective and transparent better e-Governance.

6) What is interoperability in e-Governance?

The 'Interoperability' in E-Governance is defined as 'the ability of the public agencies to work together towards mutually beneficial and agreed common goals of providing public services from multiple disparate & diverse public agencies to all other stake-holders like the Citizen and the Business'.

7) What is Enterprise Architecture?

While standards and guidelines form a framework, to establish interoperability, another option to establish interoperability is by using Enterprise Architecture (EA); which takes a broader view of

interoperability – going beyond just the technical aspects. EA is generally preferred in enterprises where there is significant central control. EA is simply defined as (i) a set of centrally-controlled common ICT resources of the enterprise, (ii) defined-rules for their use and (iii) their relations with the business functions of the enterprise & also with the external environment which influences the business functions of the enterprise. EA fills the gap between business-policies of the enterprise and the implementation of service-policies. EA aims at aligning the business processes & goals of an enterprise with the applications & systems that constitute its technical infrastructure.

EA is the process of translating business vision & strategy of the centrally-controlled enterprise into effective business-change by creating, communicating and improving the key principles and models that describe the enterprise' future state and enable its evolution.

8) What is Federated Approach?

The Indian public agencies are not centrally-controlled like the enterprise; the public-agencies are organised in three-tier structure (which consists of Central Government, State Governments and Local Bodies) with due recognition to their own autonomies. India has adopted a federal form where there is a clear demarcation of subjects and powers between the Central Government, the State Governments and the Local Bodies. Hence, in devising an interoperability framework, administration of entire Government Structure need to be considered by respecting the autonomy of each public agency involved through a 'Federated Approach'. Such a 'Federated Approach' is more appropriate for the interoperability in e-Governance scenario like in India, where multi-level structure, horizontal (various central government ministries & departments) and vertical (central, state and local-bodies), exists.

Federated Approach helps to:

Facilitate integration of resources used for e-Governance from multi-level structure

Capture the benefits of both centralised and decentralised functions of the public agencies, in a way that balances the interests of the whole (of government) with the autonomy of public agencies.

9) What is Federated Enterprise Architecture

Federated Enterprise Architecture (FEA) is defined as an umbrella for explaining the relationships among the e-Governance projects from both centralised & decentralised, disparate & diverse, public agencies and managing their changes in federated approach. FEA fills the gap between service-policies of the public agencies and their implementation.

Deliverables of FEA include a common vocabulary (including agreed definition of terms), a set of common models (such as Business, Information/Data, Services and Technology), patterns & standards (to facilitate inter-agency collaboration) and Principles (for developing common Models, common Patterns and common Standards) so that interoperability is established at different levels.

10) What are the differences between FEA and IFEG?

The standards are organised according to 'technical layers' (or domains such as interconnection, data integration, information access and presentation, content management & meta-data and security) in IFEG documents brought out earlier. Whereas FEA uses 'services or life events' (such as income taxes, personal documents, vehicle registration, permits, certificates, etc.) to classify the standards; that is, standards are organised around services. In comparison with the earlier versions of IFEG, FEA also addresses additional interoperability flavours/aspects due to 'organisation/process' and 'data/semantic'.

For example, EU and Germany (SAGA) classify the standards based on services or life-time event. But most of the countries like UK, Australia, New Zealand, Denmark, Brazil, Malaysia classify the standards based on different layers of IFEG.

Though old versions of IFEG from most of the countries covered only the technical interoperability flavour/aspect with 5 layers/domains, newer enhanced-versions of IFEG from some countries (Denmark, New Zealand, UK) are trying to address missing interoperability flavours/aspects due to 'organisation/process' and 'data/semantic'; additional layers/domains like Business services, Web-based Services, Best-Practice, Application are also included. The differences between IFEG and FEA are getting minimised over the period.

11) Describe 'Indian Official Languages'

The Eighth Schedule to the Indian Constitution recognises the following 22 list of scheduled languages at the time of preparation of this report. Inclusion in this list meant that the language was entitled to representation on the Official Languages Commission, and that the language would be one of the bases that would be drawn upon to enrich Hindi, the official language of the Union. Assamese, Bengali, Bodo, Dogri, Gujarati, Hindi, Kannada, Kashmiri, Konkani, Maithili, Malayalam, Manipuri, Marathi, Nepali, Oriya, Punjabi, Sanskrit, Santhali, Sindhi, Tamil, Telugu and Urdu.

Reference: http://lawmin.nic.in/coi/EIGHTH-SCHEDULE.pdf

12) What are the additional interoperability layers included in recent IFEG to address extra features available in FEA?

Business Services Layer

The Business Services Layer are meant to support exchange of XML-based specific content-related information in business areas like financial, product, order functionality, e-learning, e-health, etc.

Best Practice Layer

Technical standards covered in other layers alone may not ensure interoperability; they may merely offer a common approach to manage and understand the context of the information exchange. Best Practice Implementations on e-Governance, as a common approach, can be used to complement and enhance the interoperability capabilities of technical standards.

E-Governance Infrastructure Services Layer

E-Governance Infrastructure Services include Wide Area Network, Government Data Centres, e-Governance Citizen Service Centres; these are implemented by public agencies for the use of stake-holders of e-Governance.

Web Application Services Layer

A set of standardised applications to connect and integrate web-based applications over the Internet.

Annexure IX: References

Institutional Mechanism:

Institutional Mechanism for e-Governance Standards Formulation

(https://egovstandards.gov.in/sites/default/files/Policy/Institutional%20Mechanism%20for%20Standards%20Formulation/Institutional_Mechanism_for_Standards_Formulation.pdf)

Policies

National Cyber Security Policy 2013

(http://deity.gov.in/content/national-cyber-security-policy-2013-1)

Policy on Adoption of Open Source Software for Government of India

(https://egovstandards.gov.in/sites/default/files/Published%20Documents/policy_on_adoption_of_oss_0.pdf)

Policy on Open Standard

(https://egovstandards.gov.in/sites/default/files/Policy/Policy%20On%20Open%20Standards/Policy_on_Open_Standards_for_e-Governance.pdf)

Manual on the Policy on Open Standard

(https://egovstandards.gov.in/sites/default/files/Policy/Policy%20On%20Open%20Standards/Manual_On_the_Policy_on_Open_Standards.pdf)

Standards

Technical Standards for Interoperability in India

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Technical%20Standards%20for%20IFEG/Technical_Standards_for_IFEG_Ver1.0.pdf)

Meta Data and Data Standards

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Metadata%20and%20Data%20Standards/MDDS_Demographic_Ver1.1.pdf)

Biometric Standards – Face Image

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Biometrics%20Standards/Face_Image_Data_Standard_Ver1.0.pdf)

Biometric Standards – Finger Print Image

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Biometrics%20Standards/Fingerprint_Image_Data_Standard_Ver1.0.pdf)

Biometric Standards – Iris Image

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Biometrics%20Standards/Iris_Image_Data_Standard_Ver1.0.pdf)

Font Standard

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Localisation%20&%20Language%20Technology%20Standard/Font/Fonts_Standard_Ver1.0.pdf)

Character Encoding Standard

(https://egovstandards.gov.in/sites/default/files/Published_Standards/Localisation%20&%20Language%20Technology%20Standard/Character%20Encoding/Character_Encoding_Standard_Ver1.0.pdf)

Guidelines:

e-Procurement

(https://egovstandards.gov.in/sites/default/files/Guidelines/e-Procurement%20Guidelines/e-Procurement_Guidelines.pdf)

Indian Government Web Sites

(https://egovstandards.gov.in/sites/default/files/Guidelines/Guidelines%20for%20Indian%20Government%20Websites/GOI_Web_Guidelines.pdf

Digital Signature

(https://egovstandards.gov.in/sites/default/files/Guidelines/Digital%20Signature/Digital_Signature_Certificate_Interoperablity.pdf)

National e-Governance Authentication Framework (NeAF)

(http://www.mit.gov.in/sites/upload_files/dit/files/DraftNeAF1911.pdf)

Gateways

NSDG - National Services Delivery Gateway (http://www.nsdg.gov.in/)

SSDG - State e-Governance Services Delivery Gateway

Others

'A Comparative Analysis of National Interoperability Frameworks' by Yannis Charalabids, Fenareti Lampathaki & Dimitris Askounis (AMCIS 2009 Proceedings)

(http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1683&context=amcis2009)

UNDP - e-Government Interoperability: A Review of Government Interoperability Frameworks in Selected Countries, 2007

(http://www.unapcict.org/ecohub/resources/e-government-interoperability-a-review-of)

e-Government Interoperability - UNDP - e-Primers for the Information Economy, Society and Polity, 2008

(http://unpan1.un.org/intradoc/groups/public/documents/UN-OTHER/UNPAN032094.pdf)

Governance of Interoperability in Intergovernmental Services Towards an Empirical Taxonomy - Prof. Dr. Herbert KUBICEK, Dept. of Computer Science, University of Bremen, Am Fallturm 1, D-28359 Bremen, Germany.

(http://www.iiisci.org/journal/CV$/sci/pdfs/QP279YE.pdf)

Governance in Interoperability is Key to Success, From Fall 2008 TechBeat, A program of the National Institute of Justice, USA

(http://www.justnet.org/pdf/Governance.pdf)

Centre for Medicare & Medicaid Services – XLC Project Process Agreement.

(http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/PPA.html)

Mozambique IEFG

(http://www.portaldogoverno.gov.mz/docs_gov/outros/eGIF4M_v1_1web.pdf)

Annexure X: List of Contributors

Expert Committee Members

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

Other Core Contributors

1	Ms. Aruna Chaba, Former Senior Consultant, NICSI, New Delhi
2	Ms. Kavita Bhatia, Scientist-E, DeitY, New Delhi
3	Dr. Meenakshi Mahajan, Scientist-F, NIC-HQ

Other Contributors

1	Ms. Renu Budhiraja, Sr. Director, DeitY, New Delhi
1	Dr. VSR Krisnhiah, Sr.TD, e-Gov Stds, NIC-HQ
3	Mr. S.Senthil Kumar, Scientist-E, Chennai
5	Mr. Rajesh Loona, Senior Consultant, DeitY, New Delhi
4	Ms. Anita Mittal, Former Senior Consultant, DeitY, New Delhi
4	Mr. C.Senthil Kumar, Former Research Scientist Grade-I, OTC project, NIC Chennai
5	Ms. Sidhi Sehgal, Former Research Scientist Grade-I, OTC project, NIC Chennai
6	Ms. Supriya Kukreja, e-Gov Consultant, New Delhi