Ray, D., Gulla, U. & Dash, S.S. (2011). The Indian Approach to e-government interoperability, *JOAAG*, Vol. 6. No. 1

The Indian Approach to e-government Interoperability

Diakar Ray[1]

Umesh Gulla

Shefali S Dash

Abstract

Importance of interoperability of information systems in government is well recognized now. Over the globe, several countries have initiated Interoperability 'frameworks and enterprise architecture' as main tool for tackling problem of heterogeneity among government information systems. India, like many other countries is in the process of developing interoperability framework and enterprise architecture. This article analyses various interoperability frameworks and enterprise architectures to identify their salient features. Given the background of Indian effort towards achieving interoperability is highlighted. The study shows that Indian interoperability initiatives have been institutionalised with proper support from government and is part of the most important government initiatives – the NeGP. Standardisation initiatives in different interoperability domains like technical, semantic and organization have been initiated and some of them are found to be quite substantial.

Keywords: India, e-governance, interoperability, enterprise architecture

[1] Research Scholar at Guru Gobind Singh Indraprastha University, Delhi, India

This article represents the personal views of the authors and in no way reflects the views of the organisations the authors have connections with.

Introduction

High importance is given by Indian governments to e-government service delivery to its citizens and businesses. Initial initiatives towards e-government in India were focused on computerization of government departments. Application developments during the 1970's, 1980's and early 1990's was mainly related to automation of internal operations of government departments (Mathur, Gupta, Sridevi, 2009). A watershed in e-government initiatives in India came with setup of National Informatics Centre in early 1970s (Gupta, 2010). During the eighties setting up of computer networks by NIC up to district level was a very important step in the e-government history of India. Thus IT supported by the communication technologies created the right environment for providing e-government services on pan India basis. Eagerness to provide electronic services to its citizen backed by political support and citizen's demand, resulted in mushrooming of e-government services at centre state and district levels. But these isolated efforts have resulted in islands of e-government projects in the country at the national, state, district and even block level. Some of these projects have been highly successful and are ready for replication across other states. Experiences from successes as well as the failures of the various initiatives played an important role in shaping the e-government strategy of the country and at the policy level. It was felt a need for a more holistic approach towards e-government initiatives. It was realized that a programmed approach with a common vision, strategy and objectives is required to make e-government a success at various government levels. With this background, the National e-Governance Plan (NeGP) was formulated by the government on May 18th, 2006 for implementation across the country.

The plan envisages creation of the right environments to implement G2G, G2B, G2E and G2C services (http://www.mit.gov.in/content/national-e-governance-plan). NeGP takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. Such an approach among other things is expected to enable interoperability through use of standards etc, which would result in the citizen having a seamless view of government. Centrality of interoperability in the NeGP is further manifested by the fact that 'standards' is one of the five 'others plan components' of NeGP. Under 'standards plan component' various working groups and task forces have been constituted to formulate guidelines and standards for e-government initiatives. Adoption of standards is expected ensure interoperability of different information systems of government.

To ensure interoperability among applications, the Government of India has setup an institutional mechanism for formulation of standards through collaborative efforts of stakeholders like Department of Information Technology (DIT), National Informatics Centre (NIC), Standardization Testing and Quality Certification (STQC), other government departments, academia, technology experts, domain experts, industry, BIS, NGOs etc. In this process there is a provision of formal public review also (http://egovstandards.gov.in/). STQC, the constituent of DIT is responsible for release of approved standards, and also their versions control. Accordingly, an interoperability framework and enterprise framework are being developed. These documents are currently at the draft stage (http://www.mit.gov.in/content/status-standards). At the policy level the Government of India has already come out with a draft policy on open standards for e-government.

The 'National Policy on Open Standards for e-Governance' provides a set of guidelines for the uniform and reliable implementation of e-government solutions. It is expected that adoption of open standard would ensure seamless interoperability of various solutions developed by multiple agencies. It also aims to improve the technology choices available and avoid vendor lock-in. The policy document among other things delineated mandatory and desirable characteristics of standards to be used while selecting standards for e-government projects (Government of India, 2008).

For analysing India's interoperability framework, an analytical framework developed (Ray, Gulla, Gupta, and Dash, Forthcoming) is used. In addition to the interoperability framework, other standardization efforts are included into the study to get a complete picture of the current interoperability landscape at policy and implementation level.

Analytical Framework

The analytical framework is based on three core areas of interoperability frameworks, viz. context, content and process. Context defines the 'why', content defines the 'what' and process defines the 'how' of the framework. Each of these dimensions is further subdivided into sub-dimensions. The context domain has two sub dimensions – background and interoperability concept. Content domain consists of - basic interoperability policies, standards selection criteria, open standards definition and technology standards. The process domain has two sub categories - standards lifecycle, management and compliance policies. The criteria 'background' captures the background information of the government interoperability frameworks (GIF) in a free flow form for analysis. Technology standards are classified in a six layered e-government architecture to check its completeness. For rest of the criteria the absence or presence of specific features in the GIF is marked against the sub criteria defined in the analytical framework. Figure 1 describes the analytical framework.

The constituents of the e-government architecture used for analysing technology standards covered in the interoperability frameworks are – presentation, content management, application integration, data exchange, interconnection and security layers. Figure 2 gives details of the proposed architecture, with a description of each layer.

Technologies adopted at each layer would have different implications for different types of government interactions. For example, standards adopted at 'presentation layer' have a very high impact on G2C interoperability. Similarly technology adopted at 'e-government layer (web-enabled e-government service layer)' would have significant effect on the G2G interaction. In order to be truly interoperable, interoperability framework should cover standards for all the layers of the architecture.

Figure 1. Analytical Framework for Analysing Interoperability Frameworks

Background– Context of a GIF is captured in free flow text.

Interoperability Concept

- Interoperability definition – descriptive
- Interoperability dimensions - (presence of an attribute is marked as ■)
  - Organizational –
  - Semantic –
  - Technological

Scope - (presence of an attribute is marked as ■)

- Government to Government (G2G)
- Government to Citizen (G2C)
- Government to Business (G2B)
- Government to Employee (G2E)
- Other Governments (OG)

Basic Interoperability Policies - (presence of an attribute is marked as ■)

- Alignment with the Internet - all the information systems in the government ministration must be in line with the main specifications used in the Internet and the World Wide Web.
- Adoption of XML as the primary standard for data integration and data management
- Use of browser as the key interface for all government information and services
- Use of metadata for government information resources.
- Use of a semantic initiative like a controlled vocabulary to be used as an encoding scheme for the metadata standards.
- Mandatory use of GIF
- Use of Open Standards.

Definition of Open Standards - (presence of an attribute is marked as ■)

- Interoperability (IN) – standards and specifications recommended must be relevant for interoperability at different e-government layers.
- Scalability (SC)- standards selected should not be a limiting factor and should be capable of supporting a small system evolving into a nation wide application.
- Openness (OP) – specifications must conform to open standards principles.
- Market Support (MS) – selected specifications should have wide ICT industry support.
- Security (SE) – standards must ensure reliable exchange of information that can take place in conformity with established security policies.
- Internationally recognized (IR) – use of such standards would make information exchange across international boundaries easier.
- Maturity (MA) – A standard is mature if it has reached its full natural growth or development.
- Privacy (PR) – The standards must guarantee privacy.

Continued….

Open Standards Definition - *(presence of an attribute is marked as ■*

- Accessible to everyone free of charge (FC) ,
- Remain free for perpetuity(FP),
- Unambiguous documentation - document everything in detail (DC),
- Free redistribution (FR),
- Free Reuse (RE),
- The intellectual property of a standard or of parts of the standard must be accessible without payment or royalty (IP),
- Developed based on Open Collaborative decision making process (OC),
- All interested parties are given the opportunity to participate in the standards development (PA),

Technology Standards- (specifications described in the GIFs have to be classified into the following groups to see completeness)

- Presentation
- Content Management
- Application Integration
- Data Exchange
- Interconnection
- Security

Standards Lifecycle - (presence of an attribute is marked as ■)

Emerging -

- Future Consideration – A standard not yet reviewed but probably having potential.
- Under Review – A standard that is actively under assessment by GIF for future adoption.

Current -

- Adopted – These standards are mandated and represent the preferred solution.
- Recommended – These standard are emerging from the development and review. Recommended standards are generally more recent, based on newer technologies or standards. The difference from ‘Adopted’ is that of degree of maturity.

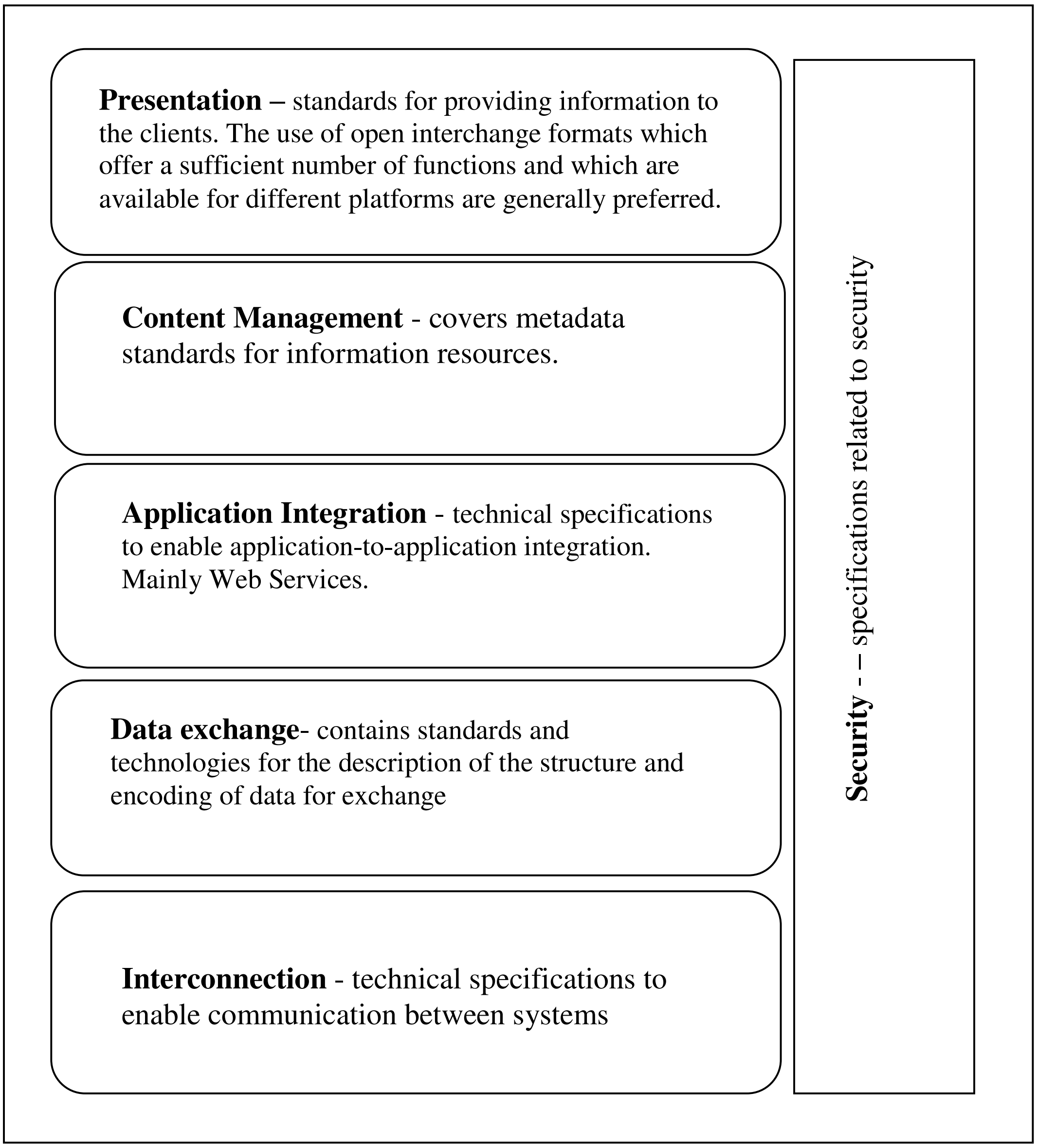
Fading -

- Undergoing Transition –not recommended because it does not meet one or more requirements of the selection policy. It is included in the GIF due to its existing significant use, and would be deactivated as soon as another specification is available to replace it. New use of this standard is discouraged.
- Deprecated **-** represents standards those have been abandoned or superseded by a better solution at the Adopted or Recommended levels. Agencies should plan to migrate away from solutions involving the standard as soon as practical. New use of this standard is discouraged.

Management and Compliance Policies - (presence of an attribute is marked as ■)

- Specific agency responsible for managing technical specifications (AG)
- Change Management procedure. (CM)
- Frequency of Review (FR)
- Compliance Policy (CP)
- Compliance Responsibilities (CR)

Figure 2. E-Government Technical Architecture



Presentation – standards for providing information to the clients. The use of open interchange formats which offer a sufficient number of functions and which are available for different platforms are generally preferred.

Content Management - covers metadata standards for information resources.

Application Integration - technical specifications to enable application-to-application integration. Mainly Web Services.

Data exchange- contains standards and technologies for the description of the structure and encoding of data for exchange

Interconnection - technical specifications to enable communication between systems

Security - – specifications related to security

Indian Interoperability Framework

In the following paragraphs Indian interoperability framework the 'Interoperability Framework for e-Governance (IFEG)' is analysed against the parameters of the analytical framework.

Background

Interoperability, as already mentioned, is an important component of NeGP. Under NeGP standards in e-governance are a high priority activity, which will ensure sharing of information and seamless interoperability of data and e-governance applications. The E-Government Standards initiative under NeGP e-governance standards are being developed for network and information security, local language, meta data and data standards for application domains, and quality. Recognizing the critical role that well designed standards and architecture play in the rapid growth of e-governance, the Department of Information Technology (DIT), has constituted an “Apex Body on Standards in DIT” in September 2005, among other things, to design the broad policy framework for setting as well as development of standards for the e-Governance initiatives in India. As a part of the e-Governance Standards initiative A draft interoperability framework for e-Governance has been prepared. The draft interoperability framework is known as Interoperability Framework for e-Governance (IFEG). The last available version is Draft Version 0.6, 2010 (http://egovstandards.gov.in/TechInteroperability) . The first version of IFEG prepared by NIC was released in 2004 (National Informatics Centre, 2009). IFEG is developed under a workgroup setting with experts from both government and industry.

IIFEG recognizes the importance of a framework initiative to support the flow of information and to improve the coherence of Information systems maintained by individual ministries and departments. As one of its objective, IFEG envisages creation of a common basis across the government and public sector for the cost-effective delivery of e-Governance to the public and other end users. IFEG contains an appropriate set of policies and specifications and guidelines governing the information flow across various Government sector agencies.

Interoperability Concept

IFEG defines interoperability from a technical point of view. IFEG defines interoperability as the ability of two or more information and communication technology (ICT) devices (hardware devices, software components, and communication devices) to seamlessly work together. Interoperability definition of IFEG also refers to the IEEE definition of interoperability. IEEE definition which includes the concept of the use of the information exchanged and indicates the acknowledgement by IFEG towards the existence of semantic dimension of interoperability. This is because the use of exchanged information requires that the information is understood by applications those of which were not initially developed for this purpose (Guijarro, 2009). Inclusion of a data integration layer in the IFEG also supports this hypothesis. However, policies discussed and standards included (like XML schemas) under data integration layer indicates an approach towards syntactic interoperability rather then true semantic interoperability.

Table1. Interoperability concepts as described in IFEG

Definition	OR	SM	TE
“The term Interoperability in technological perspective refers to the ability of two or more Information and Communication Technology (ICT) devices (Hardware devices, Software components, and Communication devices) to seamlessly work together” (IFEG, Version 2.4, page 6)		■	■

OR- Organizational Interoperability; SM- Semantic Interoperability; TE – Technical Interoperability

Scope

The objective of IFEG is defined as the enabling of interoperable services between public administration agencies, as well as between the administrations and the public (citizens and business enterprises) (see Table 1). This indicates the scope of the IFEG as G2G as well as G2C and G2B. Although not mentioned in IFEG, coverage of Government to Employee (G2E) is mentioned in the Draft Policy on Open Standards for e-Governance.

Basic Interoperability Policies

Like other GIFs basic interoperability policies adopted by IFEG are: adoption of web based standards, use of XML as data exchange standard, use of open standards, use of metadata standards, and mandatory compliance of interoperability framework. Findings are summarized in Table 2.

Table 2. IFEG Scope and Basic Interoperability Policies

Evaluation Criteria											
Scope					**Basic Interoperability Policies**						
G2G	G2C	G2B	G2E	OG	Alignment with Internet	Adoption of XML	Use of Browser	Use of Metadata	Semantic Initiatives	Mandatory use of GIF	Use of Open Standards
■	■	■	■		■	■		■		■	■

Standards Selection Criteria

Scalability, security and reliability are preferred characteristic of standards are key principles for adoption of standards. Other criteria like single open standards for a particular field and standards with multiple implementations are other selection criteria mentioned in IFEG (see Table 3).

Table 3. IFEG Standard Selection Criteria

Standard selection criteria							
Interoperability	Scalability	Openness	Market Support	Security	Internationally Recognized	Maturity	Privacy
	■	■		■			

Open Standards Definition

The definition of open standards is not covered in IFEG. However, the Draft Policy on Open Standards for e-Governance, published by Department of Information Technology (Government of India, 2008), provides the open standards selection criteria. The main criteria are: free and royalty free access for life time, open and collaborative development, free for perpetuity, open and collaborative decision making, and complete description of the standards be available in public accessible form. The draft policy also defines additional criteria like compatibility with domestic law, availability of same capability world wide, superior to already adopted standard and capability to support for all Indian languages (see Table 4).

Table 4. IFEG Open Standards Definition Criteria

Open Standards Definition Criteria								
Free Access	Free for Perpetuity	Unambiguous Documentation	Free Redistribution	Free Reuse	Without Royalty	Open Decision Making	Opportunity to Participate	International Standard Bodies
■	■	■			■	■		

Technology Standards

The interoperability architecture proposed in IFEG has four primary domains – access, presentation, process, and data integration. The access layer covers standards and specification required for achieving interoperability between different access media and applications. The presentation layer handles representation of information and data to the end user. The process layer contains standards related to aggregation and integration of services and business functions. The data layer handles the core transactional data of an application. Three more domains, namely, communication, network and security are common across all the applications and depict the communication medium for an application, the network on which an application operates and the security infrastructure of an application.

Although the domains described in IFEG does not corresponds one to one with the layers of e-government technical architecture described in Figure 2, coverage of standards and specifications is exhaustive and covers all the e-government layers. For example, standards covered under communication, network and information access and information domain - data interchange of IFEG corresponds to the interconnection layer of the e-government technical architecture.

IFEG, in addition to the domains mentioned earlier covers to other domain important from interoperability point of view. They are - National Services Delivery Gateway (NSDG) and data preservation standards. Between these two the NSDG is worth special mention. The NSDG, a Misson Mode Project under the NeGP, is expected to simplify the problem of heterogeneous systems and technologies across different departments in the centre, states and local government by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across all areas. IFEG defines specifications for eGov MessagingServic e Specifications (eGGMS) under the gateway domain. These specifications are interoperability interface protocol (IIP), interoperability interface specifications (IIS) and inter gateway interconnect specifications (IGIS).

Table 5. Technical Standard covered in IFEG

e-government Technical Architecture Layer	Corresponding layer in IFEG	Standards
Interconnection - technical specifications to enable communication between systems.	Communication; Network; Information Access ; Information Domain - Data Interchange	HTTP, IPV4. IPV6, LDAP, FTP, SMTP, POP, Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), Web service request registry, Web Services WS-I, Web Services Security
Data exchange – contains standards and technologies for the description of the structure and encoding of data for exchange.	Information Domain - Data Integration	Extensible Markup Language (XML), Extensible Style sheet Language Transformations (XSLT), UML, Schema Definition (XSD),
Content management metadata – meta data standards for information resources.	Information Domain - Metadata	Resource Description Framework (RDF), The XML Metadata Interchange (XMI).

Application integration - technical specifications to enable application-to-application integration	Process	Web Services. MOM, CORBA, Business Process Execution Language for Web Services (BPEL4WS), Web Services (SOAP, WSDL, UDDI)related Standards,
Presentation – describe standards for providing information to the clients. The use of open interchange formats which offer a sufficient number of functions and which are available for different platforms is generally preferred.	Presentation	UNICODE, UTF-8/16, HTML, XHTML, Cascading Style Sheets, XForms, WML, Ecma Script / Javascript , JPEG, GIF, PNG, TIFF, MPEG, RealAudio /RealVideo, Text File (.txt), PDF
Security	Security	SSH, Secure Electronic Mail, HTTPS, IPSec, SSL, Symmetric Encryption Algorithms, Digital Signature Algorithms, SHA-1, MD5, KCS#5, KCS#7, SAML

Standards Lifecycle

IFEG defines two types of standards, viz. mandatory and recommended. Although IFEG does not define a very exhaustive standards lifecycle management procedure as GIF of Germany, Greece and New Zealand, IFEG does define a simple procedure for the standards adoption process. The life cycle management procedure starts with reviewing of the standards set by the working group responsible for managing inclusion and removal of standards. At this stage a standard is under observation. Also at this stage, the group may either accept or reject the standard. In case a standard is rejected, it is marked in to the black list. Accepted standards can be either mandatory or recommended. Recommended standards are those where more than one standard is specified. Table 6 represents the findings. Mandatory is marked as 'adopted' and under observation is marked as 'under review' in the table.

Table 6. IFEG- Standards Lifecycle Management

Standards Life Cycles					
Emerging		**Current**		**Fading**	
Future Consideration	Under Review	Recommended	Adopted	Undergoing Transition	Deprecated
	■	■	■		

Management and Compliance Policies

The IFEG does not mention anything about a compliance policy other than suggesting that IFEG should be made mandatory. Another related document "Technical Standards and E-Governance Architecture - Approach Paper" (Pyarelal, 2005) gives details of the constituents of the working group responsible for managing interoperability framework. The document also defines the change management procedure. However, IFEG and the other document do not provide information on – frequency of review, compliance policy, compliance responsibility and procedure for exception of compliance.

Table 7. IFEG Management and Compliance Policy

Management and Compliance Policies					
Specific Agency	Change Management Procedure	Frequency of Review	Compliance Policy	Compliance Responsibility	Exception of Compliance Procedure
■	■				

Enterprise Architecture

An enterprise architecture (EA) framework for e-Governance is under preparation (DIT, n.d). Objectives of the architecture are – (1) to align the business goals to IT architecture, (2) to establish a common vocabulary to share information across multiple applications and (3) to provide a roadmap to make organisations more responsive to new and changing requirements, and (4) to enable organisations with new ways of collaboration and managing future change (Pyarelal, 2008). The expected is that the architecture would highlight the interdependencies in service delivery across ministries and within ministries beyond the traditional program delivery boundaries. The framework is also expected to provide a systematic way for government ministries/departments to describe their business using a common language and to identify gaps in service delivery models (Pyarelal, 2007).

The architecture has six components – vision, plant & programs, organization, data, process, technology, service and security architecture (Pyarelal, 2008). Enterprise Architecture Working Group, Subgroup I has developed an early draft version of the Enterprise Architecture Model (Ratan*, 2006*). The draft document defines the components in details, which is described below –

> Vision, plans and programmes – is the 'why' of the enterprise. The component defines the strategic intent of the enterprise. Vision, plans and programmes ensures that the end outcomes drives the technology and aligns objectives and IT.
>
> Organisation architecture - is the 'Who' of the organization and provides detailed structure of the organisation with a clear definition of roles and responsibilities. One of the purposes of the architecture is to establish appropriate resource levels and reconcile contention and set priorities. The architecture helps to align business and organisation with strategies, policies and plans.
>
> Data architecture – is the what of the enterprise. Data architecture defines what information the institution needs to carry out its processes. Having an enterprise view of the data asset, data architecture helps to avoid stovepipe systems containing redundant data. Data Architecture has four components - conceptual data model, logical data model (more detailed), physical data model (implementation level) and cross-reference of data classes to processes.
>
> Process architecture – is the conceptual how of the institution. Process architecture defines what the enterprise does to fulfil its strategic intent and meet the needs of its stakeholders. Process architecture ensures that the enterprise's activities contribute towards accomplishing its objectives and also provides an opportunity for process improvement.
>
> Technology architecture (incl. application architecture) - defines the major types of technologies needed to provide services and fulfil organizational objectives. Technology architecture promotes enterprise wide standards. Application architecture defines the types of applications needed to manage the data and support the processes of the Institution. Application architecture is the automated how of the enterprise and it helps to plan interoperability among applications and avoid stovepipe applications.
>
> Services architecture – provides a citizen's view of the services and the components required to deliver the same. It is the functional framework that classifies service components with respect to how they support service process and performance objectives.

Security architecture - Identifies criteria and techniques associated with protecting and providing access to information resources. It facilitates identification, authentication, authorization, administration, audit, and naming services.

Although not fully developed the organization, data, process, and technology are comparable with business, service, data, and technical reference models of FEA. So it can be inferred that the EA of India suggests interoperability through Government wide description of Business, by use of commons data, process and technology standards. Service oriented architecture (SOA) is also promoted to be an important component of e-Governance architecture in order to encourage reuse of software components within government.

Semantic Interoperability Initiatives

Department of Information Technology has identified 'metadata and data for application' domain as one of the areas which require urgent attention. Accordingly, a working group with representation from the IT Ministry, academia, industry etc was formed for standard formulation. Recently the experts' committee on metadata and data standards have come up with draft version of Standards for Person Identification, and Land Region Codification.

The draft Land Region Codification (Expert Committee on Metadata and Data Standards, 2008a) standard provides attributes of an address location for a premise and provides code directories and the owner/s. The draft standard provides a unique code and description of land region and locations of various premises like buildings, establishments, residential /non-residential units, commercial units, institutes, and markets etc. Most of the codes used here are based on those used by office of Register General & Census Commissioner Office, India (RGI), who have wide experience in developing and managing such location based codes. The draft version of the Person Identification Codification standard (Expert Committee on Metadata and Data Standards, 2008b) attempts to identify a citizen uniquely at the national level to ensure interoperability of information related to individuals collected by various govt./non govt. organizations. The standard provides attributes required to capture personal identification, related codes and ownership of the code directories. For this standard too, instead of generating code directory on its own ownership of the code directories is assigned to organizations that have expertise in that particular domain. This would ensure better management of these code directories.

As personal identification and their address are one of the most common pieces of Information collected and exchanged by government agencies for providing various services, standardisation of them would help interoperable data exchange among government departments. The final version of Data Standards for Person identification and Land Region Codification has recently be published and notified by Department of Information Technology for use for data exchange in all e-government applications (http://www.mit.gov.in/content/status-standards).

Other Interoperability Initiatives

Over and above mentioned interoperability initiatives, the Government of India has initiated standardisation activities in other areas like localization and language technology standards, network and information security, digital signature, quality & documentation and biometrics standards.

Given the requirements of providing government information and services in local languages, standardisation efforts in 'localization and language technology' standards becomes important in the Indian scenario. The Department of Information Technology has notified ISO/IEC-14496-

OFF (Open Font Format) and Unicode 5.1.0 as Localization and Language Technology Standards for e-government applications (http://www.mit.gov.in/content/status-standards).

Under 'information security standards and guidelines for e-government', the government has published an approach paper on e-Governance Security Standards Framework (eSAFE). eSAFE is based on ISO 27001 and is in line with the Information Security Program for Federal Information Systems in USA. Six guideline documents under the 'information security standards', were published on the standards portal (http://egovstandards.gov.in) on Feb 26, 2010 for implementation of ISO 27001. These documents are: Information Security Assessment Framework; Guidelines for Security Categorization of Information Systems; Catalog of Security Controls; Baseline Security Controls for Low Impact Information Systems; Baseline Security Controls for Medium Impact Information Systems; and Baseline Security Controls for High Impact Information System.

To ensure interoperability of digital certificates issued by various certifying authorities, interoperability guidelines for Digital Signature Certificate (DSC) has been published on the standards portal on Feb 16, 2010 (Controller of Certifying Authorities, 2009).

For 'quality & documentation standards', documents named Quality Assurance Framework and Conformity Assessment Requirements have been prepared and posted for public review. The Quality Assurance Framework (QAF) document enhances the e-Governance framework conditions in India to support the National e-Governance Plan's vision of providing reliable, cost-effective and transparent citizen services by applying international good practices and guidelines. The present QAF document prepared by STQC and by members of Working Group on Quality and Documentation. QAF addresses the Quality Assurance requirements in a project life cycle covering implementation, evaluation and conformation stages. On the other hand, the purpose of defining 'conformity assessment requirements' (CARE) is to enforce implementation of standards and best practices in e-governance solutions throughout the project lifecycle.

Standards in another important area of e-government application, viz., biometric standards for facial image, finger prints and minutia is under preparation.

Analysis of the Findings

India, like many countries, has initiated many important steps towards achieving interoperability of the information systems. Most early and important initiative is the e-government interoperability framework. While other GIFs define the interoperability policies and catalogue of technical standards, the interoperability concept presented in the IFEF is mainly technical in nature. However standards selected and data standardization initiatives indicate that semantic interoperability has also been recognized as an important parameter of interoperability. The interoperability policies and open standards selection criteria described in IFEG also are in the line with GIF of other countries.

Recent development indicates that India government initiatives shift from developing a complete GIF to developing standards in individual problem areas. For example, the government has already come up with standards for 'localization and language technology' standards, 'network and information security' etc. Above all, India has decided to use open standards for all new e-government systems (Government of India, 2008) and has clearly defined criteria for selecting an open standards. This draft policy would make it easier for standard selection bodies to select standards for any area much easier.

For non technical area like data standardisation for ‘person identification, and land region codification’ are major achievements. These data are generally the most commonly found data exchanged among government departments. However, so far, there is no major effort in the area of semantic interoperability. At the present juncture metadata standards for information resources is the primary requirement. However, it is expected that National Portal India project, an important NeGP, would soon come up with such standards (National Portal Team, 2007; National Portal Secretariat, 2009). Another requirement is that of a standard vocabulary of government services in same line as that of Integrated Public Sector Vocabulary (IPSV). It is expected that such standards would soon be available to enable the Indian government to provide integrated service and information to the citizens and businesses alike.

Another important step taken by the Indian government is the setting up of the e-Governance Standards Portal (http://egovstandards.gov.in). The e-Governance Standards Portal is setup in order to provide a platform for sharing of ideas, knowledge, and draft documents among the various people involved in the standards formulation process. Draft standards are published here by the closed user group and the public. Final version of the standards and specifications are made available at the STQC website (http://www.stqc.nic.in/index3b35f.html).

EA is the preferred tool for achieving organizational interoperability. Evidence suggests that India already has initiated steps towards development of EA. First at the policy level the institutional support has been ensured for EA by making it a part of the NeGP. At the operational level the objectives and the architectural components of the EA have already been identified (Payarelal, 2007). So it may be expected that full EA would be made available soon. EA, along with the complete semantic initiatives, would make interoperability of government information systems a reality.

Conclusion

After exploration of interoperability initiatives of various national governments all over the world, this paper explores interoperability initiatives taken up by Indian government. This paper began by discussing the NeGP program and the important position interoperability holds in the whole program. Next the paper described the Indian interoperability framework within the interoperability framework for e-Governance (IFEG). Different characteristics of the IFEG are evaluated using an analytical framework. The nine evaluation criteria used for the study were – background; interoperability concept; standards selection criteria; open standards definition; technology standards; standards lifecycle; management and compliance policies. The draft policy on open standards is found to be an important step taken by government of India in achieving interoperability at technical level. The next step explores the enterprise architecture (EA) initiative of India. The objectives and the components of the EA are described. Analysis of semantic interoperability initiatives show that quite a lot has been done in data standardisation of the person identifier and land region identification. However it is found that true semantic initiatives like standard vocabulary is still missing. Next other interoperability initiatives in the area of network and information security, digital signature, quality and documentation were explored.

The study shows that Indian interoperability initiatives have been institutionalised with proper support from government and is part of the most important government initiative – the NeGP. Standardisation initiatives in different interoperability domains like technical, semantic and organization have been initiated and some of them are found to be quite substantial.

References

Controller of Certifying Authorities 2009. Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, Version 2.0. Retrieved December 7, 2009, from http://egovstandards.gov.in/egscontent.2010-02-15.5232763495/at_download/file

Expert Committee on Metadata and Data Standards. 2008a. Land Region Codification. Draft Version 0.9, August 2008. Retrieved December 7, 2009, from http://egovstandards .gov.in/public-review/egscontent.2008-09-04.2547401347/at_download/file

Expert Committee on Metadata and Data Standards. 2008b. Person Identification Codification. Draft Version 0.8, August, 2008. Retrieved December 7, 2009 from http://egovstandards.gov.in/public-review/egscontent.2008-09-04.3708808455/at_download/file

Government of India 2008. Draft Policy on Open Standards for e-Governance, Draft Policy Version 1.0. June 2008. Retrieved 23 Nov, 2009, from http://egovstandards.gov.in/public-review/egscontent.2008-08-22.3525430649/base_view

Guijarro, L. 2009. Semantic interoperability in eGovernment initiatives. *Computer Standards & Interfaces archive.* 31 (1), 174-180.

Gupta, M.P. 2010. Tracking the Evolution of E-Governance in India, *International Journal of Electronic Government Research (IJEGR),* 6(1), pp. 46-58.

Mathur, D., Gupta, P. and Sridevi, A. 2009. In Bagga, R.K. and Gupta, P.(Eds), *Transforming Government e-Governance Initiatives in India,* The ICFAI University Press, Hyderabad, pp. 3-50.

National Informatics Centre 2009. I F E G, Interoperability Framework for e-Governance, version 2.4. Government of India. Retrieved 14 Dec 2009 from http://www.cots.nic.in/IFEGV2.4.pdf

National Portal Secretariat 2007. National Portal of India: Content Framework. National Informatics Centre, New Delhi. Retrieved 12 Dec 2009 from http://india.gov.in/cfw/

National Portal Secretariat 2009. State Portal Framework, version 1.0. Available at http://spf.india.gov.in/

Pyarelal, S. 2005. Technical Standards And E-Governance Architecture: Approach Paper. Retrieved 24 Nov 2009 from egovstandards.gov.in/standards_technical_app

Pyarelal, S. 2007 January. Standards in E-Governance, Presentation at ELITEX' 2007. Retrieved 24 Nov 2009 from www.elitex.in/presentation2007/suchitrapyarelal.ppt

Pyarelal, S. 2008 July. Standards & Interoperability: for E-Governance, Presentation at Management Development Programme for NIC, 2nd July 2008. Retrieved 24 Nov 2009 from elearning.nic.in/mdp/5-e-gov-standards/1-mdp_e_gov_sp1.pdf

Ray, D., Gulla, U., Gupta, M. and Dash, S. (Forthcoming), A Critical Survey of Selected Government Interoperability Frameworks, Transforming Government: People, Process and Policy

Ratan, N. 2006. E-Governance Architecture Framework: Components Defined, Working Draft, Subgroup I- Enterprise Architecture Model.