

Version
1.0

I F E G

**Interoperability Framework
for
E-Governance
Technical Standards**



Government of India
Ministry of Communications and Information Technology
Department of Information Technology
National Informatics Centre

INTEROPERABILITY FRAMEWORK FOR ELECTRONIC GOVERNANCE (IFEG)

Prepared by: IFEG Standards Team

Reviewed by: IFEG Review Team

Approved by: Director General

**No part of this document shall be reproduced without prior permission of
Director General, National Informatics Centre**

Amendment Log

| Version No. | Date | Change Number | Brief Description | Sections Changed |
|-------------|-----------|---------------|---|-------------------|
| 0.2 | 10-May-04 | 1 | Foreword brought to the Beginning of document and enhanced. | -- |
| 0.2 | 10-May-04 | 2 | Executive Summary includes more focus on proposed way forward | |
| 0.2 | 15-May-04 | 3 | Role of NIC is enhanced and created as a new and separate section | 3.1 |
| 0.2 | 13-May-04 | 4 | The Definition of Interoperability is re-written. | 4.1 |
| 0.2 | 17-May-04 | 5 | Open standards and open source Section enhanced | 4.5 |
| 0.2 | 13-May-04 | 6 | Global Initiatives- Write up on Germany enhanced and Write-up on Italy and Australia included | 5.6, 5.7, 5.8 |
| 0.2 | 15-May-04 | 7 | Scope of IFEG modified | 6.3 |
| 0.2 | 19-May-04 | 8 | The IFEG Architecture Model modified | 9 |
| 0.2 | 18-May-04 | 9 | Process Definition re-written | 9.3 |
| 0.2 | 14-May-04 | 10 | Management Overview re-written | 9.10.1 |
| 0.2 | 17-May-04 | 11 | Additional Working group for managing the framework suggested | 12 |
| 0.2 | 10-May-04 | 12 | Two columns owner and Nature of Standard added in technical Standards table | 13 |
| 0.2 | 20-May-04 | 13 | Change Management added | 13.9.2 |
| 0.2 | 20-May-04 | 14 | Outsourcing and BPR added | 13.9.5, 13.9.6 |

| | | | | |
|-----|-----------|----|---|--------|
| 0.2 | 20-May-04 | 15 | Interaction with Legacy application added | 13.9.7 |
| 0.2 | 15-May-04 | 16 | Additional Working Groups suggested | |



| | |
|--|-----------|
| I F E G..... | 1 |
| Amendment Log..... | 3 |
| Foreword..... | 5 |
| Executive Summary..... | 7 |
| 1.Introduction..... | 8 |
| 1.1BACKGROUND INFORMATION..... | 8 |
| 1.2PURPOSE AND SCOPE OF THIS DOCUMENT | 8 |
| 1.3STRUCTURE OF THIS DOCUMENT..... | 9 |
| 2.E-Governance - Global Trends and National Initiatives | 11 |
| 2.1 E-GOVERNANCE OBJECTIVES AND POLICY ISSUES | 11 |
| 2.2QUALITIES OF E-GOVERNANCE SERVICES | 12 |
| 2.3E-GOVERNANCE: GLOBAL TRENDS..... | 12 |
| 2.4E-READINESS OF INDIA..... | 15 |
| 3. National Initiatives on E-Governance..... | 19 |
| 3.1ROLE OF NATIONAL INFORMATICS CENTRE (NIC)..... | 19 |
| 4 Overview of IFEG (Interoperability Framework for E-Governance)..... | 23 |
| 4.1INTEROPERABILITY..... | 23 |
| 4.2BENEFITS OF INTEROPERABILITY..... | 23 |
| 4.3SCOPE OF INTEROPERABILITY..... | 23 |
| 4.4DATA INTEROPERABILITY PROBLEMS AND STRATEGIES | 24 |
| 4.5OPEN STANDARDS AND OPEN SOURCE..... | 25 |
| 4.6THE INTEROPERABILITY FRAMEWORK (IF)..... | 25 |
| 4.7NEED FOR AN INTEROPERABILITY FRAMEWORK..... | 26 |
| 4.8IMPACT OF THE INTEROPERABLE FRAMEWORK..... | 27 |
| 4.9LEGAL ISSUES | 28 |
| 4.10PARTNERSHIPS WITH ICT INDUSTRY..... | 28 |
| 5.Global Interoperability Framework Initiatives | 29 |
| 5.1UNITED KINGDOM:..... | 29 |

| | |
|---|-----------|
| 5.2 THE NEW ZEALAND GOVERNMENT..... | 30 |
| 5.3 PAN EUROPEAN COUNTRIES..... | 31 |
| 5.4 MALAYSIAN GOVERNMENT..... | 31 |
| 5.5 GOVERNMENT OF THE HONG KONG..... | 32 |
| 5.6 GERMANY..... | 33 |
| 5.7 ITALY..... | 34 |
| 5.8 AUSTRALIA..... | 35 |
| 6 Interoperability Framework for E-Governance (IFEG)..... | 37 |
| 6.1 GOALS AND OBJECTIVES..... | 37 |
| 6.2 IEFG ARCHITECTURE..... | 38 |
| 6.3 IFEG GUIDING POLICIES..... | 38 |
| 6.4 SCOPE OF IFEG | 41 |
| 7. Management and Compliance of the Interoperability Framework (IF)..... | 42 |
| 8. Interoperability Technical Standards..... | 43 |
| 9. IFEG Architecture | 45 |
| 9.1 ACCESS..... | 46 |
| 9.2 PRESENTATION..... | 47 |
| 9.3 PROCESS..... | 48 |
| 9.4 DATA INTEGRATION | 49 |
| 9.5 DATA SCHEMA..... | 49 |
| 9.6 METADATA..... | 50 |
| 9.7 NETWORK..... | 54 |
| 9.8 SECURITY..... | 54 |
| 9.9 COMMUNICATION..... | 57 |
| 9.10 MANAGEMENT | 58 |
| 10. Software Architecture..... | 60 |
| 10.1 MIDDLEWARE AND TECHNOLOGY STANDARDS..... | 60 |
| 10.2 USING SERVICE-ORIENTED ARCHITECTURE(SOA) AND COMPONENT- BASED DEVELOPMENT TO BUILD WEB SERVICE APPLICATIONS..... | 60 |
| 10.3 COMPONENT WARE ARCHITECTURE..... | 62 |
| 10.4 REUSABILITY..... | 63 |

| | | |
|------------|---|-----------|
| 11 | Supporting Network Architecture | 64 |
| 12 | Implementation Plan..... | 65 |
| 12.1 | IFEG ADVISORY GROUP | 65 |
| 12.2 | DATA STANDARDS WORKING GROUP:..... | 65 |
| 12.3 | SCHEMAS WORKING GROUP..... | 65 |
| 12.4 | DOMAIN LEVEL STANDARDS FOR DATA AND METADATA..... | 66 |
| 12.5 | INTEROPERABILITY WORKING GROUP..... | 67 |
| 12.6 | WORKING GROUP ON GOVERNMENT PROCESS..... | 67 |
| 12.7 | COMPONENT LIBRARY WORKING GROUP..... | 67 |
| 12.8 | WORKING GROUP FOR LEGACY APPLICATIONS..... | 67 |
| 12.9 | WORKING GROUP ON NETWORK LAYER..... | 67 |
| 12.10 | WORKING GROUP ON SECURITY LAYER..... | 68 |
| 12.11 | WORKING GROUP FOR AUDITING/REVIEW OF THE STANDARDS..... | 68 |
| 12.12 | GOVERNMENT PROCESS GROUP..... | 68 |
| 13 | Technical Standards Specifications for IFEG | 69 |
| 13.1 | ACCESS | 71 |
| 13.2 | PRESENTATION | 75 |
| 13.3 | PROCESS..... | 78 |
| 13.4 | DATA INTEGRATION..... | 79 |
| 13.5 | DATA | 80 |
| 13.6 | META DATA..... | 82 |
| 13.7 | NETWORK | 83 |
| 13.8 | SECURITY..... | 83 |
| 13.9 | COMMUNICATION | 89 |
| 13.10 | MANAGEMENT | 91 |
| 14. | Annexure..... | 96 |
| 14.1 | ANNEXURE 1 -ADDITIONAL REFERENCES..... | 96 |
| 14.2 | ANNEXURE 2: GLOSSARY OF TERMS..... | 97 |
| 14.3 | ANNEXURE 3 QUICK REFERENCE GUIDE FOR STANDARDS..... | 103 |
| 14.3 | ANNEXURE 4: TABLE OF MISSION PROJECTS OF DIT FOR NATIONAL E-GOVERNANCE..... | 104 |
| | | 105 |

FOREWORD

Though relatively new, the powerful E-Governance concept promises many benefits to various sectors. E-Governance makes it easy for citizens to do business with the Government; reinforce relationship between citizen and democratic Government; and reduce costs of Government operations. Information Communication Technology (ICT) is the cornerstone of E-Governance, providing an amazing opportunity to alter how public services are delivered.

E-Governance application architecture requires that it have a well-defined set of rules to drive both the integration between specific Government functions ('vertical' applications) and shared Government functions ('horizontal' applications) and data sharing between applications. It is also necessary to define a set of rules for interoperability and workflow coordination between different Government functions, as the need for interoperability and the multifaceted benefits it could usher are now widely recognized. Such a framework is now firmly established as the cornerstone of all E-Governance strategies.

National Informatics Centre (NIC) has always been in the forefront to help automate Government businesses and has significantly contributed to ICT-led developmental functions at the Central and State Governments level. Having developed a large number of E-Governance applications and generated a huge inventory of ICT solutions, NIC recognizes the importance of interoperability across these applications mainly to reduce administrative and software costs to Governments. NIC further considers that it should take a major initiative to evolve an Interoperability Framework for all E-Governance applications developed in-house. The foremost thrust of this framework is to adopt Internet and World Wide Web Standards for all applications developed by NIC for Government systems.

This document, an outcome of considerable thinking and effort, examines various aspects of Interoperability Framework for E-Governance and attempts to define specifications and standards for the framework. It shall be NIC's endeavor to take this initiative forward and disseminate the framework for wider acceptance across the country.

Director General, NIC

Executive Summary

Provision of quality services tailored to the needs of the citizen and businesses is the primary objective of E-Governance. Ensuring seamless flow of information is a prerequisite for effective E-Governance and as such, it is founded on highly efficient Information and Communication (ICT) Technology infrastructure.

There is an increasing awareness that the interoperability of national public ICT infrastructures is a precondition for successful E-Governance. This is achieved by evolving a framework that sets standards and specifications for various aspects of ICT systems. Such an Interoperability Framework (IF) supports the E-Governance strategies of providing citizen-centric services by facilitating the interoperability of ICT systems between all the stakeholders of E-Governance. In addition to technology, this framework must also address both procedures and content.

The purpose of this Interoperability Framework for E-Governance (IFEG) is to establish an agreed set of technical policies and standards for achieving interoperability and coherence of ICT systems across all E-Governance applications developed by various NIC development teams geographically distributed across the country. The main thrust of this framework is to adopt the Internet and World Wide Web standards and specifications for all Government systems.

Many national Governments in developed and developing countries have either evolved or in the process of evolving Interoperability Standards for their E-Governance applications. While establishing this framework, standards and specifications adopted by different countries have been looked into. Those, which are considered relevant to the Indian context, have been absorbed and incorporated into this document.

1. Introduction

1.1 Background Information

The strategic and contemporary importance of E-Governance is now widely recognized globally. The emerging E-Governance practices are firmly founded on public ICT infrastructure. Various Ministries of the Government of India and a number of State Governments have taken many E-Governance initiatives to provide e-services to individuals and the private sector.

There is also a growing awareness among state administrators that interoperability of national ICT infrastructure is a necessary prerequisite for providing better and more efficient e-services to citizens and other end users. Government of India is now focusing on the national dimension of E-Governance and on the interoperability requirements to practice good E-Governance.

An agreed Interoperability framework is required to underpin the speedy and proper development, and delivery of e-services. This framework will address technology, procedures and information content.

1.2 Purpose and scope of this document

E-Governance is built on interoperable information and communication systems, which interact seamlessly. Well-defined formats, standards and specifications help to achieve interoperability of information and communication systems. This document identifies and describes a framework containing the necessary specifications and standards, founded on firm technical policies.

These sets of standards consider only those areas, which have a major influence on the declared objectives of IFEG.

1.3 Structure of this document

[Section 2](#) narrates some global trends on E-Governance. In this section, e-readiness specific to India is also described briefly.

[Section 3](#) gives the National Initiative on E-Governance and the role of NIC in promoting E-Governance across the country.

[Section 4](#) gives an overview of Interoperability framework, including its objectives, benefits, scope, need, data interoperability problems and impact.

[Section 5](#) attempts to picture some of the Global initiatives in evolving E-Governance interoperability framework.

[Section 6](#) lists the goals, initiatives and guiding policies for IFEG (Interoperability framework for E-Governance).

[Section 7](#) describes the processes and steps for the Management and compliance of the Interoperability framework.

[Section 8](#) gives the guidelines and recommendations that are considered appropriate to use while selecting standards under the Interoperability Framework.

[Section 9](#) describes the IFEG (Interoperability Framework for E-Governance) layered Architecture model.

[Section 10](#) details the Software Architecture.

[Section 11](#) details the supporting Network Architecture.

[Section 12](#) describes the implementation plan for the framework.

[Section 13](#) gives the details of the Technical standards in each of the layers detailed in the architecture model.

[Section 14](#) gives the domain level standards for data and metadata.

[Section 15](#) lists the annexure to this document.

2. E-Governance - Global Trends and National Initiatives

2.1 E-Governance objectives and policy issues

The application of Information Communication Technology (ICT) enabled processes and systems for the Government is called E-Governance. E-Governance involves Information Technology enabled initiatives that are used for improving (a) the interaction between Government and citizens or Government and businesses, as well as (b) the internal Government operations. Governments have realized the importance of using ICT that can make the provision of the services to the citizen more efficient, transparent, can save costs and lead to a higher level of efficiency.

The major objectives of good E-Governance should focus on:

Effectiveness: e.g., E-Government will not be limited to the provision of standard administration services electronically; they will also promote delivery of entirely new services;

Efficiency: e.g., improved access to information and cost reduction by integrating Local, State and Central administrations;

Flexibility: e.g., multi-channel access to information and services for every citizen and enterprise, 24 hours a day, 7 days a week;

Transparency: e.g., ease of finding and consuming services, thus allowing citizens and enterprises better access to and participation in administrative matters and political issues.

The above objectives are conditioned by the existing national realities and it is important to identify obstacles, if any, and to overcome them. Some areas of concern are:

- The state of technology growth and absorption level in the country;
- The wide economic disparities existing between different States;
- Socio-economic disparities between groups of citizens;

- Cultural and language differences.

2.2 Qualities of E-Governance Services

If the citizen or other end user is to derive the maximum benefit from the provision of e-services through E-Governance, the e-service must possess the following quality attributes:

- The users must know the information about the available e-services and the users are aware of the benefits of these services;
- The user should be able to locate the e-services easily;
- The e-services must be accessible to all members of the intended target groups, including disabled and elderly persons;
- The information from the e-services should be comprehensive, correct, readily available, and easy to understand with respect to language and structure;
- The provision of e-services should be safe, confidential, and in no way violate the privacy of either party;
- The design of E-Government applications should comply with the existing legal data protection requirements.

2.3 E-Governance: Global trends

In the past decade, many Governments all over the world have embraced the digital revolution to improve intra-Government and inter-Government businesses and the services they provide to its citizen. The emergence and widespread use of Internet and Web-enabled services have accelerated these endeavors. However, most E-Governance programs and applications have not grown beyond the information provision stage. Only a few countries offer citizens, the opportunity to conduct on-line transaction, such as payment of taxes or receipt of pension.

The Division for Public Economics and Public Administration of the United Nations has brought out a report titled ' Benchmarking E-Government- a Global

Perspective'. This report presents a synthetic 'E-Government index' that reflects and incorporates the country's official on-line presence, evaluates their Information Communication infrastructure and assesses their human development capacity. In other words, the index reflects the requisite parameters that constitute an enabling environment for E-Government. On the basis of the level of this index, the report classifies the countries into four categories, as shown in Table.1. (**Table 1:** [The 2001 E-Government Index](#))

The index also reflects the country's general economic and social development levels; people in the developed countries enjoy the benefits of better access to information and a more interactive and participatory relationship with their Government.

India is placed in the third category of countries having a Global Index between 1.00 and 1.59, an index below the Global Index of 1.62. This category of countries is identified as countries having minimal E-Government capacity.

Table 1: 2001 E-Government Index

| High E-gov Capacity | | Medium E-gov Capacity | | Minimal E-gov Capacity | | Deficient E-gov Capacity | |
|----------------------------|----------|------------------------------|------|-------------------------------|------|---------------------------------|------|
| 2.00 - 3.25 | | 1.60 - 1.99 | | 1.00 - 1.59 | | Below 1.00 | |
| USA | 3.1 1 | Poland | 1.96 | Armenia | 1.59 | Cameroon | 0.99 |
| Australia | 2.6 0 | Venezuela | 1.92 | Brunei | 1.59 | Cent Africa Rep. | 0.98 |
| New Zealand | 2.5 9 | Russian Fed. | 1.89 | South Africa | 1.51 | Ghana | 0.98 |
| Singapore | 2.5 8 | Colombia | 1.88 | Paraguay | 1.50 | Nepal | 0.94 |
| Norway | 2.5 5 | Latvia | 1.88 | Cuba | 1.49 | Thailand | 0.94 |
| Canada | 2.5 2 | Saudi Arabia | 1.86 | Philippines | 1.44 | Congo | 0.94 |
| UK | 2.5 2 | Turkey | 1.83 | Costa Rica | 1.42 | Maldives | 0.93 |

| | | | | | | | |
|------------------|-----|-----------|------|----------------|------|--------------|------|
| | 2.5 | | | | | | |
| Netherlands | 1 | Qatar | 1.81 | Panama | 1.38 | Sri Lanka | 0.92 |
| | 2.4 | | | | | | |
| Denmark | 7 | Lithuania | 1.81 | Nicaragua | 1.35 | Mauritania | 0.91 |
| | 2.4 | | | | | | |
| Germany | 6 | Ukraine | 1.80 | Djibouti | 1.35 | Bangladesh | 0.90 |
| | 2.4 | | | | | | |
| Sweden | 5 | Bahamas | 1.79 | Dominican Rep. | 1.34 | Kenya | 0.90 |
| | 2.3 | | | | | | |
| Belgium | 9 | Hungary | 1.79 | Trin & Tobago | 1.34 | Laos | 0.88 |
| | 2.3 | | | | | | |
| Finland | 3 | Greece | 1.77 | Indonesia | 1.34 | Angola | 0.85 |
| | 2.3 | | | | | | |
| France | 3 | Jordan | 1.75 | Jamaica | 1.31 | Haiti | 0.84 |
| | 2.3 | | | | | | |
| Rep of Korea | 0 | Bolivia | 1.73 | Iran | 1.31 | Mauritius | 0.84 |
| | 2.3 | | | | | | |
| Spain | 0 | Egypt | 1.73 | Azerbaijan | 1.30 | Tanzania | 0.83 |
| | 2.2 | | | | | | |
| Israel | 6 | Slovakia | 1.71 | India | 1.29 | Senegal | 0.80 |
| | 2.2 | | | | | | |
| Brasil | 4 | Slovenia | 1.66 | Kazakhstan | 1.28 | Madagascar | 0.79 |
| | 2.2 | | | | | | |
| Italy | 1 | Mongolia | 1.64 | Belize | 1.26 | Zimbabwe | 0.76 |
| | 2.2 | | | | | | |
| Luxembourg | 0 | Oman | 1.64 | Barbados | 1.25 | Burkina Faso | 0.75 |
| | 2.1 | | | | | | |
| Unit. Arab Emir. | 7 | Ecuador | 1.63 | Guyana | 1.22 | Zambia | 0.75 |
| | 2.1 | | | | | | |
| Mexico | 6 | Suriname | 1.63 | Honduras | 1.20 | Mozambique | 0.71 |
| | 2.1 | | | | | | |
| Ireland | 6 | Malaysia | 1.63 | El Salvador | 1.19 | Sierra Leone | 0.68 |
| | 2.1 | | | | | | |
| Portugal | 5 | Romania | 1.63 | Guatemala | 1.17 | Cambodia | 0.67 |
| | 2.1 | | | | | | |
| Austria | 4 | Belarus | 1.62 | Gabon | 1.17 | Comoros | 0.65 |
| | 2.1 | | | | | | |
| Kuwait | 2 | Peru | 1.60 | Turkmenistan | 1.15 | Guinea | 0.65 |
| | 2.1 | | | | | | |
| Japan | 2 | | | Uzbekistan | 1.10 | Namibia | 0.65 |
| | 2.1 | | | | | | |
| Malta | 1 | | | Vietnam | 1.10 | Togo | 0.65 |
| | 2.1 | | | | | | |
| Iceland | 0 | | | Samoa (West) | 1.09 | Gambia | 0.64 |
| | 2.0 | | | | | | |
| Czech Republic | 9 | | | Cote d'Ivoire | 1.05 | Malawi | 0.64 |

| | | | | | |
|-----------|-----|-------------|------|----------|------|
| Argentina | 2.0 | China | 1.04 | Mali | 0.62 |
| | 9 | | | | |
| | 2.0 | | | | |
| Estonia | 5 | Pakistan | 1.04 | Ethiopia | 0.57 |
| | 2.0 | | | | |
| Bahrain | 4 | Nigeria | 1.02 | Chad | 0.55 |
| | 2.0 | | | | |
| Uruguay | 3 | Kyrgyzstan | 1.01 | Niger | 0.53 |
| | 2.0 | | | | |
| Chile | 3 | Botswana | 1.01 | Uganda | 0.46 |
| | 2.0 | | | | |
| Lebanon | 0 | Taijikistan | 1.00 | | |

Source: United Nations Division for Public Economics and Public Administration: 'Benchmarking E-Government: a Global Perspective', May 2002.

2.4 E-readiness of India

Sources: *E-readiness Assessment (India)*-, DIT; *Readiness for Networked World-Center for International Development*; -NCAER Report.

E-readiness: of a country is central to implementing E-Governance in a cost-effective and efficient manner. Among the many definitions of e-readiness, the most appropriate in the Indian context seems to be the one given by the Center for International Development at Harvard University. They have defined an E-Ready society as one that has necessary physical ICT infrastructure; has integrated ICTs throughout businesses; and has used ICTs in everyday life and the Government. E-readiness assessment of a country can guide development efforts by providing benchmarks for comparison and monitoring progress.

Global Ranking: The Global Information Technology Report brought out by the World Economic Forum in 2001-02 ranks India 54th amongst 75 countries in terms of E-Readiness and 37th amongst 85 countries in 2002-03. Many other agencies have also made e-readiness assessment of countries, each doing within their own perspective. For example, the 2002 Global Technology Index ranks India at 34th, just above Russia. These rankings indicate that India is rapidly emerging as one of the leading nations in terms of ICT development.

E-Readiness Assessment: The NCAER, in their report on e-readiness assessment of various Indian States, view e-readiness as the ability of the states to provide and use governance equitably and cost effectively through network development and the capacity to participate in the provincial level digital economy and further networking with the national level digital economy. To develop an overall e-readiness index, NCAER used six broad parameters- Network Access; Network Learning; Network Society; Network Economy; Network Policy; and E-Governance. On the basis of the e-readiness index, the States were classified in to six categories: leaders; aspiring leaders; average achievers; below average achievers; and least achievers. While Karnataka, Maharashtra, Tamil Nadu, and Andhra Pradesh are the leaders in respect of their e-readiness, Goa, Gujarat and Chandigarh occupy the second rung as aspiring leaders.

Network Access: According to the Center for International Development, India's 39 million –line telephone network is one of the largest in the world and second largest among developing economies (after China). The current telephone penetration rate is only 4 per 100 people of population, far below the global average. However, this scenario offers vast scope for growth, and India has one of the fastest growing telecommunication systems in the world with an annual growth of about 22% for basic telephone services and over 100% for cellular and Internet services over the last five years. The tele-density in India expected to reach the figure of 15 per 100 people of population by 2010.

The bandwidth availability in India is set to get a boost with the commissioning of the National Internet Backbone (NIB) project. This project will connect 183 cities in a fiber ring and take Indian telecom infrastructure to world-class levels.

Network Infrastructure and Quality: Till recently, Videsh Sanchar Nigam Limited (VSNL) was India's only Telecom gateway to the world. VSNL operates a network of earth stations, switches, submarine cable systems, and value added service nodes. Its main gateway centers are located at Mumbai, New Delhi, Calcutta and Chennai. The international telecommunication circuits are derived via *Intelsat* and *Inmarsat* satellites and wide band submarine cable systems. The

international connectivity, which totals over 80 Mbps, is considered adequate for meeting India's requirements with current level of subscribers.

VSNL offers high-speed Internet services to its ISDN subscribers. ISDN users can now download information @ 64 Kbps or 128 Kbps which is much faster than the dial up system (5-10 times). Recent developments in high-speed data communications include Digital Internet Access System (DIAS) to provide 128Kbps connectivity for voice and data on the existing local loop. DIAS uses a Digital Subscriber Line (DSL) and promises affordable access to Internet.

In April 2002, the Government of India has allowed private Internet Service Providers for setting up international gateway via satellites and submarine optical fiber cables.

Internet Availability and Affordability: VSNL was the major provider of Internet services in India till the federal Government of India ended its monopoly in 1998. Currently there are more than 200 private sector Internet Service Providers catering to the ever increasing public demand for Internet connectivity.

Internet penetration into India's large rural population is still low. This is mainly on account of affordability as the costly dial up access remains as the primary means available to Indian citizen to establish connectivity to Internet.

Network Society:

Domestic Internet usage and ICT penetration into public domain are crucial indicators of e-readiness of any country. In order for the public to derive maximum benefit from the applications of ICT, people should be able to use it and appreciate its huge potential. In order to prompt the Government to deliver quality e-services and make the benefits of ICT enabled products available to the masses, the society itself must come forward to demand the same.

It is heartening to note that there has been significant increase in the usage of Internet across the country. NASSCOM has estimated that in 2002, there are 486 ISP license holders catering to approximately 15 million Internet users in

India. The Internet culture has percolated into the society and significant changes can be seen in various sectors such as health; education; agriculture etc.

Language is no longer a barrier to the usage of Internet. The Net is fast transforming with the adoption of regional languages for information processing. However, the use of languages other than English is inhibited by the quality of web content, and the natural tendency to visit English language sites.

To sum up, a networked society is slowly emerging in India with the increased use of computers for personal purposes and in the workplaces.

3. National Initiatives on E-Governance

Having recognized the importance of E-Governance in the matter of providing better state-related services to its citizens, the Government of India announced a number of new initiatives on its 55th Independence Day in the year 2002. The intention to accelerate E-Governance at all levels of the Government to improve efficiency, transparency and accountability at the Government-citizen interface was declared by the Government. At the meeting of the National Development Council held in December 2002 it was declared thus: “E-Governance, which can contribute significantly to better Governance, is a major thrust of the 10th Plan and urged all concerned to implement this strategy.

In tune with the above strategy of the Government of India, the Department of Information Technology prepared a National E-Governance Action Plan .The Action Plan seeks to create the right governance and institutional mechanisms, set up the core infrastructure and policies, and implements a number of Mission Mode Projects at the Center, State and integrated services level to create a citizen-centric and business-centric ambience for E-Governance.

3.1 Role of National Informatics Centre (NIC)

[National Informatics Centre \(NIC\)](#) was created as part of a high priority plan project nucleated by the Central Government in 1975-76 with assistance from UNDP. With the primary aim of promoting informatics in the government, NIC was entrusted with responsibilities to:

- Provide this informatics service to various user agencies in Government
- Play a promotional role in creating appropriate information systems in Government
- Act as a focal point for developing, managing and operating information system in Government
- Act as a focal point for development of methodologies for designing and implementing national information systems and data management techniques

- Train users in information technology, data management and computing techniques

Ever since its inception, NIC has been promoting ICT led development in the country and in the process it has amassed state-of-the-art ICT infrastructure and valuable experience in the field of E-Governance. The core E-Governance infrastructure and assets of NIC include:

Data Centre – Equipped with 10 Terabytes of storage capacity, upgradeable to 90 Terabytes, the Storage Area Network (SAN) at NIC supports a number of e-services that include citizen services, portals, databases, e-mail and other Internet services. The strategic SAN, which is established in Delhi is backed up by a Disaster Recovery Centre at Hyderabad.

Integrated Network Operation Centre (iNOC) – The state-of-the-art Integrated Network Operation Centre (iNOC) at NIC Delhi monitors all NICNET nodes located across the country. It acts as a single point access, control, analysis and management tool that coordinates distributed bandwidth, maintains security and performs constant auditing of NICNET.

Communication Infrastructure - The communication infrastructure established by NIC includes a satellite based Wide Area Network that comprises SCPC/DAMA, FTDMA and DVB – a total of around 1600 VSATs up to Block level in the country. NIC is providing Video-conferencing facilities at 167 locations in the country. A high-speed terrestrial leased line backbone connects all the State capitals and Delhi. Coupled with this infrastructure, the Metropolitan Area Networks and Local Area Networks within Central Government Bhawans & State Secretariats have helped creating a Government wide Intranet across the country. Besides, NIC is also providing hub based wireless network facilities and terrestrial connectivity to solve last mile problem.

Certification Services – NIC is an approved certification authority responsible for the issuance and maintenance of digital certificates for usage within the government sector. NIC-CA provides services related to certificate enrolment, renewal, suspension and status information request.

Software Management Skills – NIC has more than 3000 ICT professionals with diverse skill set that includes knowledge of all popular operating systems (Linux, Windows, Solaris, Unix etc.), host of software development environments (JAVA/ASP/Visual Basic etc.) and interoperation enabling technologies like XML. NIC has in-house skills to host time critical web applications in a clustered environment such as examination results etc.

Capacity Building Expertise – The availability of NIC resources up to the district level has helped building the human capacities within the government to a considerable extent. Since inception, NIC has been conducting training programs for government officials facilitating better usage of E-Governance solutions.

Domain Knowledge – NIC has been working hand-in-hand with the Central and State government and in the process it has acquired considerable domain knowledge in various sectors of government including Health, Finance, Rural development, Education, Agriculture, Commerce, External Affairs, Civil Aviation etc aggregating to a total experience of 60,000 man years. The domain knowledge thus gained places NIC in a better position in developing and implementing E-Governance strategies and solutions while, at the same time, effectively addressing the ground realities.

NIC's close relationship with Central and State Government coupled with its ICT capacities and skilled resources has resulted in a number of E-Governance solutions for Central Ministries, State and District Governments. NIC is also instrumental in extending the reach of E-Governance solutions up to Block and Village level. Notable areas of E-Governance implementations at Central level include Passport, Customs, ROC, DGFT, Employment Exchange, Transport, Courts, Immigration and Central Excise etc. Major E-Governance solutions provided at State and District level include Land Records, Treasuries, Taxes, Registration, Certificates, Licenses, rural informatics solutions, citizen services through a single-window etc. NIC has also been instrumental in Block level ICT initiatives such as Community Information Centers in the North East Region and village level efforts like Wired Warana.

The next logical step on the evolutionary path toward E-Governance involves integration of E-Governance solutions developed so far, so that the citizens, businesses, NGOs and other agencies are able to interact with the government as a single entity through a single window. The current applications work in isolation from other applications, as they were developed to meet the department specific needs using the technologies available and preferred by the user department at the time of development. The joined-up service delivery entails integration of the heterogeneity that exists in the E-Governance solutions in the form of data formats, software platforms, software languages, hardware and networking platforms. With the current technological advancements, it is now possible for applications to interoperate irrespective of the underlying technologies.

To carry forward its efforts to the next logical stage, NIC undertakes to standardize the E-Governance solutions to allow for seamless exchange of information across the government departments through its proposed Interoperability Framework for E-Governance (IFEG), which is discussed later in the document.

To gain an understanding of issues related to interoperability and to learn from similar experiences in other parts of the globe, the subsequent two chapters provide an overview of the general issues related to Interoperability, the key elements of an Interoperability Framework and a window view of some of the Global Initiatives undertaken by various countries in the area of E-Governance Interoperability Framework.

Feedback may be sent to:
The Interoperability Framework Advisory Group
ifeg@nic.in

4 Overview of IFEG (Interoperability Framework for E-Governance)

4.1 Interoperability

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.

Definition of Interoperability as per IEEE is “The ability of two or more systems or components to exchange information and to use the information that has been exchanged”.

Interoperable systems working in a seamless and logical manner across the Government sector are crucial to providing better services, satisfying the needs of the citizen and other users at a lower cost.

4.2 Benefits of Interoperability

Connectivity and interoperation among computers, among different entities (Governments, businesses, citizens, and individuals), and among software components can increase the flexibility and agility of ICT systems, thus reducing administrative and software costs for Government. They will also reduce the time needed to implement software and E-Government services.

At the national level, E-Government flexibility and agility will increase as interoperability increases. Interoperability can, for instance, assist in the delivery of E-Government services based on life events, and help the business sector interact electronically with administrations, reducing administrative costs.

4.3 Scope of Interoperability

Interoperability, as an issue, is not restricted to a framework for E-Governance sector. It extends through the wide use of ICT technology and embraces the whole gamut of ICT-embedded industry and services, from the smallest to the largest entities. Hence, *interoperability* is not just a country-specific issue, but is **global in scope**. This international perspective has led key policy and decision makers to realize that there is a need for interoperability both within and between Government agencies and other end user entities.

There are various components of an inter-operable E-Government system: citizen and business (end users); the multiple access channels; the portals (local authorities, Governments and private sector); and the Gateway infrastructure. All this requires different kinds of interoperability for different groups.

Interoperability with individuals/citizens: This is accomplished primarily through Internet/Web browser interfaces. It also includes direct data exchanges, mobile communications etc., which are likely to grow in importance in the coming years.

Interoperability with private enterprises must take into account the wide range of systems they have. This may involve more sophisticated business-to-Government data exchanges.

Interoperability sought by Government and Public Authorities both within their own administration and with others will face the same interoperability challenges that private enterprises face in accomplishing enterprise application integration and B2B integration. Interoperability with other Government entities must take into account, the diverse application software systems and ICT hardware that they already have in place.

4.4 Data Interoperability Problems and Strategies

Software development project teams sometimes experience problems on account of incompatibility of *data definition and data representation*. The parties planning to exchange information accurately must agree on the definition and

implementation (i.e. structure, permissible values, etc.) of each data element to be exchanged and conduct a data alignment exercise. Whenever a new party needs to be involved in a joint-up service, the data alignment exercise may need to be repeated and the data conversion software rewritten to satisfy possible new requirements from the new party.

The problems mentioned above, namely repetitive data alignments and observing the following data interoperability measures can alleviate data conversion.

- Adopt industry standards where appropriate
- Design quality and reusable Project Schemas – a project schema is the collection of information models and XML Schema developed by the project team
- Share project schemas with other teams

4.5 Open Standards and Open Source

Adoption of open standards cannot only significantly contribute in achieving interoperability but can allow flexibility in the selection of technology and solutions. It does not bind the user to a particular vendor or technology. Compatibility with open standards should be one of the major criteria for selection of software. Open Source is software whose code is publicly available. Most of the Open Source solutions are based on Open Standards / public specifications; the availability of open source code in general promotes open, free discussions on specifications; thus their open specifications are in general robust and interoperable.

4.6 The Interoperability Framework (IF)

An Interoperability Framework (IF) is defined as a set of standards and policies, which describe the way in which different organizations have agreed to interact

with each other. The purpose of Interoperability Framework is to facilitate interoperability with other systems as necessary, while at the same time providing flexibility in the choice of hardware and systems, and application software used to implement solutions.

The Interoperability Framework for E-Governance (IFEG) creates a common basis across the Government and public sector for the cost-effective delivery of E-Governance to the public and other end users. It defines an appropriate set of policies and specifications and guidelines governing the information flow across various Government sector agencies. Included in this domain are interconnectivity, data integration and management, data access and content management.

- Interconnection
- Data Integration
- Information Access
- Security, and
- Metadata

4.7 Need for an Interoperability Framework

The E-Governance initiatives seen in many countries are an evolving process underpinned by emerging ICT technologies. The primary need of this endeavor is to improve Government productivity as well as the quality of provision of its services.

A key business objective of most E-Governance initiative is to provide client-centric joined-up Government services to the public. In order to attain this objective, the Government needs to be perceived as a single entity, with seamless flow of information across individual ministries and departments as necessary. An Interoperability Framework is essential to support the flow of information and to improve the coherence of information systems maintained by individual ministries and departments.

The Interoperability Framework aims to define the set of specifications to facilitate Government systems to communicate and interoperate with other systems, both within Government and external to it, efficiently and effectively. In addition, the framework promotes and fosters the adoption of eXtensible Markup Language (XML) as the primary standard for exchange of data between applications.

By bringing together the relevant specifications under an overall framework, IT management and software developers have a single point of reference when ever a need arises to locate the required interoperability specifications that should be followed for a specific project. By adopting these interoperability specifications, system designers can ensure interoperability between systems while at the same time have the flexibility to select different hardware, and systems and application software to implement solutions.

4.8 Impact of the Interoperable Framework

Generally, the Interoperable Framework applies to Government to Government and Government to public interactions. It has no binding on interaction of public themselves. Nevertheless, when members of the public build systems to interact or communicate with the Government electronically, now or in the future, the framework can provide necessary specifications to enable effective communications and interactions between the private sector and the Government.

Government departments will feel the greatest impact of Interoperable Framework. In the short to medium term, the impact of change resulting from compliance with the Interoperable Framework specifications might mean extra effort and cost. Care need to taken in the selection of specification to technology in use, emerging industry trends and industry standards in order to minimize the impact on Government departments. The impact of the framework on citizens and other private sectors will be far less than that on Government sector.

4.9 Legal Issues

While framing the standards, the IT Act 2000 and relevant cyber laws should be factored into.

4.10 Partnerships with ICT Industry

One of the major steps in the approach towards ensuring interoperability is to have partnership with the ICT industry. This will help to quickly adopt interoperable standards, take advantage of emerging technologies and continued support.

5. Global Interoperability Framework Initiatives

Having recognized the importance of Interoperability Framework and its relevance and impact on E-Governance, many countries have evolved or in the process of evolving their national Interoperability Framework for Government business as well as for other sectors. These national E-Governance frameworks address the use of various technologies and protocols. Each national framework addresses some combination of the following technologies/frameworks, as well as others:

- Networking LAN/WAN protocols
- Directory Services
- Domain naming
- File, Hypertext and Message transfer protocols
- Messaging/Data Integration
- Schema/Metadata Registries
- Web-based Services and Middleware
- Security
- Authentication
- Character sets
- Newsgroup services
- Browsers and Viewers
- SMS/WAP/iMode
- Reusability

Notable Interoperability Framework initiatives by some of these countries include:

5.1 United Kingdom:

The UK online strategy envisages better public services tailored to the needs of the citizen and business, founded on seamless flow of information across Government. The E-Government Interoperability Framework for UK sets out the

Government's technical policies and specifications for achieving interoperability and ICT coherence across the public sector. The e-GIF defines the essential pre-requisites for joined-up and web-enabled Government.

The UK E-Government Interoperability Framework model focuses on 4 aspects- interconnectivity, data integration, access and content management. The main thrust of the framework is to adopt the Internet and World Wide Web specifications for all Government systems. The framework also sets out policies for establishing and implementing metadata across the public sector.

The UK Government has launched a website known as 'GovTalk' to provide technical support, best practice guidelines, toolkits and centrally agreed schemas. This is a joint Government and industry facility for generating and agreeing XML schemas for use throughout the public sector.

5.2 The New Zealand Government

The New Zealand e-GIF is built on five elements. They are:

Business Process Interface: Takes care of matters needed to enable managers to map processes to support inter-agency business solutions; and define the services to be presented based on business solutions.

Service Delivery: This element covers matters needed to provide answers to queries from clients.

Access: Matters needed for obtaining access to information are covered in this element. Included are security; features of access methods; and types of expected transactions.

Information Sharing & Exchange (Data Integration):

Matters needed to allow for the recognition of data- codes, recognition methods, interpretation and formats used.

Interconnection: Matters needed for the exchange of information between a user and an entity of E-Government- transmission mechanisms; transfer mechanisms (interfaces) that link the transfer medium (internet) and an end user, security and protocols for managing the connection.

5.3 [Pan European Countries](#)

The European Interoperability Framework identifies three aspects, namely,

Technical- Linking up computer systems in agreement on standards for presenting, collecting, exchanging, processing, and transporting data.

Semantic- ensuring that transported data shares the same meaning for link up systems.

Organizational- organizing business processes and internal organization structure for better exchange of data.

5.4 [Malaysian Government](#)

The Malaysian Government Interoperability Framework (MyGIF) defines a set of collection of ICT standards and related technical specifications governing the communication of systems, flow of information, as well as the exchange of data and business processes that relates to Government Ministries, agencies and departments. MyGIF basically covers the following five (5) interoperability areas:

- Interconnection
- Data Integration
- Information Access
- Security
- Metadata.

Instead of creating new standards or specifications, MyGIF adopts internationally recognized open and *de facto* ICT standards as well as technical specifications for all interoperability areas mentioned above.

MyGIF's objectives are:

- To enable different Government systems and applications , both within and external to Government, communicate and interoperate efficiently and effectively
- To promote and foster the adoption of eXtensible Markup Language (XML) that enables the exchange of data between applications.
- To promote the addition and use of Metadata
- To align with Internet by adoption of common specifications used in Internet and WWW for all Government information systems and
- To adopt open standards and specifications that is widely supported by the market in order to reduce the total cost of ownership of Government information systems.

The key drivers guiding the recommendations of ICT standards and technical specifications for MyGIF are: Interoperability; Maturity and Popularity of Standards; Market Support; Open Standard; Internet Alignment; and Compliance with existing Standards.

5.5 [Government of the Hong Kong](#)

A key strategy of the E-Government initiative by the Hong Kong Government is to develop joined-up E-Government services. The necessary conditions for implementing joined-up services are:

- **Process Interoperability:** agreement on how the business activities of the concerned parties affect each other, i.e. the business rules.

- **Data Interoperability:** agreement on what information has to be transmitted from one party to another and the definition and representation of such information.
- **Technical Interoperability:** agreement on what communication protocol and message format to be used when one party sends information to another.

The Interoperability Framework of the Government of Hong Kong is an enabler for the implementation of joined-up E-Government services. The framework facilitates technical interoperability and data interoperability among departments and their clients or business partners. This is achieved by promulgating technical standards, and by putting in place a mechanism for the concerted alignment and specification of the **data elements** that have potential for reuse in multiple joined-up projects.

5.6 Germany

The Standards and Architectures for E-Government applications (SAGA) are based on the following principles:

- E-Government applications primarily use the browser as front-end, unless the services to be implemented cannot be reasonably handled via a browser.
- They do without active contents in order to avoid forcing users to reduce the browser's security settings and thus making damage by unsafe websites possible.
- E-Government applications do not store any program parts or data on the users' computers beyond the users' control.

In addition, a complete standardization approach on four development directions is underlined. They include

- Definition of Technical normative references, standards and architectures
- Process modeling

- Data modeling
- Development of basic components.

The four-tier architecture model followed adopts and makes the use of object-oriented software development and a component-based software development approach.

A public agency is made responsible for an E-Government application to be responsible for conformity with SAGA. This agency will also be responsible for examining ways to migrate special applications to conform to SAGA standards.

5.7 Italy

The Italian Initiative on E-Government for Development, the **E-Model** provides value in following ways:

1. by providing interested countries with a set of guidelines to evaluate the opportunities opened up by E-Government;
2. by offering interested countries some concrete guidelines to design “good practice in Government administration” in terms of:
 - legal framework: enabling laws, simplification/rationalization.
 - organization and human resources: skills, mobility
 - technologies: ICT applications, infrastructures, channels
 - functionality of applications;
3. by identifying the best existing E-Government solutions, thus allowing interested countries to avoid the process of trial-and-error experienced by other countries;
4. by providing a modular framework for E-Government applications, allowing the re-use of common architecture components and preventing duplication;
5. by conforming to current best practice in terms of up-to-date technical infrastructure and info-structure, open technical architecture standards, and multi-channel strategy;
6. by highlighting the major legal and regulatory prerequisites that enable the digitalization of services and underpin the process of meaningful integration, especially over virtual channels (e.g. Internet, call centers).

The basic principles envisaged in the document include:

- It focuses on the end-to-end integration of administrative processes
- It supports front office activity vis-à-vis citizens and enterprises (G2C and G2B);
- It also supports the efficiency and effectiveness of government back office activities, which are usually not as efficient and effective as they might be.

5.8 [Australia](#)

The E-Governance Framework is designed with the following objectives for better Governance.

- Endeavors to achieve whole-of-Government solutions.
- Integration of Government information and services.
- Openness and transparency across Government.
- A strategic focus on business outcomes.
- Efficiency gains through reduced duplication of effort.
- Improvements in providing information and services to citizens.
- Economic growth through optimum use and reuse of information and resources.

It has been decided by the Government of Australia to :

- Use internationally accepted standards wherever available and appropriate.
- To use standards that are scalable.
- To use open standards wherever possible.
- The premise that information may, at some time, be transferred across agency boundaries should underpin decisions when agencies are designing and investing in new information and communication technology (ICT) systems;
- Maintaining the trust of citizens in the business of Government must be a fundamental principle that underpins integrated service delivery initiatives. The privacy of personal information and of commercial-in-

confidence information must be an essential consideration of all E-Government projects.

A need is felt for creating an Interoperable working environment to exchange information across various applications. The following sections elaborate the standards required for Interoperability.

6 Interoperability Framework for E-Governance (IFEG)

NIC has initiated the development of an **Interoperability Framework for E-Governance** (IFEG) that comprises a set of policies and technical standards to facilitate interaction between isolated E-Governance applications. Once IFEG is followed, it will result in better interaction among Government, business and citizen. Leveraging the recent technical advancements that allow applications to interoperate, regardless of the underlying technologies, IFEG envisages facilitating joined-up service delivery through a single window.

Keeping in line with the International Standards being adopted in many parts of the globe in the area of Interoperability, as discussed in the previous chapter and also taking into account the Indian context, IFEG identifies key areas for defining interoperability standards and recommends Standards for each one of them, which are discussed later in this chapter. As a Proof of Concept, NIC has also initiated the implementation of IFEG standards in six National Level Projects, which include Employment Exchange, Land Records, Hospital Services, Property Registration, Treasury and Courts.

6.1 Goals and Objectives

Major objectives of IFEG are:

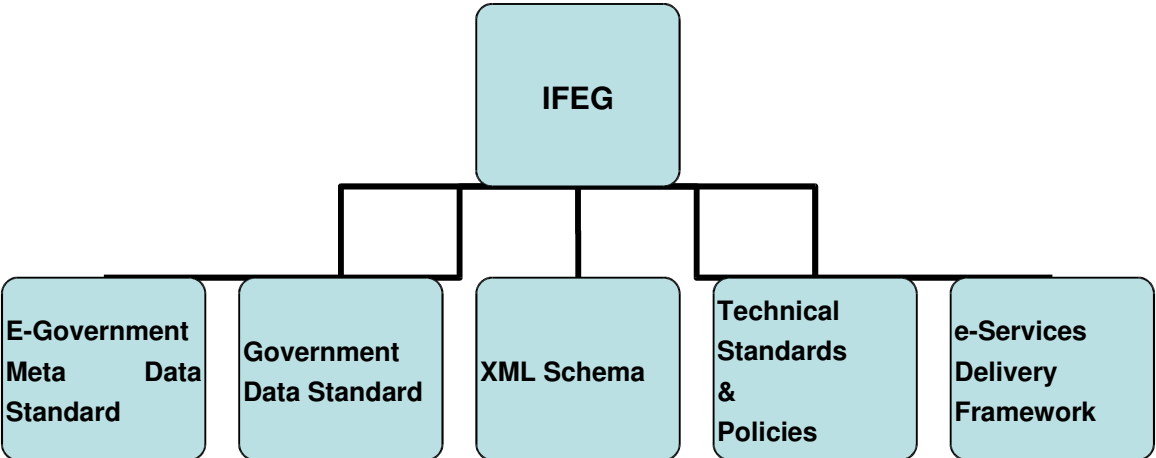
- To provide user-centered e-services by facilitating the interoperability of services and systems between public administration agencies, as well as between the administrations and the public (citizens and business enterprises) at national level.
- To help achieve interoperability, both within and across different policy area, and where appropriate, with business and citizens
- To facilitate E-Governance applications development by Central and various State Governments around a common framework so that these applications are interoperable across the country. This will enable the developers to focus

on the integration of services to the citizens without regard to various competing technology standards.

- To provide detailed descriptions of the elements, which are, considered important for E-Governance services by the Central and State Governments, and public sector undertakings.
- To support E-Governance activities and projects to be launched by the state Governments.
- To stay tuned with global standards and protocols.

6.2 IFEG Architecture

The IFEG architecture covers high level policy statements, technical policies and management, implementations and compliances etc.



6.3 IFEG Guiding Policies

The development of IFEG should be governed by a set of underpinning policies and guidelines. The following policy issues are considered important while developing the E-Governance Interoperability Framework.

Dynamic Environment: Technologies, standards and the end user requirements are continually changing with time. The framework should be able to respond to these changes and should be able to function in a dynamic environment.

Easy Access to Information: Central to the effectiveness and utility of E-Governance is the ability of end users to gain easy access to Government and public sector information. Option to an end user to complete all transactions at a single point; provision of integrated services; availability of services in different languages; multi-channel and multimedia communication means; are all crucial to the success of E-Governance and hence to the design and development of the framework.

Adoption of Web-based Standards: It is essential that the framework is aligned with the specifications and standards adopted by the Internet and World Wide Web in respect of all public domain information systems.

Browser-based Technology: Primary means of access to all public domain information systems must be through browser-based technology.

Use of Primary Standards: XML (eXtensible Markup Language) may be adopted as the primary standard for data integration and presentation tools for all public domain information systems.

Use of Open Standards: To the extent possible, focus should be on open standards and open source software. Open standards allow exchange of information between dissimilar hardware, operating systems and application software. For example, XML allows creation of common information formats. It permits sharing of both the format and the data over the Internet and intranet and the transformation of data from one format to another.

Use of Open Source Software: Open Source Software has publicly available specifications. The open availability of their source code encourages further development in the public domain, making them robust and interoperable. The objectives of this framework are in tune with those of open source software (OSS) and therefore, they should be assessed and considered favorably alongside proprietary products.

Use of Reusable Software Components: It is important to speed up the life cycle of large software project mainly to avoid time overrun and to keep the cost of development under control. This requirement can be partially met by employing reusable software components and processes. Efforts should be made to identify and create components which can be used within the application as well as across various applications in different ministries and departments. The use of tried and tested components enhances the quality of the entire system.

Scalability: There could always be changing demands made on the information system, such as changes in data volumes, number of transactions or number of users. It is essential that the specifications chosen have the capability to be **scaled** to satisfy these changing demands.

Metadata Standards: Standardisation of metadata is essential if the data is to be truly interoperable. It also ensures that information access and services rendering to the citizens is achieved without the knowledge of the structure of the Government.

Compliance with IFEG: Compliance with the Interoperable Framework must be made mandatory for any system in the Government. Suitable mechanisms must be adopted by existing and legacy systems to conform to the framework.

Information Security & Reliability: Information security is fundamental and central to provision of services to and interaction with the public. The E-Government application architecture recognizes data security as an all-pervasive component which can be supported by suitable processes, methods, data

formats in every element. The aims of data security are to ensure Confidentiality, Integrity, Authenticity and Availability.

6.4 Scope of IFEG

Interoperability Framework for E-Governance (IFEG) covers the exchange of information and interaction between:

- Government and citizens (G2C)
- Government ministries and departments (G2G)
- Government and Businesses (G2B)

All E-Governance applications designed & developed by NIC shall adhere to the approved specifications laid down in the IFEG document. IFEG standards shall also set a preferred mode of information exchange between NIC developed E-Governance applications and any third-party application. IFEG defines standards for the following key areas:

- Access
- Presentation
- Data Integration
- Processes
- Network
- Security
- IFEG Management

7. Management and Compliance of the Interoperability Framework (IF)

Management of the Interoperability Framework implies continuous monitoring of the development and maintenance of the framework so that the framework tracks and responds to the change in technology or other environment. The management process or mechanism involves:

- Periodical review and update of the set of specifications that constitute the Interoperability Framework.
- Tracking technology changes and makes appropriate changes in the specifications.
- Obtain feedback from the Government agencies and the end users in respect of changing requirements and co-ordinate with the technology teams working on the revision of specifications.
- Advising on the development of policies, guidelines and procedures to support the development and management of XML schemas for E-Government.

Adherences to Interoperability standards are central to the success of implementation and adaptation of the framework and good E-Governance practices. Where appropriate, adherence should be made mandatory for all Government businesses and infrastructure development.

8. Interoperability Technical Standards

While implementing the Interoperability Framework, the emphasis should obviously be on ‘interoperability’. Standardization in technology and coordination with Government decisions/legislations can achieve this. In general, adherence to some prescribed guidelines and principles should result in a more efficient Interoperability Framework. The following guidelines and recommendations are considered appropriate to use while selecting Standards under the Interoperability Framework:

General Requirements:

- The cost should be low for usage.
- It should be adopted on the basis of open decision-making process
- No obstacle to use any version of the standard
- Use of extensions of any adopted standards should not be allowed

Industry Standards: The specifications adopted should be either globally recognized standards or existing de- facto industry-standards.

Open Standards: To the extent possible, select widely adopted open standards in place of their propriety alternatives.

Vendor Neutral Products: The specifications adopted should be vendor neutral as far as possible.

Limited Number of Specifications: For any Interoperability Domain, the number of allowable specifications should be limited, as far as practicable and without compromising the overall objective of interoperability, in order to minimize the cost and complexity to support these specifications.

Alignment with Internet: The specifications should be aligned with Internet standards as the Internet is a primary channel for delivering E-Government services.

Global Initiatives: The specifications adopted should take due notice of similar global initiatives, demonstrating good practices.

New versions: Versions of standards may need to be revised as new functionality is introduced. Special attention should be paid to ensure backward compatibility to minimize the impact of transition to a new version of a specification, thereby facilitating continued interoperability.

Version Selection: The selected version by the user need not be the latest available version; this is because the selected version may meet the functional requirements.

9. IFEG Architecture

The IFEG architecture adopts a layered approach by way of classifying the system functions and mapping them into each layer.

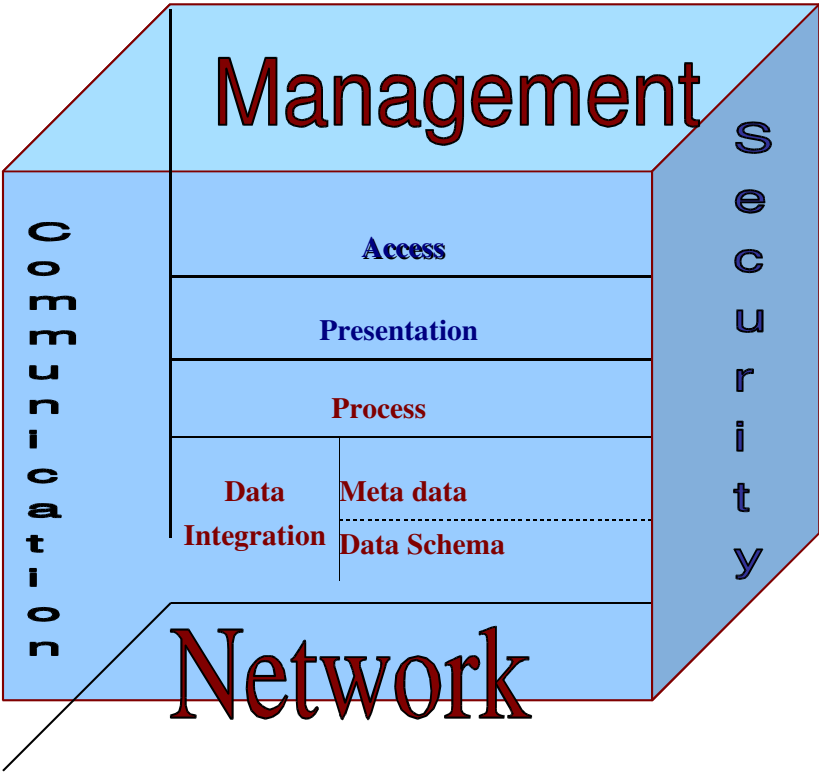


Fig 1: IFEG Layered Architecture Model

The components of the architecture model are as follows:

9.1 Access

9.1.1 Overview

The principal use of Government Information Systems is interactive or non-interactive access to the documents and applications, which can be typically through web browsers, audio players and other interactive front-end systems. Access layer covers the interoperability components and the technical specifications requiring the communication between different types of devices and thus help the devices talk to the applications for the exchange of information. The information can be sought via multiple channels to access the information systems.

The technology is moving at a fast pace and thus more and more communication devices are adding to the pool of already available devices for the smooth exchange of information whether it is wireless or through network. While a large group of people still depend on the network access, Internet browsing, email etc, what is becoming common is the wireless communication. Wherever full geographical mobility is not required an alternative to network is wireless networking, which requires access to LAN without physical wires. Standards in this layer are to provide essential information services to the user coming through any mode.

9.1.2 Channels for Access

There are various modes of access to information:

- Web/Internet
- Digital TV
- Computer workstation
- Mobile phones
- Touch Screen Kiosks
- PDA and other devices
- Telephone (Interactive Voice Response)
- Wireless LAN
- LAN/WAN Internetworking
- Smart Cards

As such the information systems should be capable of handling and delivering the information to these devices to suit the needs of the citizens. Browser based access to the applications render web pages, which require standard protocols like hypertext to render the information in the form of web pages. While Internet Protocol can handle the routing transmitting blocks of data from sources to destinations, TCP handles packet flow between systems. Standard on Mobile Device is required to support Internet-based access from mobile devices that enables mobile phone users to access the internet-based information. WAP is the standard for providing internet communications and advanced telephony services on digital mobile phones, pagers, PDAs and other wireless terminals.

Access to Disabled: This document will cover standards relating to access of information by physically disabled (visual) and insist on providing services in addition to the existing browser based services. Necessary standards related to the same will be discussed in the presentation layer also.

9.2 Presentation

9.2.1 Overview

The Presentation layer provides the interface to the user for accessing the information. Since the applications differ, standards are required to define the different format and file types.

9.2.2 Presentation Formats

As multiple access channels are used to access information presented in the presentation tier, open interchange formats available under different platforms is required. This offers a sufficient number of functions and is compatible with most of the available platforms. Style Sheets help to maintain a standard presentation format across various browsers. Hence, standards for style sheets are necessary. For varying requirements, data interchange must make use of Comma Separated value (CSV).

9.3 Process

The Process layer deals with standardization 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 of and interoperation among processes. This section will lay more emphasis on Software process and business process will be covered in detail under the Management layer as many of these processes are related to process management.

Software process standards relate to:

- Software process modeling – a common language for modeling the various components of a software
- Software architecture standards – Certain architectural standards and best practices, if adopted, promote re-usability, interoperability, scalability, resilience etc. of the service delivered. Such standards & best practices must be adopted as and when they emerge. For e.g., if a component-based architecture is adopted by applications delivering a joined-up service, any component that is failing to scale up to the requirements of the service may be pulled out and replaced with a more efficient one without affecting the availability of the service.

9.4 Data Integration

The Data Integration layer deals with standards that provide proper context to the information to allow a meaningful exchange. It entails agreement on ways to discover, represent and provide context to information to facilitate semantic interoperability between E-Governance data elements. The technical standards related to this layer include metadata standards, data standards and web-services standards.

(i) Forms : For forms based data **entry and exchange** an XML output based should be considered. An XML output based Electronic Forms (e-Forms) will be a mandatory requirement in IFEG. There should also be a e-Forms Working Group. The applicability of the **XFORMS** specifications, as defined by W3C to the IFEG, should be undertaken by the working group.

9.5 Data Schema

9.5.1 Overview

Information presentation on a higher plane, involves agreement on complex issues, which ensures that precise meaning of exchange of information is understood. It has to ensure the following:

- Proper exchange between computer systems
- Combine with other information sources for processing in a meaningful manner.

This calls for the use of general data definitions for major data identities and for the data to be exchanged between various processes and applications. Interoperability in applications requires common semantics for the data exchanged between systems.

Schemas provide shared vocabularies and allow machines to carry out rules made by people. The purpose of using such schemas is to minimise the divergence of descriptions between organisations across Government.

XML Schema defines the structure, content and semantics of XML documents and is primarily for data-oriented message exchanging and processing.

- *XML Schema Structures* specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The Schema Definition Language (XSD), which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs).

- *XML Schema Data types* define facilities for defining data types to be used in XML Schemas as well as other XML specifications. The data type language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 Document Type Definitions (DTDs) for specifying data types on elements and attributes. The W3C XML Schema Definition Language (XSD) is an XML language for describing and constraining the content of XML documents.

9.5.2 Technical Policies

The Working group for Schema will coordinate the creation of a central repository for XML schema. They will work towards a consistent XML schema to promote interoperability. Checking the availability of registered schemas in the repository and adopting it when initiating new projects must become mandatory.

9.6 Metadata

9.6.1 Overview

Metadata commonly defined as data about data, relates to a set of attributes that will capture the semantics of individual data items. Each element contains information related to a particular aspect of the information resource and metadata describes the technical aspects of information resources. A metadata record consists of a set of attributes, or elements, necessary to describe the information resources. Metadata captures information about information in the online context. It is descriptive and targeted, and is used by search engines to locate relevant resources with greater precision and ease. One of the main uses of metadata is to assist Internet users find resources based on its description. Descriptive elements will be used to improve the visibility and accessibility of their services and information over the Internet. Use of the IFEG metadata standards is essential if data is to be truly interoperable.

9.6.2 Need for Metadata Standards

A single reference framework is required for meeting the Government's information management and retrieval needs. IFEG Metadata Standard will encompass the set of elements that contain data needed for this. Metadata standards improve the granularity of a search, essential when navigating around large information resources.

As noted by Weibel and Lagoze, two leaders in the field of metadata development:

"The association of standardized descriptive metadata with networked objects has the potential for substantially improving resource discovery capabilities by enabling field-based (e.g., author, title) searches, permitting indexing of non-textual objects, and allowing access to the surrogate content that is distinct from access to the content of the resource itself." (*Weibel and Lagoze, 1997*)

Metadata is also a valuable tool for those managing records. Specialized local versions have been used for many years to identify, authenticate, describe and manage official records. The change to electronic record keeping provides an opportunity to streamline records management systems while making them more flexible, efficient and joined-up. Metadata is also invaluable when making non-text items, such as photo or music collections, forms and services, available electronically.

9.6.3 Underlying requirements

Standards for Data resource description Language

To avoid ambiguity in describing resources it is necessary to follow uniform or standard descriptions. For ensuring consistency for understanding and terminologies, Data Resource description Language will be used. Hence, standards on Data Resource Description although by itself do not define the metadata but instead defines the language for representing the metadata. Therefore, for applications of any type to exchange metadata, DRDL¹ will be referred to.

Resource Data Description data model

The Resource Description Framework (RDF) is an evolving metadata framework that provides a degree of semantic interoperability among applications that exchange machine-understandable metadata on the Web. RDF (Resource Description Framework) allows multiple metadata schemes to be read by humans as well as parsed by machines. It uses XML (EXtensible Markup Language) to express structure thereby allowing metadata communities to define the actual semantics. This decentralized approach recognizes that no one scheme is appropriate for all situations, and further that schemes need a linking mechanism independent of a central authority to aid description, identification, understanding, usability, and/or exchange.

RDF allows multiple objects to be described without specifying the detail required. The Resource Description Framework (RDF) is an infrastructure that enables the encoding, exchange and reuse of structured metadata. RDF is an application of XML that imposes needed structural constraints to provide unambiguous methods of expressing semantics. RDF additionally provides a means for publishing both human-readable and machine-processable vocabularies designed to encourage the reuse and extension of metadata semantics among disparate information communities. The structural constraints RDF imposes to support the consistent encoding and exchange of standardized

¹ Data Resource Description Language

metadata provides for the interchangeability of separate packages of metadata defined by different resource description communities.

RDF model is a descriptive data model that can be expressed in XML, as well as other syntaxes.

9.6.4 Standards for Central Component Repository:

One of the essential conditions for achieving Interoperability objective is to have a uniform software process, broadly encompassing design, development & deployment of sub-processes.

Control over the entire software process, helps in attaining a stable and easily re-deployable system environment. Extensive use of reusable components greatly helps in attaining this goal. A central repository of reusable components provides foundation to this concept.

The following basic four properties of Object Oriented Technology, may form part of the components. They are:

1. Abstraction
2. Encapsulation
3. Polymorphism
4. Inheritance

First Generation Class/Component libraries may look simple and single layered, but subsequent generations may encompass properties of previous layers, there by inducting inheritance characteristics.

The components will have well defined access mechanism, incoming and out going parameters. The complexities of the process will be hidden from the user.

Access to Central Repository:

Access to components can be made either through a physical medium or can be accessed on the fly from the centralised server. The access restrictions should be taken care of.

9.7 Network

9.7.1 Overview

The Network layer constitutes an important layer as it provides the integration platform for all the remaining layers. It encompasses the interoperability components that facilitate the communication and exchange of information within the distributed information-processing environment. The Network layer specifies how information-processing resources are interconnected, and documents the standards for protocols (for network access and communication), topology (design of how devices are connected together), and wiring (physical medium or wireless assignments).

9.7.2 Networks

Local Area and Wide Area Internetworking networking protocol is required to enable transmission of data between computers on LAN/WAN based on the unique address on the network. Since open standards does not yet exist for all components of Local Area Networks (LANS), a combination of industry standards, de facto industry standards, mutually agreed upon product standards, and open standards are currently required to support the nation wide heterogeneous operating environment.

Wireless LAN specification will be required for mobile users connecting to a LAN via a wireless connection. The features offered in a wired environment are extended to a wireless one.

9.8 Security

9.8.1 Overview

Ensuring data security is a major aspect for the successful implementation of services under IFEG. Data security represents and supports the trusted and

secure interaction between citizens, public authorities and business. IT Act 2000 stresses the importance of proper data security mechanisms and appropriate security controls incorporated in the E-Governance system, in order to prove in a court of law that the data has not been tampered with by any means.

Data security is mandatory among citizens, authorities and business. The complexity of security may grow exponentially with the number of services offered. Security is required at each layer of E-Government Architecture model and wherever the components communicate with each other, they should follow the defined security services.

9.8.2 Objectives of Data Security

- **Authenticity:** It is the process of uniquely identifying the clients of your applications and services. These might be end users, other services, processes, or computers.
 - **Confidentiality:** It is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users.
 - **Integrity:** Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks.
 - **Availability:** From a security perspective, availability means that systems remain available for legitimate users.

9.8.3 Security Levels

For an application to be reliable and trusted, security should cover the following levels:

- Security at the Network level
- Security at the Host level
- Security at the Application level

9.8.4 Security services

- Authentication & Identification: Process used to confirm the identity of the individual or to prove the integrity of specific information.
- Authorization: The granting of rights, including the ability to access specific information or resources.
- Audit Controls: Procedure used to validate that controls are in place and adequate for the purposes defined.
- Encryption: Process of transferring plain text data into an unintelligible form (cipher text).
- Data Privacy: Protection of sensitive and private data confidentially.
- Digital Signature: Authentication of electronic record by a subscriber by means of electronic method.
- Data Integrity: Condition in which data has not been altered or destroyed in an un-authorized manner.
- Non-repudiation: Provides proof of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.

In addition to the technical security, the management and E-Governance components address the physical safeguard to be followed. Schedule II of IT Act 2000 gives the security guidelines for information technology (IT) systems. It is essential that all the E-Governance system follow these guidelines to establish appropriate security process. Following are the guidelines:

- Security Policy: Adopting a security process that outlines organization's / department's expectations for security, which can then demonstrate management's support and commitment to security.
- Security Structure: Having a management structure for security, delegating security management responsibilities and establishing security incidence response process.
- Asset Classification: Conducting a detailed assessment and inventory of information infrastructure and information assets to determine an appropriate level of security.
- Personal Security: Making security a key component of human resources and E-Governance operations.

- Physical and environmental Security: Establishing a policy that protects the IT infrastructure, physical plant and employees.
- Monitoring and Control: Implementing preventive measures such as anti-virus protection, maintaining and monitoring logs and having incident response procedures.
- Access Control: Protecting against internal abuses and external intrusions by controlling access to network resources.
- Continuity Plan: Planning for disasters, natural and man-made, and recovering from the disasters.

9.9 Communication

9.9.1 Overview

Communication layer deals with the intra process communication within application systems as well as the intercommunication between systems. Its functions spread over all the layers.

9.9.2 Modes and Components of Communication

- Server to Server
- Client to Server
- Communication with Legacy Systems
- Batch Processing
- Program to Program

- Network Protocols:

LAN/WAN Internetworking Protocols are required to communicate from one computer to another.

Wireless LAN specification is required to support Internet based access from mobile devices.

- Application protocols

This includes File Transfer Protocol for exchanging files.

Hypertext Transfer Protocol (HTTP) used for communication between client and server.

Simple Mail Transfer Protocol (SMTP) for exchanging messages.

Post Office Protocol (POP) for electronic mail communication.

- Directory Access

Directory Access Protocol is necessary to locate and access information stored in standard directories that provide a centralized or distributed repository of an organisation, people, IT resources etc.

9.10 Management

9.10.1 Overview

Management of the organization plays vital role to implement the Standards for achieving the interoperability & integration of various applications of E-Governance. Management will not only present the functional aspects of the interoperability of standards to all the stakeholders, but also establish the policies and guidelines for physical management architecture of interoperability.

The rules for adherence of the standards, regularity mechanism, inter linkages with other organization/customer etc are some of the important components of the management layer. The tasks of establishing and deploying standards for various ICT processes and enforcing the same across the organization will be a challenging role of the management. The co-ordination with the other layers in the overall framework of interoperability architecture is based solely on policy-based management. The monitoring of various functional units of the organization regarding the compliance with the standard, monitoring of the environment and also interaction with international bodies and the vendors will be the operators of the management layer.

9.10.2 Need for Management Standards

- To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- To ensure compliance of systems with organizational policies and standards
- To ensure that various standards set by the Department's Management, international bodies, other Government agencies are implemented and that the ICT Processes within the Department are compliant with them.

10. Software Architecture

Interoperability and integration of Government services depend on the sharing of data within and across departments. However, the large number of E-Governance applications developed in isolation, resulted in self-contained islands of information. Every application followed its own standards with the main objective of delivering process-centric results irrespective of other applications. Hence, at the outset there is a need for an architecture that is aimed at reuse and customization.

10.1 Middleware and Technology Standards

There is a need to introduce the concept of middleware and technology standards as a tool to develop integrable, scalable and robust E-Governance solutions, while employing multiple solution providers. The middleware should support processes involving multi-department and multi-agency workflows. For this purpose, it is necessary that the different department offices and also external agencies are interconnected and share the same underlying back-end databases and applications. The middleware also should be able to facilitate integration with legacy systems.

Middleware needs to provide services such as identification, authentication, authorization, directories, and security to all applications. By promoting standardization and interoperability, middleware will make advanced network applications much easier to use. The key middleware components are (a) Web Application Server, (b) Inter-application communication and messaging and collaboration software (c) Language and data interchange standards.

10.2 Using Service-Oriented Architecture(SOA) and Component- Based Development to Build Web Service Applications

Service-Oriented Solutions: Applications must be developed as independent sets of interacting services offering well-defined interfaces to their potential users. Similarly, supporting technology must be available to allow application

developers to browse collections of services, select those of interest, and assemble them to create the desired functionality.

A service is generally implemented as a coarse-grained, discoverable software entity that exists as a single instance and interacts with applications and other services through a loosely coupled (often asynchronous), message-based communication model.

In many ways, the terminology for services is much the same as the terminology used to describe component-based development; however, there are specific terms used to define elements within Web services

Service : A logical entity; the contract defined by one or more published interfaces.

- Service provider: The software entity that implements a service specification.
- Service requestor: The software entity that calls a service provider. Traditionally, this is termed a “client”; however, a service requestor can be an end-user application or another service.
- Service locator : A specific kind of service provider that acts as a registry and allows for the lookup of service provider interfaces and service locations.
- Service broker: A specific kind of service provider that can pass on service requests to one or more additional service providers.

This description of services, and the context of their use, imposes a series of constraints. Furthermore, efficient use of services suggests a few high-level best practices. Here are some key characteristics for effective use of services:

1Coarse-grained -Operations on services are frequently implemented to encompass more functionality and operate on larger data sets, compared with component-interface design.

2Interface-based design - Services implement separately defined interfaces. The benefit of this is that multiple services can implement a common interface and a service can implement multiple interfaces.

3Discoverable - Services need to be found at both design time and run time, not only by unique identity but also by interface identity and by service kind.

4Single instance - Unlike component-based development, which instantiates components as needed, each service is a single, always running instance that a number of clients communicate with.

Loosely coupled services are connected to other services and clients using standard, dependency-reducing, decoupled message-based methods such as XML document exchanges.

Asynchronous — In general, services use an asynchronous message passing approach; however, this is not required. In fact, many services will use synchronous message passing at times.

Some of these criteria, such as interface-based design and discoverability, are also used in component-based development; however, it is the sum total of these attributes that differentiate a service-based application from an application developed using component architectures such as a J2EE or .NET.

10.3 Component ware Architecture

Component ware Architecture enables efficient reuse of existing application assets, faster deployment of new applications, and improved responsiveness to changing business needs. Reusable software components are the building blocks that make a system able to respond quickly to change. Components are program modules that provide a complete package of business functionality. Shared components must be designed for portability across platforms.

Components within an application system can be developed in any supported language, with any development tool appropriate for the particular tier where they are deployed.

10.4 Reusability

Software reuse must become a key part in the software architecture. The continuing need for speeding up the software development life cycle and reducing the cost of development to manageable proportions exists in all large software projects. One of the ways to address this requirement is to have reusable software components. Systematic techniques for reuse adoption must therefore be enabled. Planning for reuse must begin at the architecture stage itself.

Some of the advantages are as follows:

- Software can operate in heterogeneous environments.
- Software can be customized for any environment.
- Software can be delivered in local languages and standards

In short it delivers the much needed openness and flexibility.

11 Supporting Network Architecture

The Network Architecture defines a unified, high-speed statewide network based on open systems standards. The biggest benefit to a nation wide network solution is the ability to efficiently share information processing resources across the enterprise. When departments share common application services and data, they avoid duplicative efforts and costs. The key to successfully sharing these resources is a network connecting all state departments together in a way that reduces redundancy. A nation wide network must be strategically planned, strongly backed, and expertly managed. This network must:

- Utilize standard communication protocols.
- Sustain and support high capacity and high performance communication.
- Be scalable, reliable, and extensible
- Provide a variety of advanced telecommunications functions.
- Smoothly integrate with other private and public communication networks.

12 Implementation Plan

12.1 IFEG Advisory Group

The overall Interoperability Framework should be coordinated by an advisory group (EAG). Members should be drawn from Government Departments, Academia and the Industry. The Advisory Group will be mainly responsible for:

- Devising suitable and appropriate mechanisms for proper coordination of the Interoperability framework (IF).
- Ensure compliance with the Interoperability Framework for any new system.
- Periodic review of the framework. Suitable updation in the framework so as to include technological advancements.
- Will have to promote the production and management of the XML schemas necessary to support data interoperability.
- Coordinate the various working groups.

12.2 Data Standards working group:

The primary responsibility of this group would be to lay out the specifications and development of data Standards in the form of common schemas. The common schemas will define the information model and XML schema of data elements.

This group will coordinate the management of XML schema. They will serve as the reusable components for composing project-defined data specifications.

12.3 Schemas working group

This will be a specialist group for:

- Development of the schemas

- Setting the specifications for and coordinating the production of XML schemas
- Any new schemas developed will have to be submitted for review to this group, for acceptance and publication.
- They will keep track of international XML specifications through links with standards organizations such as W3C and OASIS.

12.4 Domain level Standards for Data and Metadata

The Data Standards working group will develop the data standards in the form of common schemas. The common schemas define the information model and XML schema of data elements that are used in E-Governance applications and they serve as reusable components for composing project-defined data specifications.

XML working group will develop the XML Schema design and Management Guide. This will provide a methodology to convert information models into XML.

By bringing together all the relevant specifications under an overall framework, IT management and developers can have a single point of reference when there is a need to identify the required interoperability specifications that should be followed.

The IFEG Metadata working group will be responsible for development and maintenance of E-Governance metadata standards. The broad principles to be followed by this working group are as follows:

- It should not be vendor or product specific.
- It should be compliant with internationally recognized standards.
- It should have the capacity to be scaled for changing demands.
- It should be based on the International Dublin core model.

12.5 Interoperability Working Group

This group will be responsible for all aspects of the framework including policies, specifications, implementation and management.

12.6 Working Group on Government Process

This group will be primarily responsible for identifying Process and Data handling aspects across Government Organisation.

12.7 Component Library Working group

This group will be responsible for all aspects relating to the maintenance of the component library and their reusability. It is suggested that the working group can elaborate on the following areas of component repository.

- Identify areas for creation of components
- Access modality specifications
- Contribution Modality / Technical Evaluation
- Repository Management
- Deployment Management
- Version Control
- Documentation

12.8 Working Group for Legacy Applications

As legacy applications should also be made to interoperate, a working group will be formed which will recommend the framework / methodology to be adopted in getting the legacy application interact with other applications.

12.9 Working group on Network Layer

This working group will review the new standards evolving under Network technology to be incorporated in the IFEG document.

12.10 Working group on Security Layer

This working group will review the new standards evolving under Security to be incorporated in the IFEG document.

12.11 Working Group for Auditing/Review of the Standards

The standards developed by each working group will have to be audited before they are published.

The above working groups will operate under the E-Governance Advisory Group (EAG). In addition to these working groups, specialist groups in some domains can be formed to work on Interoperability Framework for their respective domains. This will be monitored by the EAG and finally be included in the IFEG Library.

12.12 Government Process Group

A “Government Process Group” should be included to identify and rationalize processes and data handling.

13 Technical Standards Specifications for IFEG

This section contains suggested specifications and technical standards for the E-Government Interoperability Framework. The IFEG covers the following basic domains.

- Information Access
- Presentation
- Process
- Data Integration
- Data Schema
- Metadata
- Network
- Security
- Communication
- Management

The different interoperability components under each domain area are listed in the following tables together with the standard specification and the rationale for selection.

Description of the Table:

- **Specification:** This will list down the standards relating to each component under the specific layer in standard way.
- **Standard Name and Version No:** The Name of the standard and its version number with links to the respective sites(if any) will be specified under this column
- **Owner:** This will specify the owner of the standards
- **Nature of the Standard:** This will indicate if it is open source or Community based
- **Maturity Level:** The maturity level may be specified either as 'Matured' or 'Evolving'.

- **Nature of recommendation:** This will have one of three distinct values such as 'Under Observation', 'Recommended', or 'Mandatory'
- **Remarks:** This will give the rational for selecting the specific standard.

Adoption of Standards:

It is proposed to follow three different guidelines on adopting the standards. They are Under Observation, Recommended or Mandatory. In addition, a list of black listing of standards will also be maintained. The following sequence is followed when a new standard is to be introduced.

The standards working group will review the new / upcoming standards. This stage is known as under observation. At this stage, the group may either accept or reject the same. If the same is rejected, the same will be marked to black list. In case, the same is accepted, the same may be kept either as recommended or may be considered mandatory subject to the fulfillment of following conditions.

Mandatory: Only standards that are in use and are mature in nature and if it is of open standards or community supported, then the standard will be mentioned as Mandatory. If mandatory is specified in this document then the same has to be necessarily enforced in all the applications.

Recommended: In case, no specific mandatory standard is specified or more than one standard is specified and if there is a requirement to use the specific standard which has been classified as recommended, then that standard may be adopted with necessary justification.

Under observation: Some of the standards, which are new may be kept under observation till it matures.

This document will specify the Nature of recommendation as **Recommended** till it is in draft version.

13.1 Access

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--|------------------------------|-----------------------|------------------------|----------------|--------------------------|---|
| 13.1 Information Access for Client applications | | | | | | |
| LAN | <u>IEEE 802.3 Family</u> | <u>IEEE</u> | Community | Mature | Recommended | The widely used standard for Ethernet LAN |
| WAN | <u>IP v4</u> | <u>Iana /internic</u> | Community | Mature | Recommended | Globally used standards for usage of IP based network |
| Wireless | <u>IEEE802.11b</u> | <u>IEEE</u> | Community | Mature | Recommended | High degree of product interoperability, for high-rate wireless LAN |
| LAN | | | | | | |
| Network | <u>TCP</u> | <u>ISO/OSI</u> | Community | Mature | Recommended | TCP is defined in Request For Comment (RFC) standards document number 793 [10] by the Internet Engineering Task Force (IETF). Most applications on the Internet make use of TCP |
| Layer | <u>UPD</u> | <u>ISO/OSI</u> | Community | Mature | Recommended | UDP used by some programs instead of TCP for fast data transmission |
| Mobile Access | | | | | | |
| | <u>GPRS</u> | <u>ETSI</u> | Community | Mature | Recommended | General Packet Radio Service |
| | <u>WAP</u> | <u>WAP Forum</u> | Community | Mature | Recommended | Wireless Application Protocol |
| | <u>SMS</u> | <u>ETSI</u> | Community | Mature | Recommended | Short Message Service |
| | <u>MMS</u> | <u>ETSI</u> | Community | Mature | Recommended | Multimedia Messaging Services |
| | <u>3G</u> | <u>ITU</u> | Community | Mature | Recommended | Industry standard for third-generation (3G) wireless networks and 3G CDMA efficiently provides high quality voice services and high-speed packet data access |
| Conferencing system over IP | | | | | | |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--------------------------|---|-------|------------------------|----------------|--------------------------|--|
| Assembly | ITU H.323 (07/03), version 5 | ITU | | Mature | Recommended | Standards for the assembly of Audio, Video, Data and Control (AVDC) |
| Audio | ITU G.723.1 and G.722 | ITU | | Mature | Recommended | Minimum audio standards |
| Video | ITU H.261 and H.263 | ITU | | Mature | Recommended | Minimum video standards |
| Data | ITU T.120 | ITU | | Mature | Recommended | Minimum data standards |
| Control and signal | ITU T.H.225 and H.245 | ITU | | Mature | Recommended | Minimum control and signal standards |
| VoIP | | | | | | |
| Assembly | ITU H.323 (07/03), version 5 | ITU | | Mature | Recommended | Standards for the assembly of Audio, Video, Data and Control (AVDC) |
| Gateway control | Media Gateway Control Protocol (MGCP): RFC 3435 | | | Mature | Recommended | Standards for multimedia gateways |
| | Media Gateway: RFC 2805 | | | | | |
| | Simple Gateway Control Protocol: RFC 3525 | | | | | |
| | Megaco Protocol version 1.0: RFC 3015 | | | | | |
| Application layer signal | Session Initiation Protocol (SIP): RFC 3261 | | | Mature | Recommended | An application-layer control (signal) protocol for creating, modifying, and terminating sessions with one or more participants |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--------------------------------|--|-------|------------------------|----------------|--------------------------|--|
| Resource setup | Resource ReSerVation Protocol (RSVP): RFC 2205 and RFC 2750 | | | Mature | Recommended | A resource reservation setup protocol designed for an integrated services Internet. RSVP provides receiver-initiated setup of resource reservations for multicast or uni-cast data flows |
| Transport and control protocol | Real Time Protocol (RTP) and Real Time Control Protocol (RTCP): RFC 3550 | | | Mature | Recommended | RTP and RTCP provide end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services |
| Delivery control | Real Time Streaming Protocol (RTSP): RFC 2326 | | | Mature | Recommended | RTSP is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video |
| Announcement protocol | Session Announcement Protocol (SAP): RFC 2974 | | | Mature | Recommended | An experimental RFC for multicast announcement of session description information and defines an announcement protocol |
| Session description | Session Description Protocol (SDP): RFC 2327 | | | Mature | Recommended | SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. Other SDP RFCs include RFC Recommended 3524 |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|-----------------------------------|---|------------|------------------------|----------------|--------------------------|--|
| Extended RTCP | RTP Control Protocol Extended Reports (RTCP XR): RFC 3611 | | | | | Defines the Extended Report (XR) packet type for the RTP Control Protocol (RTCP), and defines how the use of XR packets can be signaled by an application if it employs the Session Description Protocol (SDP) |
| Video Conferencing on ISDN & VSAT | <u>ITU H.320</u> | <u>ITU</u> | | Mature | Recommended | |
| | Audio - G.711, G.722, G.722.1, G.728 | | | | | |
| | Video - H.264, H.263, H.261 | | | | | |
| | Data - H.239, T.120 | | | | | |
| | Control: H.221, H.231, H.242, H.243 | | | | | |

13.2 Presentation

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--------------------------------------|------------------------------|--|------------------------|----------------|--------------------------|--|
| Hyper Text Markup Language | HTMLv3.2/HTML v4.01 | W3C | Community | Mature | Recommended | |
| Extensible Hypertext Markup Language | XHTML v1.0 | W3C | Community | Mature | Recommended | |
| Style Sheets | | | | | | |
| | CSS2 | W3C | Community | Mature | Recommended | Simple mechanism for adding style (e.g. fonts, colors, spacing) to Web documents. CSS2 simplifies Web authoring and site maintenance |
| Extensible Style Sheets | | | | | | |
| | XSL v1.0 | W3C | Community | Mature | Recommended | XSLT is a language for transforming XML documents into other XML documents. |
| Document | | | | | | |
| | .txt | W3C | Community | Mature | Recommended | Simple document is edited and exchanged using this standard |
| | rtf v1.6 | Rich Text Format (RTF) Version 1.6 Specification | Community | Mature | Recommended | Rich Text Format (RTF) Specification is a method of encoding formatted text and graphics for easy transfer between applications |
| Extensible Style Sheets | | | | | | |
| | XSL v1.0 | W3C | Community | Mature | Recommended | XSLT is a language for transforming XML documents into other XML documents. |
| Document | | | | | | |
| | .txt | W3C | Community | Mature | Recommended | Simple document is edited and exchanged using this standard |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|------------------------------|--|--|------------------------|----------------|--------------------------|---|
| | rtf v1.6 | Rich Text Format (RTF) Version 1.6 Specification | Community | Mature | Recommended | Rich Text Format (RTF) Specification is a method of encoding formatted text and graphics for easy transfer between applications |
| | pdf | Adobe | | Mature | Recommended | Platform independent portable document format |
| Spreadsheets | | | | | | |
| | CSV (comma separated values) | | Community | Mature | Recommended | The values are separated by commas, to indicate the separating points for columns |
| Graphics | | | | | | |
| | TIFF | Adobe Systems | Community | Mature | Recommended | Tag based file format for storing and interchange of images |
| | JPEG | ISO/JPEG Committee | Community | Mature | Recommended | Coding of still images of photographic quality |
| | PNG | PNG | Community | Mature | Recommended | PNG provides a useful format for the storage of intermediate stages with fully lossless compression |
| | ECW | ER Mapper | Community | Mature | Recommended | ECW is the popular format to cater for all image management with unmatched speed and performance |
| Moving Image | | | | | | |
| | MPEG | ISO/IEC | Community | Mature | Recommended | Open framework for multimedia delivery |
| Audio/Video Streaming | QuickTime (.avi,.mov,.qt) | Apple | Community | Mature | Recommended | Worldwide standards for the creation, delivery, and playback of multimedia over new, high-speed wireless networks |
| Character Sets and Alphabets | | | | | | |
| | ISO 10646-1:2000 | ISO | Community | Mature | Recommended | Universal multiple-octet coded character set that encompasses the world's scripts |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|---------------------------------|--------------------------------------|----------------------------|------------------------|----------------|--------------------------|--|
| | <u>UNICODE v3.0 UTF-8 and UTF 16</u> | <u>UNICODE</u> | Community | Mature | Recommended | Unicode is a universal encoding, any abstract character that ever could be encoded is potentially a member of the actual set to be encoded, whether we currently know of that character or not |
| Scripting | | | | | | |
| | <u>ECMA 262</u> | <u>Ecma international</u> | Community | Mature | Recommended | Scripting Language for consistency of browser |
| Smart Card | | | | | | |
| | <u>ISO 7816-1</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Physical characteristics |
| | <u>ISO 7816-2</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Dimensions and location of the contacts |
| | <u>ISO 7816-3</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Electronic signals and transmission protocols |
| | <u>ISO 7816-4</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Industry commands for interchange |
| | <u>ISO 7816-5</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Number system and registration procedure for application identifiers |
| | <u>ISO 7816-6</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Inter industry data elements |
| | <u>ISO 7816-7</u> | <u>ISO/IEC</u> | Community | Mature | Recommended | Inter industry commands for Structured Card Query Language (SCQL) |
| Geographical Information System | <u>GML3.0</u> | <u>Open GIS Consortium</u> | Community | Mature | Recommended | For storage and transmission of GIS data |
| | | | | | | |

13.3 Process

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|---------------------------------|------------------------------|------------|------------------------|----------------|--------------------------|---|
| Business Process | | | | | | |
| Business Process Modeling | <u>UML 1.5 8</u> | <u>OMG</u> | Community | Mature | Recommended | A specification defining a graphical language for visualizing, specifying, constructing, and documenting the artifacts of distributed object systems. |
| Software Process | | | | | | |
| Software Process Modeling | <u>UML 1.5 8</u> | <u>OMG</u> | Community | Mature | Recommended | A specification defining a graphical language for visualizing, specifying, constructing, and documenting the artifacts of distributed object systems. |
| Software Architecture Standards | Component Technology | | | | Recommended | Component based architecture allows high degree of reusability. |

13.4 Data Integration

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|-----------------------------------|------------------------------|--------------|------------------------|----------------|--------------------------|--|
| Web Services | | | | | | |
| Web service request delivery | <u>SOAP 1.2 1</u> | <u>W3C</u> | Community | Mature | Recommended | SOAP Version 1.2 (SOAP) is a lightweight protocol for exchanging structured information in a decentralized, distributed environment, independent of any programming model and other implementation specific semantics. |
| Web services description language | <u>WSDL 1.1 2</u> | <u>W3C</u> | Community | Mature | Recommended | WSDL is an XML format for describing network services as a set of endpoints operating on messages, regardless of the message format or network protocol used for communication. |
| Web service request registry | <u>UDDI 3.0 3</u> | <u>OASIS</u> | Community | Mature | Recommended | UDDI defines of a set of services supporting the description and discovery of (1) Web services providers, (2) the Web services they make available, and (3) the technical interfaces which may be used to access those services. |

13.5 Data

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|---|--|------------|------------------------|----------------|--------------------------|---|
| Data Schema Definition | <u>XML Schema Part 1</u> : Structures 4, XML Schema Part 2 : Datatypes 5 | <u>W3C</u> | Community | Mature | Recommended | XML Schemas provide mechanisms to define and describe the structure, content, and to some extent semantics of XML documents. |
| Data Transformation for Presentation | <u>XSL 1.0 6</u> | <u>W3C</u> | Community | Mature | Recommended | This specification defines the features and syntax for the Extensible Stylesheet Language (XSL), a language for expressing stylesheets. Given a class of arbitrarily structured XML documents or data files, designers use an XSL stylesheet to express their intentions about how that structured content should be presented. |
| Data Transformation for conversion from XML schema format to another format | <u>XSLT 1.0 7</u> | <u>W3C</u> | Community | Mature | Recommended | This specification defines the syntax and semantics of XSLT, which is a language for transforming XML documents into other XML documents. XSLT is designed for use as part of XSL. |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--|------------------------------|------------|------------------------|----------------|--------------------------|---|
| Data Modeling Language | <u>UML 1.5 8</u> | <u>OMG</u> | Community | Mature | Recommended | A specification defining a graphical language for visualizing, specifying, constructing, and documenting the artifacts of distributed object systems. |
| Data Description Language (for exchange of data) | <u>XML 1.1 9</u> | <u>W3C</u> | Community | Mature | Recommended | The Extensible Markup Language (XML) is a subset of SGML. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML. |

13.6 Meta Data

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|-------------------------------|------------------------------|------------|------------------------|----------------|--------------------------|---|
| Metadata Description Language | <u>RDF 11</u> | <u>W3C</u> | Community | Mature | Recommended | The Resource Description Framework (RDF) is a language for representing information about resources in the World Wide Web. It is particularly intended for representing metadata about Web resources. RDF can also be used to represent information about things that can be <i>identified</i> on the Web, even when they cannot be directly <i>retrieved</i> on the Web. |

13.7 Network

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|----------------------------|------------------------------|----------------|------------------------|----------------|--------------------------|---|
| Internet Protocol | IP v4 | iana /internic | Community | Mature | Recommended | Globally used standards for usage of IP based network |
| Wireless LAN | IEEE802.11b | IEEE | Community | Mature | Recommended | IEEE 802.11b is the standard for wireless LAN. It is most widely available and implemented. |
| Routing Information | BGP 4 | IEEE | Community | Mature | Recommended | IEEE 802.11b is the standard for wireless LAN. It is most widely available and implemented. |
| Video conferencing over IP | ITU H.261 and H.263 | | | | | Specifications for conferencing over IP |

13.8 Security

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--|------------------------------|-------------------------------|------------------------|----------------|--------------------------|---|
| Secure multipurpose Internet Mail Extension, which provides authentication, message integrity and non repudiation of origin (via digital signatures), and privacy and data security (via encryption) | <u>S/MIME v3</u> | Network Working Group/RSA LAB | Community | Mature* | Recommended | Ensures mail integrity and confidentiality. S/MIME was originally developed by RSA Data Security, Inc. It is based on the PKCS #7 data format for the messages, and the X.509v3 format for certificates. PKCS #7, in turn, is based on the ASN.1 DER format for data. |
| Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL | <u>HTTPS</u> | Netscape | | Mature* | Recommended | SSL is an open nonproprietary protocol that Netscape has proposed to W3C |
| Security Architecture for Internet Protocol, it is a standard for securing internet protocol | <u>IPSec</u> | IETF | | Developing | Recommended | RFC 2401 |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--|------------------------------|--|------------------------|----------------|--------------------------|---|
| Ensures Cryptographic Security and Interoperability | SSL V3.0 | IETF | Community | | Recommended | http://wp.netscape.com/eng/ssl3/ssl-toc.html |
| A block cipher - i.e. it acts on a fixed-length block of plaintext and converts it into a block of cipher text of the same size by using the secret key | 3DES | IBM/NSA/ NIST (National Institute of Standards & Technology) | Community | Mature | | http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html |
| Advanced Encryption Standard | AES | NIST | Community | Mature | | http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html |
| The Digital Signature Standard, created by the NIST, specifies DSA as the algorithm for Digital signatures | <u>DSA</u> | NIST | Community | Mature | Recommended | <u>NIST, specifies DSA as the algorithm for digital signatures and SHA-1 for hashing</u> |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|---|------------------------------|---|------------------------|----------------|--------------------------|--|
| <u>An public-key encryption technology developed by RSA Data Security, Inc.</u> | RSA | RSA Security Inc. | Community | Mature | Recommended | The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique |
| The Secure Hash Algorithm developed by NIST, along with the NSA. | SHA-1 | NIST/NSA | | | | The Secure Hash Algorithm (SHA), developed by NIST, along with the NSA, for use with the Digital Signature Standard (DSS) is specified within the Secure Hash Standard (SHS) SHA-1. SHA is a cryptographic message digest algorithm similar to the MD4 family of hash functions developed by Rivest. |
| Message-Digest Algorithm | MD5 | R. Rivest | | | | Request for Comments: 1321. |
| | | MIT Laboratory for Computer Science and RSA data Security Inc | | | | http://www.faqs.org/rfcs/rfc1321.html |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|---|------------------------------|-------------------------|------------------------|----------------|--------------------------|---|
| Password-Based Cryptography Standard | PKCS#5 | RSA Data Security, Inc | Community | Mature | Recommended | http://www.rsasecurity.com/rsalabs/node.asp?id=2127 |
| Cryptographic Message Syntax Standard | PKCS#7 | RSA | Community | Mature | Recommended | http://www.rsasecurity.com/rsalabs/node.asp?id=2129 |
| | V1.5 | Data Security, Inc | | | | - |
| This standard describes syntax for private-key information, including a private key for some public-key algorithm and a set of attributes | PKCS#8 | RSA , Data Security Inc | Community | Mature | Recommended | http://www.rsasecurity.com/rsalabs/node.asp?id=2130 |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of recommendation | Remarks |
|--|--|-------|------------------------|----------------|--------------------------|---|
| This is for cryptographic tokens to identify themselves to multiple, standards-aware applications, regardless of the application's cryptoki (or other token interface) provider. | PKCS #15 | RSA | Community | Mature | Recommended | http://www.rsasecurity.com/rsalabs/node.asp?id=2141 |
| XML Encryption Syntax and Processing | W3C XML Encryption Recommendation (REC). | W3C | | Developing | Under Observation | http://www.w3.org/TR/xmlenc-core/ |

13.9 Communication

| Specifications | Standard Name and Version No | Owner | Nature of Standard | Maturity Level | Nature of Recommendation | Remarks |
|----------------------|--|-------|--------------------|----------------|--------------------------|---|
| Hypertext Transfer | HTTP v1.1 | IETF | Community | Mature | Recommended | Application level protocol for exchanging files on the Internet |
| File Transfer | FTP | IETF | Community | Mature | Recommended | FTP is proposed as an IETF standard and defined in RFC 959. |
| E-mail Transport | SMTP | IETF | Community | Mature | Recommended | It is proposed as an IETF standard and defined in RFC 2821 and RFC 2822 and supported in popular email software |
| | MIME (Multipurpose Internet Mail Extensions) | IETF | | | Recommended | Globally accepted standard |
| Mailbox Access | POP3 | IETF | Community | Mature | Recommended | To access and retrieve mails stored in a server. |
| Directory Access | LDAP v3 | IETF | Community | Mature | Recommended | It is to provide access to X.500 and other directories |
| Domain Name Services | DNS | IETF | Community | Mature | Recommended | It is an IETF standard which is global and widely adopted. |

| Specifications | Standard Name and Version No | Owner | Nature of the Standard | Maturity Level | Nature of Recommendation | Remarks |
|--------------------------------|------------------------------|-------|------------------------|----------------|--------------------------|--|
| Newsgroup Services | NNTP | IETF | Community | Mature | Recommended | Protocol for distribution, inquiry, retrieval and posting of news standards. Protocol used by computer clients and servers for managing the notes posted on Usenet newsgroups. |
| Remote Method Invocation (RMI) | RMI | IETF | Community | Mature | Recommended | Communication between applications or application components. It is based on J2EE architecture. |

13.10 Management

13.10.1 Human Resources:

With the technology changing continuously, Human Resources component remain as one of ICT's major problems. Staff needs to be trained regularly. More often, job classifications are faulty and they neither reflect the Department's needs nor the qualifications of the recruits.

Responsibilities, generally horizontal in the ICT environment, are not clearly understood nor efficiently discharged. Some procedures and Good Practices related to Human Resources are set by identifying the:

- Required Competencies per Position
- Actual Competency Levels of all Staff
- Analyze Competencies to Identify Training Requirements
- Training Resources
- Managing Training Material
- Maintaining Training Records
- Recruitment Standards

13.10.2 Change Management: One of the important aspects of the Human Resource management is Change Management. A proper plan for upgrading the skills of employees should be in place. This should include system designers and application developers aware of adhering to standards as envisaged in IFEG. A thorough training on migrating the existing applications to IFEG complaint without disturbing the existing system should be planned. Similarly, while developing new applications, the Standards, as put forth in IFEG should be enforced. This requires complete training and follow-up on IFEG standards.

13.10.3 Workflow component ensures that the flow of tasks within an organization to complete a transaction moves smoothly and in the correct order. For example, a citizen sends a letter of complaint to the e-mail link at the bottom of one of your web pages. The Webmaster or e-mail recipient forwards the letter to the appropriate department. The department addresses the problem and sends a response to the citizen.

13.10.4 Electronic Data Interchange provides the transfer of large bodies of data electronically through the use of established standards. Usually, EDI is used in larger Governments and business to conduct secure business transactions electronically.

13.10.5 Business Process Reengineering (BPR)

Business Process Re-engineering Standards – BPR is the process of studying and, if required, re-engineering the existing processes of an organization to achieve efficiency and effectiveness in its business goals. In the context of E-Governance, a BPR exercise additionally focuses on the potentialities offered by ICTs in achieving a government department's goals with respect to its efficiency and effectiveness of service delivery. It is important to explore and evolve a standardized procedure/model for carrying out a BPR exercise, keeping in mind the importance of effective service delivery through joined-up services. This could mean the evolving of a service-oriented BPR exercise rather than a Government-function based exercise.

- Define the task assigned for the process
- Identify potential areas for automation
- Divide the potential business functions into processes and sub processes
- Determine the inputs, processing activities and outputs for each of the process and sub-processes
- Measure the service level process metrics in terms of operational efficiencies like lead times, effort and costs
- Identify bottlenecks in the process
- Identify redundancies in terms of actors involved in the process, their roles and responsibilities and take a critical look at the same.

- Identify areas of improvement and need for reengineering
- Communicate, brainstorm and counsel the stake holding business entities regarding process and Structural changes
- Policy and procedural changes
- Radical improvement in the productivity / output of the
- Process
- Implement the reengineered process
- Monitor the performance of the process with reference to the defined task

This process results in

- Better and increased bargaining power with the vendors
- Reduced lead time in procurement and delivery by 50%
- Elimination of purchase and evaluation processes at the District level
- Effective utilization of Government machinery

13.10.6 Outsourcing - Whenever an outsourcing project is undertaken, a set of standard procedures, policies and guidelines need to be in place to ensure that the outsourced ICT deliverable adheres to the specified IFEG interoperability standards. The standard procedures would be part of the outsourcing procedures such as RFP and outsourcing agreement. Every iota of the partnering companies should be considered while evaluating an outsourcing vendor

- Ensure proper planning procedures are in place which will allow the ICT department to identify outsourcing opportunities
- Performance and service standards has to be separately identified
- Costs of the program area are properly benchmarked
- Clear and measurable objectives are properly defined
- Evaluation criteria has to be established
- Ensure adequate documentation

13.10.7 Request for proposals:

The request for proposals should provide a clear, precise and accurate description of the requirement for the work and the expected activities, services, products and level of effort to be delivered under the contract.

13.10.8 Interoperating with Legacy Applications:

There are already a number of successful software applications that are running on a variety of platforms and language environments within the government framework. These applications can be broadly classified into the following

- **Applications which do not need to interoperate with any other application.** This could be any internal government application, which is not directly involved in any service delivery process.
- **Applications which need to interoperate, as they are part of a larger service delivery framework.** One solution to enable interoperability of these applications with newer applications is to migrate them to newer application & architecture environments. However, such a strategy may not always be acceptable in view of certain time and cost constraints. Further, the application itself may be a well-tested, robust application, which is also mission critical. This rules out the possibility of introducing a newer version on an immediate basis. In such situations, it may be required to accept the legacy application as it is and look for a more immediate but reliable solution that ensures its interoperability with other peer applications.

Building a web-service-aware wrapper application around the legacy application usually facilitates this requirement. The purpose of building the wrapper application is to hide the technical complexities that may arise from the archaic technologies used by the legacy application. Invoking the wrapper application through a web service could then access the services of the legacy application.

A working group would be required to look into the technical complexities of such legacy applications on a case-to-case basis and suggest customized solutions and migration strategies for them.

13.10.9 Electronic Data Interchange:

Interoperability and Conformance following EDI standards need to be adopted:

- ANSI X12

- National standards - developed by Accredited Standards Committee
- EDIFACT
- Worldwide standards - developed by a UN committee provide a framework for formatting a given EDI message.

14. Annexure

14.1 Annexure 1 -Additional references

International Initiatives:

United Kingdom: This was the first electronic Government Interoperability Framework to be created. Office of the envoy: E-Government Interoperability Framework Version 5.0 2003

http://www.govtalk.gov.uk/documents/e-gif_v5_part1_2003-04-25.pdf

http://www.govtalk.gov.uk/documents/e-gif_v5_part2_2003-04-25.pdf

Hong Kong

http://www.itsd.gov.hk/itsd/english/infra/eif.htm - if_spec

New Zealand has mandated the use of their e-GIF23 for use by Government agencies.

<http://www.E-Government.govt.nz/docs/e-gif-v-1-0/>

Germany

http://www.kbst.bund.de/Anlage304417/Saga_2_0_en_final.pdf

Malaysia

<http://www.mampu.gov.my/mampu/bm/program/ICT/ISPlan/ispdoc/Interoperability Framework.pdf>

Australia

http://www.egov.dpc.wa.gov.au/docs/e-gif_technical_standardsV0-4August.pdf

Italy

<http://www.innovazione.gov.it/ita/documenti/emodel.zip>

14.2 Annexure 2: Glossary of Terms

| | |
|----------------|---|
| 3DES | Triple Data Encryption Standard |
| 3G | Third Generation Mobile Phones |
| AH | Authentication Header |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| Authentication | A way of making sure people is who they say they are so that the right people get access to the right information or service. |
| ANSI | ANSI American National Standards Institute (USA) |
| ASCII | American Standard Code for Information Interchange |
| B2B | Business to Business |
| CCS | Coded Character Set |
| CDMA | Code Division Multiple Access |
| CSV | Comma Separated Variable |
| CMS | Content Management System |

| | |
|-----------|---|
| CORBA | Common Object Request Broker Architecture |
| CSS | Cascading Style Sheets Language |
| DES | Data Encryption Standard |
| DNS | Domain Name System |
| DSA | Digital Signature Algorithm |
| DSML | Directory Services Markup Language |
| DSS | Digital Signature Standard |
| Directory | A central list of Government agencies and staff that is used within Government organisations to manage access to information systems within and between agencies. |
| DOM | Document Object Model - a tree-based representation of an XML document. The whole document is parsed before the document can be read - considered suitable for small XML documents. |
| DNS | Domain Name Server |
| ebXML | E-business XML - a joint project of the UN and OASIS to bridge electronic document interchange (EDI) and XML |
| EDI | Electronic Data Interchange |
| EGU | The E-Government Unit of the State Services Commission |
| ESP | Encapsulating Security Payload |
| ERP | Enterprise Resource Planning |
| FTP | File Transfer Protocol |
| G2B | Government to Business |
| G2C | Government to Citizen |
| G2E | Government to Employee |
| G2G | Government to Government |
| GIF | Graphic Interchange Format |
| GPRS | General Packet Radio Service |

| | |
|-----------------|--|
| GSM | Global System for Mobile Communications |
| GCSB | Government Communication Security Bureau |
| GML | Geography Markup Language |
| Guideline | A statement of desired, good or best practice approved by the Government, or its nominee (i.e. the e-GIF governing body). Generally non-compulsory. |
| HTML | Hypertext Markup Language - the lingua franca of the Internet |
| HTTP | Hypertext Transfer Protocol |
| IEEE | Institute of Electrical and Electronic Engineers |
| IMAP | Internet Message Access Protocol |
| IP | Internet Protocol |
| J2EE | Java 2 Platform, Enterprise Edition |
| JPEG | Joint Photographic Experts Group |
| JSP | Java Server Pages |
| JDBC | Java Database Connectivity |
| JPEG | Joint Photographic Experts Group |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Message Authentication Code |
| MIME | Multipurpose Internet Mail Extensions |
| MPEG | Moving Picture Experts Group |
| Metadata | Electronic catalogue entries that describe information and services in a structure way. The information in a library card system is metadata that helps you find books you want. |
| MIME and S/MIME | Multi-Purpose Internet Mail Extensions and Secure Multi-Purpose Internet Mail Extensions |
| NAT | Network Address Translation |

| | |
|----------|--|
| OASIS | Organization for the Advancement of Structured Information Standards |
| PDA | Personal Digital Assistant |
| PKI | Public Key Infrastructure - a lock and key system that allows one person to scramble information before sending it to another in a way that can be unscrambled only by the person holding the appropriate key. |
| PNG | Portable Network Graphic |
| Policy | A formal statement of compulsory practice made by the Government. |
| PDF | Portable Document Format |
| PKCS | Public Key Cryptography Standards |
| PNG | Portable Network Graphics |
| POP | Post Office Protocol |
| RDF | Resource Description Framework |
| RFC | Request for comments |
| RFP | Request for Proposals |
| RMI | Remote Method Invocation |
| SAX | Simple API for XML - an event based parser for XML documents that is useful for reading large XML documents as they continue to load. |
| S.E.E.TM | Secure Electronic Environment |
| SGML | Standard Generalized Markup Language |
| SHA | Secure Hash Algorithm |
| SMS | Short Messaging Service |
| SMTP | Simple Mail Transfer Protocol |
| SSL | Secure Sockets Layer |
| SOAP | Simple Object Access Protocol |
| SSC | State Services Commission |

| | |
|-----------------|---|
| Stakeholder | Any person or organisation with a vested interest in a public resource or the public good. While each agency will have its own definition of stakeholders, they will generally include, Parliament, the Government-of-the-day, individual Ministers, the public, customers, businesses, or other Government agencies etc. |
| Standard | Either an agreed process/practice/tool promulgated by an Internationally approved standards setting body |
| Structured Data | Information that has been organised to allow identification and separation of the context of the information from its content. |
| SVG | Scalar Vector Graphics |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| TIFF | Tagged Image File Format |
| TLS | Transport Layer Security |
| UDP | User Datagram Protocol |
| UDDI | Universal Description, Discovery and Integration |
| VML | Vector Markup Language |
| VPN | Virtual Private Network |
| W3C | World Wide Web Consortium |
| WAN | Wide Area Network |
| WAP | Wireless Application Protocol |
| WFS | Web Feature Server |
| WMS | Web Map Server |
| WSDL | Web Services Definition Language |
| XMI | XML Metadata Interchange |
| XHTML | Extensible Hypertext Markup Language |
| XML Schema | W3C extensible markup language (XML) schema definition language for defining the structure, contents and semantics of XML documents. |

| | |
|------|---|
| XSL | Extensible Stylesheet Language |
| XSD | Extensible Markup Language Schema Definition |
| XSLT | Extensible Stylesheet Language Transformation |

14.3 Annexure 3 Quick reference guide for standards

| | | |
|-----------------------|----------|---|
| Networks | IPv4 | http://www.ietf.org/rfc/rfc0791.txt |
| | IPv6 | http://www.ietf.org/rfc/rfc2460.txt |
| | HTTP/1.1 | http://www.ietf.org/rfc/rfc2616.txt |
| | UDP | http://www.ietf.org/rfc/rfc0768.txt |
| Mail Transfer | SMTP | http://www.ietf.org/rfc/rfc2821.txt |
| Directory Services | LDAPv3.0 | http://www.ietf.org/rfc/rfc1777.txt |
| Name Services | DNS | http://www.ietf.org/rfc/rfc1035.txt |
| Security | SSLv3.0 | http://home.netscape.com/eng/ssl3 |
| S-HTTP | | |
| File Transfer | FTP | http://www.ietf.org/rfc/rfc0959.txt |
| | HTTP/1.1 | http://www.ietf.org/rfc/rfc2616.txt |
| Primary character set | UTF-8 | http://www.ietf.org/rfc/rfc2279.txt |
| Web Services | XML | http://www.w3c.org/XML |
| | SOAP 1.1 | http://www.w3.org/TR/SOAP |
| | WSDL 1.1 | http://www.w3.org/TR/wsdl |
| | Schemas | |
| | | http://www.w3.org/TR/xmlschema-1 |
| | | http://www.w3.org/TR/xmlschema-2 |
| Transformation | XSL | http://www.w3.org/TR/xsl |
| | XSLT | http://www.w3.org/TR/xslt |
| | Metadata | http://dublincore.org |

14.3 Annexure 4: Table of Mission Projects of DIT for National E-Governance

| S.No | Mission Mode Projects | Line Ministries/ Departments responsible |
|---------------------------|-------------------------------------|---|
| Central Government | | |
| 01 | Income Tax | Ministry of Finance/Central Board of Direct Tax |
| 02 | Passport Visa & Immigration Project | Ministry of External Affairs/Ministry of Home Affairs |
| 03 | DCA21 | Department of Company Affairs |
| 04 | Insurance | Deptt. Of Banking |
| 05 | National Citizen Database | Ministry of Home Affairs/Registrar General of India (RGI) |
| 06 | Central Excise | Department of Revenue/Central Board of Excise & Custom |
| 07 | Pensions | Dep't. Of Pensions & Pensioners welfare & Dep't. Of Expenditure |
| 08 | Banking | Dept. of Banking |

| State Government (tentative, to be finalized in consultation with the States) | | |
|--|------------------------|--|
| 01 | Land Records | Ministry of Rural Development |
| 02 | Road Transport | Ministry of Road Transport & Highway |
| 03 | Property Registration | Department of Land Resources |
| 04 | Agriculture | Department of Agriculture & Cooperation |
| 05 | Treasuries | Ministry of Finance |
| 06 | Municipalities | Ministry of Urban Development and Poverty Alleviation |
| 07 | Gram Panchayats | Ministry of Rural Development |
| 08 | Commercial Taxes | Ministry of Finance |
| 09 | Police (UTs initially) | Ministry of Home affairs |
| Integrated Services | | |
| 01 | EDI (E-Commerce) | Ministry of Commerce and Industry |
| 02 | E-Biz | Department of Industrial Policy & Promotion / Department of Information Technology |
| 03 | Common Service Centres | Department of Information Technology |
| 04 | India Portal | Department of Information Technology and Department of Administrative Reforms and Public Grievances |
| 05 | EG Gateway | Department of Information Technology |