Brazilian Government

Executive Committee on Electronic Government

e-PING
Standards of Interoperability for Electronic Government

Reference Document
Version 2.0.1
December 5, 2006

GOVERNO FEDERAL

SUMMARY

PRESENTATION **4**

PART I - OVERVIEW OF THE e-PING **5**

1. INTRODUCTION **6**

2. SCOPE **7**

2.1. Subscribing to the e-PING 8
2.2. Focus on Interoperability 8
2.3. Subjects not Approached 8

3. OVERALL POLICIES **9**

4. SEGMENTATION **10**

4.1. Interconnection 10
4.2. Safety 10
4.3. Means of Access 10
4.4. Organization and Exchange of Information 11
4.5. Areas of Integration for Electronic Government 11

5. ADMINISTRATION OF THE e-PING **12**

5.1. Background 12
5.2. Implementation Strategy 13
5.3. Managerial Model 13
    5.3.1. Attributions 14
    5.3.2. Responsibilities 15
5.4. Additional activities 15
    5.4.1. Selection and Approval of Technological Standards 15
    5.4.2. Conformity Auditing 16
    5.4.3. Site Creation and Maintenance 16
    5.4.4. Legal and Institutional Support 16
    5.4.5. Dissemination 17
    5.4.6. Capacity Building 17
5.5. Relationship with Governments and Society 17
    5.5.1. Federal Government - Executive Branch Organizations 17
    5.5.2. Other Government Instances (otherFederal Branches, State and Municipal governments) 18
    5.5.3. Private Sector and Third Sector Organizations 18
    5.5.4. Citizenry 18

PART II. TECHNICAL SPECIFICATION COMPONENT OF THE e-PING 19

6. INTERCONNECTION 20
6.1. Interconnection: Technical Policies 20
6.2. Interconnection: Technical Specifications 21
6.3. WEB Services 22
6.4. Electronic Messages (e-mail) 23
6.5. Wireless LAN 24
6.6. VPN 24
6.7. Peer-to-peer Networks 24

7. SAFETY 25
7.1. Safety: Technical policies 25
7.2. Safety: Technical specifications 26

8. MEANS OF ACCESS 30
8.1. Means of Access: Technical Policies 30
8.2. Means of Access: Technical Specifications for Work Stations 31
8.3. Means of Access: Technical Specifications for Tokens and Smart Cards in General 35

9. ORGANIZATION AND EXCHANGE OF INFORMATION 41
9.1. Organization and Exchange of Information: Technical Policies 41
9.2. Organization and Exchange of Information: Technical Specifications 41
9.3. Notes on XML and MIDDLEWARE 41
9.4. Notes on Subjects under Study and Elaboration 42

10. AREAS OF INTEGRATION FOR ELECTRONIC GOVERNMENT 43
10.1. Areas of Integration for Electronic Government: Technical Policies 43
10.2. Areas of Integration for Electronic Government: Notes on the Catalog of XML SCHEMAS 43
10.2.1. Brief Considerations 43
10.2.2. Objective 43
10.2.3. Scope 44
10.2.4. Property and Responsibility 44
10.2.5. Mechanisms for Managing the Catalog of XML Schemas 44
10.2.6. Standards for XML Schemas 45
10.2.7. Classification of the XML Schemas Catalog 45
10.3. Areas of Integration for Electronic Government: Technical Specifications 46

11. GLOSSARY OF ACRONYMS AND TECHNICAL TERMS 50

12. BIBLIOGRAPHY 56
13. LIST OF COLLABORATORS 57

PRESENTATION

The e-PING architecture - Standards of Interoperability for Electronic Government - defines a minimum group of assumptions, policies, and technical specifications, which regulate the utilization of the Information and Communications Technology (ICT) in the interoperability of Services of Electronic Government, establishing the conditions for interaction with other spheres of power and government agencies, and with the society in general.

The areas covered by the e-PING are as follows:

- Interconnection
- Safety
- Means of Access
- Organization and Exchange of Information
- Areas of Integration for Electronic Government.

For each one of those segments there are specific components and the respective standards.

The whole content of this reference document complies with the guidelines of the Electronic Government Executive Committee created by the October 18, 2000 Decree, and is available in the Internet (http://www.eping.e.gov.br) in order to provide public access to common interest information, and intrinsic transparency to the e-gov initiative. The Brazilian government is committed to assuring that these policies and specifications stay aligned with the needs of the society and with the technology and market evolution.

The reference document for the e-PING contains:

- The foundations for the conception, implementation, and administration of the e-PING, the expected benefits, the reach of the e-PING architecture, the assumptions made, and the established policies.
- The managerial model of the e-PING, including the assignment of responsibilities, the criteria for verification of conformity, the change management procedures, and the guidelines for popularization and capacity building.
- The policies and technical specifications of all components of each one of the e-PING segments.
- A glossary of technical terms.
- A list of professional who collaborated in the preparation of the present document.

Part I. Overview of the e-PING

1. Introduction

The main requirement for the supply of better services that are appropriate to the citizens and the businesses at a lower cost is the availability of an infrastructure of Information and Communications Technology (ICT) for service delivery. Modern governments, which aim at being integrated and efficient, require systems which are equally modern, integrated, interoperable, and which operate in the public sector with integrity, security, and consistency.

In this context, the interoperability of technologies, processes, information, and data is a vital condition for the provision of quality services, and is an assumption all over the world for the electronic government concept - the e-gov. Interoperability allows rationalizing ICT investments through sharing, reutilization, and exchange of technological resources.

Countries such as the US, Canada, Britain, Australia, and New Zealand invest heavily in the development of policies and processes, and in developing ICT standards having set up structures for achieving interoperability to provide better quality and lower cost government services.

The Brazilian government is consolidating its e-PING architecture to serve as a paradigm for the establishment of policies and technical specifications that will allow for the provision of high quality electronic services to the society.

What is Interoperability?

For the establishment of the e-PING objectives it is fundamental to define clearly, what is meant by interoperability? Four definitions, which the Brazilian government has used to build its own conception, are presented below.

"Coherent exchange of information and services among systems. It should allow replacing any component or product used at the intersecting points by another one of similar specification without compromising the functionalities of the system" (United Kingdom Government.)

"Ability to transfer and to use information in a uniform and efficient way between several organizations and systems of information” (Australian Government.)

"Ability of two or more systems (computers, communications means, networks, software and other components of information technology) to interact and interchange data in accordance with a defined method, to obtain the expected results." (ISO.)

"Interoperability defines whether two components of a system, developed with different tools, coming from different suppliers, can or cannot work together". (Lichun Wang, European Institute of Computer Science. CORBA Workshops.)

Interoperability is not only the integration of systems nor is it only the integration of networks. It does not only refer to the exchange of data among systems neither does it simply contemplate the choice of technology.

It is actually the sum total of all these factors while considering also the existing systems, hardware platforms and working software. It builds on principles that deal with the diversity of components and the use of products from several different suppliers. It aims at considering all of the pertinent factors so that the systems can cooperate with each other, and establishes the norms, the policies, and the necessary standards for the attainment of those objectives.

For interoperability to be conquered, the users should be engaged in a continuous effort to assure that the systems, the processes, and the cultures of an organization are managed and directed to maximize the opportunities for the exchange and recycling of information.

2. Scope

Clearly defined policies and specifications of interoperability and management of information are fundamental to propitiate the government's connectivity, both internally and in relation to the society and, more widely speaking, with the rest of the world - other governments and companies operating in the world market. The e-PING is conceived as a basic structure for electronic government strategy, starting within the Executive Branch of the federal government, but not restricting the participation on a voluntary basis of other branches and spheres of government.

The government's information resources are valuable economic assets. While guaranteeing that government information can be quickly located and exchanged between the public sector and the society under privacy and safety conditions, the government will foster the widespread use of information to stimulate the country's economic development.

The e-PING architecture regulates the exchange of information between the federal government's systems and their interactions with

- Citizens
- State and Municipal levels of government
- Other Federal branches and the Federal Public Attorney's Office
- International agencies
- Foreign governments
- Businesses (Brazilian and foreign)
- Third Sector institutions.

The following illustration maps out these relationships.

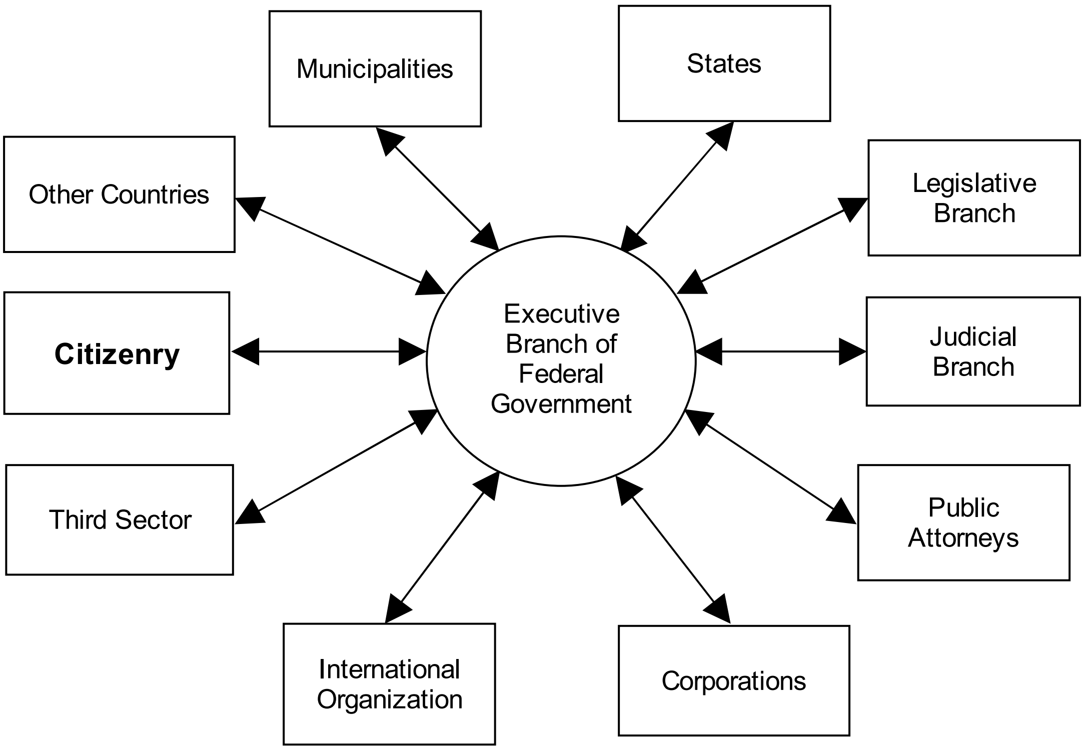

Figure 1 – Federal Government Relations

2.1. Adhesion to e-PING

The adoption of the e-PING standards and policies cannot be imposed on the citizens and the other government instances within and outside the country. Nevertheless, the Brazilian government has established its chosen specifications, which it will use as standards to interoperate with the entities not belonging to the Executive Branch of the Brazilian Federal Government. These entities may subscribe on a volunteer basis without any constraints on the part of the e-PING Coordination.

For the Executive Branch units of government the adoption of the e-PING standards and policies is mandatory.

The Executive Branch of the Brazilian Federal Government includes

- The units of Direct Administration: Ministries, Secretariats and other of same legal nature, directly or indirectly linked to the Presidency of the Republic.
- The Autarchies and Foundations.

Within the jurisdiction of the above-mentioned entities, the e-PING specifications are mandatory for:

- All new information systems that are implemented within the government and society interaction scope.
- The legated information systems that are the object of implementations involving the provision of electronic government services or the interaction among systems.
- Other systems that purport to provide electronic government services.

Subscribing to e-PING will happen in a gradual way, according to an implementation plan that will consider the situation of each one of the applicants concerning their likelihood to adapt to the e-PING specifications and recommendations.

For the government information systems that are out outside the scope of mandatory enforcement, it is advisable that their managers consider adapting them to the e-PING standards whenever significant updates are made.

All government purchasing and recruiting for the development of electronic government services and the updating of extant systems must comply with the present specifications and policies.

The e-PING welcomes the cooperation of all interested parties in the development and continuous updating of its specifications and recommendations. The e-PING management holds its Internet site (http://www.eping.e.gov.br) as preferential means of contact between its operators and the society.

2.2. Focus on Interoperability

The e-PING will not encompass all ICT subjects, and will only cover those specifications that are relevant to guaranteeing system interconnectivity, data integration, access to electronic government services and content management as they are dealt with in the segments presented in section 4 of the present document.

2.3. Subjects not approached

The e-PING does not purport to standardize the form of presentation of the information provided by the electronic government services, and limits itself to defining the requirements for data exchange and availability through the access devices.

3. Overall policies

Each one of the e-PING segments contains a set of technical policies to direct the establishment of specifications for their components. The specific sets of each segment were built according to the following general policies:

Alignment with the INTERNET: all government information systems should comply with the main specifications used in the Internet and by the World Wide Web.

Adoption of XML as the main standard of data exchange for all public sector systems.

Adoption of navigators (browsers) as the principal means of access: all government information systems should be accessible preferentially through browser technology. Other interfaces are permitted for specific purposes such as updating and data reception routines for which there is no navigator based technology available.

Adoption of metadata for handling government information resources.

Development and adoption of Standardized Metadata for Electronic Government (e-PMG) based on internationally accepted standards (see http://www.eping.e.gov.br).

Development and maintenance of a List of Government Subject Matters - Navigation Taxonomy (LAG) that presents in directory format all of the topics related to government operations (see http://www.eping.e.gov.br).

Market support - All e-PING specifications contemplate solutions that have market support. The objective is to cut costs and risks in the conception and delivery of services by the government information systems.

Scalability - The selected specifications should be able to respond to system demand fluctuations such as changes in data loads, and frequency of transactions and users. The established standards cannot be restrictive factors, and should be aid the development of services that fill out most of the demands, from small transaction volumes and number of users, to the nationwide access demands involving great amounts of information and high numbers of users.

Transparency - The e-PING documentation is available to the society in the Internet, and there are mechanisms for dissemination and the reception and evaluation of suggestions. The deadlines and other commitments involving implementation and site management are defined and posted in the Internet (see http://www.eping.e.gov.br).

Preferential adoption of Open Standards - The e-PING defines that whenever possible open standards will be adopted while establishing technical specifications. Proprietor standards are accepted until there are migration conditions. The situations where there is a need to account for information safety and integrity requirements will be dealt with appropriately. When available, free software solutions will be considered preferential, in keeping with the policies defined by the Electronic Government Executive Committee (CEGE).

The e-PING is friendly to ICT solutions such as the Brazilian Government's Directive on Migration to Free Software (see http://www.governoeletronico.gov.br).

Guaranteed privacy of information - All units in charge of delivering e-gov services should take measures to guarantee the privacy of information in regard to citizens, business, and government organizations, and to respect and enforce the legally defined restrictions on access to and dissemination of information.

4. Segmentation

The e-PING architecture was segmented in five parts for the purpose of the definition of standards. For each one of the **segments** was created a work group of specialists from Federal, State and Municipal governments. Those groups were charged with elaborating the present version of the e-PING architecture, which is the groundwork for setting up the Brazilian government's interoperability standards.

The five segments, namely "Interconnection", "Safety", "Means of Access"", "Organization and Interchange of Information" and "Areas of Integration for Electronic Government" were subdivided into **components**, for which were established the technical policies and specifications to be adopted by the federal government. The components of each one of the five segments are presented below.

4.1. Interconnection

This segment establishes the conditions under which the government units will interconnect, and the interoperability conditions between the government and the society.

It contains the specifications for

- Hypertext Transfer Protocol
- Transfer of Electronic Messages
- Content Safety of Electronic Messages
- Access to mailbox
- Safe access to mailbox
- Directories
- Domain Nomination Services
- Mail Addresses
- File Transfer Protocol
- Intercommunications LAN / WAN
- Transfers
- Web Services SOAP, UDDI, and WAD.

4.2. Safety

This segment covers the ICT safety aspects to be considered by the federal government, including the standards for

- IP safety
- Electronic mail safety
- Cryptography
- Systems development
- Net services
- Collection and filing of evidences.

4.3. Means of Access

This segment deals with the standards that apply to the means of access to electronic government services. The present version approaches exclusively the policies and specifications for workstations, smart cards, tokens and other cards. In future versions other access means will be treated such as cellular telephones, handhelds, and digital televisions. The following two subgroups of components are covered:

Standards for access through work stations

- Navigators (browsers)
- Character and Alphabet sets

- Navigators (browsers)
- Character and Alphabet sets
- Hypertext Exchange Format
- Document Type Files
- Chart Type Files
- Presentation Type Files
- Data Bank Type Files for Work Stations
- Specifications for the Exchange of Graphic Information and Static Images
- Vector graphs
- Specifications for Animation Standards
- Audio and Video Type Files
- Compacting General Use Files
- Files for Geo-referral.

Smart Cards / Tokens / Other Devices

- Data definition
- Applications (including multi-applications)
- Electric components
- Communications protocols
- Physical interface standards
- Safety
- Data terminal infrastructure.

4.4. Organization and Exchange of information

This segment covers the aspects related to the treatment and transfer of information in electronic government services. It includes the standards for government subject matters and metadata, and encompasses the following components:

- Data exchange language
- Data transformation language
- Definition of data to be exchanged
- Catalog of Data Standards (CPD)
- List of Government Subject Matters - Navigation Taxonomy (LAG)
- Standardized Metadata for Electronic Government (e-PMG).

4.5. Areas of Integration for Electronic Government

The analysis and proposition goals of this segment are

- XML Schemas of applications related to the Areas of Government Performance that are displayed as a Catalog in the e-PING site whose current contents are presented in a latter topic.
- Components related to issues that cut across the Areas of Government Performance whose standardization is relevant for the interoperability of Electronic Government services such as geographical processes and information.

5. Administration of the e-PING

This item deals with the administration of the e-PING architecture. It specifies the form by which the Brazilian government intends to consolidate the implementation of the policies and technical specifications as standards effectively adopted, both internally by the Federal Public Administration units, and in their interactions with external entities such as other government instances, private sector and third sector institutions, and the citizenry.

5.1. Background

The e-PING architecture has the purpose of being the interoperability paradigm for the federal government, initially within the Executive Branch. The initiative of assembling this architecture fell to three federal agencies, namely

- The Ministry of Planning, Budget, and Administration's Secretariat of Logistics and Information Technology (SLTI / MP).
- The National Institute for Information Technology of the Presidency of the Republic (IT / PR).
- The Federal Data Processing Service (SERPRO), a public company attached to the Treasury Department.

These agencies organized a Seminar involving several federal government entities, during which they created an interdepartmental steering committee to drive the initial work of assembling the e-PING architecture.

After being formalized by Normative Act no. 5, of July 14, 2005, this committee became the e-PING Coordination. Besides the three original organizers, also take part in this group the public entities DATAPREV, Bank of Brazil, Federal Savings bank, DATASUS, and ABEP (Brazilian Association of State Owned Data Processing Agencies).

The Committee established the following work program:

- Definition in the initial format for elaboration and administration of the e-PING architecture.
- Definition of the segmentation of the subjects to be covered by the e-PING.
- Creation of five work groups responsible for the initial definitions of policies and technical specifications for each one of the segments.
- Establishment of a timetable for the construction and popularization of the initial version (version 0) of the e-PING architecture.
- Extensive consultations and public audiences in five Brazilian States (RS, SP, DF, RJ, MG, and PE) to collect contributions of the society in general on the content proposed in the version 0.
- Release of version 1.0 together with the institutionalization of the e-PING as part of the Federal Public Administration.
- Release of version 1.5 containing the update and review of the technical specifications and general overview of the e-PING. (Versions 1.1 up to 1.4 were discussed internally by the work groups and the e-PING coordination staff.)
- Consultations and public audiences to collect contributions of the society in general on the content proposed in version 1.9.
- Release of version 2.0 containing the update and review of the technical specifications, and the comprehensive overview of the e-PING.

Similar experiences by governments of other countries are researched on a regular basis. The British government’s e-GIF (Government Interoperability Framework) was adopted for the construction of the Brazilian government's e-PING architecture. The e-PING administration replicates the format adopted by the UK government in the year 2000, which has achieved great maturity and is internationally recognized as a reference.

5.2. Implementation strategy

The popularization of the standards and specifications established by the Brazilian government will be done through versions. The elaboration of an annual version is foreseen, with intermediate publication of updates whenever significant changes are made.

The present version consolidates the work of the five segment task groups. Its whole content was made available for public consultation to obtain contributions to the proposals of standards released in version 1.9.

5.3. Managerial model

This item specifies the ways in which the e-PING architecture will be managed, and lists the main attributions and the mode of implementation of those activities within the government's organizational structure.

5.3.1. Attributions

The administration of the e-PING covers managerial and technical attributions.
The following **managerial attributions** stand out:

- To define the strategic and government administration objectives for the establishment of the standards.
- To administer the Brazilian government's interoperability architecture by providing the necessary managerial infrastructure for its correct use and guaranteeing its update, considering the government's priorities and goals, the needs of the society and the readiness of new technologies that are tested and approved by the ICT market .
- To act as the coordination center of the e-PING architecture, overseeing the alignment among the interoperability efforts and assuring the coherence of the initiatives undertaken by all government organs.
- Specifically for the segments of interoperability, to handle the federal government's relationship with the other instances as defined in item 2 of the Scope section.
- To manage and operationalize the popularization of the e-PING standards, considering the
  - Creation and administration of the Internet e-PING site (see http://www.eping.e.gov.br).
  - Coordination of the public consultations process.
  - Coordination of the process of reception and evaluation of change and amendment proposals.
  - Coordination of the e-PING suggestion seeking process.
  - Release of the final and intermediate versions of e-PING updates.
- To manage the interaction with same purpose initiatives by other governmental entities in the country and abroad.
- To promote the training of Federal government staffs by acting upon the public agencies to have them include the e-PING in their house training programs through corporate events aimed at disseminating the e-PING standards.
- To establish, to implant, and to publish performance indicators of the e-PING implementation work.
- To manage the interaction with technical standards organisms (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, as well as norms institutes such as ABNT, INMETRO, ISO, NIST, etc.). These organisms as well as others are chosen by the e-PING coordination based on their international reputation, competence in the respective areas of performance and friendliness to open standards.
- To manage the interaction with national and international fomenting agencies to channel resources to assist the creation of the e-PING infrastructure and to promote research and development.
- To make possible the implementation and approval of the standards to be established for the government.
- To make possible the implementation and to manage the auditing processes for verifying the level of compliance with the e-PING recommendations and specifications.
- To act cooperatively in support of the government organs to accomplish their necessary adaptation to the e-PING standards and to evaluate the possibility of sponsoring comprehensive programs to promote the intensive use of the proposed standards.

Among the **technical attributions** stand out:

- To establish the protocols for the elaboration and maintenance of the policies and technical specifications which compose the e-PING by means of the
    - Identification, creation, and administration of specific work groups.
    - Establishment of agreements and definitions of government institutions that will be responsible for the policies and technical specifications of each component of the interoperability segments.
    - Identification and implementation of alternate ways of handling the technical subjects within the scope of the e-PING.

- To coordinate the development and maintenance within the federal government of
    - Standardized Metadata for Electronic Government (e-PMG).
    - List of Government Subject Matters - Navigation Taxonomy (LAG).
    - Catalog of Data Standards (CPD).
    - Reference Catalog of XML Schemas.
    - Other standards for the organization and exchange of information.
    - Interconnection standards.
    - Safety standards.
    - Standards for means of access to government electronic services.
    - Standards for the use of smart cards, tokens and other cards.
- To guarantee the unified conception, conceptual and definitional framework, and establishment of standards by those in charge of the technical segments of the e-PING.

5.3.2. Responsibilities

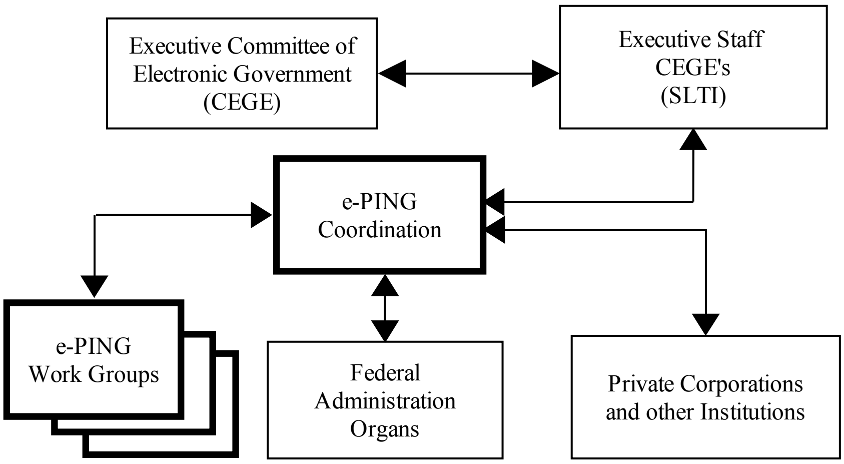
Executive Committee of Electronic Government (CEGE)
Executive Staff CEGE's (SLTI)
e-PING Coordination
e-PING Work Groups
Federal Administration Organs
Private Corporations and other Institutions

Figure 2 – e-PING Administration

The e-PING administrative structure is presented in the following chart.

The Secretariat for Logistics and Information Technology of the Ministry of Planning, Budget, and Administration is the operating arm of the Information and Computer Science Resources Management System (SISP), which was created by Decree no. 1048 on January 21, 1994 to oversee the institutionalization of the e-PING and to define the legal format of its Coordination.

The e-PING Coordination's performance will abide by the following guidelines:

- Implementation of the e-PING architecture through the necessary actions to consolidate the current version and oversee the dynamics of its evolution.
- Administration of the e-PING architecture.
- Establishment and management of the norms and institutional/legal instruments that guarantee the effectiveness of the e-PING recommendations and specifications.
- Administration of the e-PING standards.

- Warranty of maintenance of the updated e-PING catalogs.
- Dissemination and popularization of the e-PING standards, decisions, and activities including the publication of new versions and intermediate updates.
- Creation of an e-PING stamp and administration of e-PING compliance certification of services or products.
- Supply of criteria and subsidies for the preparation of the Federal Government's Annual Budget Law.
- Procurement and agreement management for the consolidation of the e-PING standards, including the evaluation of e-gov project proposals within the Federal Public Administration (APF), the approval of standards, and conformity verification.
- Establishment of the contact points with the several organs of APF.
- Work group management by defining their composition and determining their operating guidelines based on the general and specific technical policies, the needs of government, and the results of technological scenario monitoring.

The e-PING work groups gather together suitable representatives from the units of the Federal Public Administration and representatives from institutions of other governmental spheres, and they are responsible for

- Dealing with the subject matters included in the e-PING segments.
- Monitoring the technology market systematically with a focus on the segments under its responsibility to detect the need for technological updating of the policies and technical specifications.
- To give support to the e-PING Coordination in the performance of its administrative and technical attributions.

The work group coordinators will share in the e-PING management.

5.4. Additional activities

In addition to its managerial and technical attributions for the implementation and up keeping of the e-PING architecture, the e-PING Coordination will be in charge of other activities, as follows.

5.4.1. Selection and Approval of Technological Standards

The present technical policies are the basis for setting the e-PING standards and provide the rationale for the selection of the technical specifications of the e-PING components.

A new standard may be added to the e-PING architecture through a process of analysis that includes the selection, approval, and classification of the selected specifications in one of five possible situations according to its compliance with the general and specific technical policies of each segment:

- **Adopted (A)**: the item passed through formal review by a government specialist body or an accredited institution with formal delegation to accomplish the required analyses. Alternately, the item was proposed by one or more the segment coordinators, posted in the Internet site, and approved by the e-PING Coordination.
- **Recommended (R)**: the item complies with the e-PING technical policies, is recognized as an item that should be used by the government, but has not been submitted to a formal process of approval.
- **In Transition (T)**: the item is not recommended because it does not comply with one or more of the requirements as set up in the general and technical policies of the architecture. It is included in the e-PING because of its wide use in government institutions, but will be replaced by some other component that presents adequate conditions. It may become a "recommended" component in case it complies with all of the established technical policies. It should be pointed out that the development of new services or the reconstruction of significant parts already extant should avoid the use of components classified as transitory.
- **Under Evaluation (E)**: the component is undergoing evaluation and will be classified in one of the above situations, as soon as the evaluation process is completed.

- **Future Consideration (F)**: the component was not yet appraised and will be submitted to further study.

The responsibility for the selection of the e-PING components and their classification in one of the above situations falls on the specialist work groups made up of government professionals and experts from partner institutions.

The starting point of the selection process may be formal proposals, demands from government units, and/or research done by the work groups.

The final approval of an item requires thorough consideration by the e-PING coordination staff. Given the great variety of possible components, it is necessary to set up a system that covers from the review of the physical aspects of certain components such as smart cards, to others that require studying the component's application in the development and delivery of services related to the organization and exchange of information and safety.

That being the case, the government should enter agreements with specialized institutions or accredit them to elaborate the conformity tests, while defining which components should be submitted to approval processes, which are the criteria of evaluation of the results and which are the conditions for the accomplishment of the procedures.

The complete definition of the selection and approval process will take into account the specifics of each segment, under the responsibility of the e-PING Coordination.

5.4.2. Conformity Auditing

It is critical for the successful implementation and consolidation of the e-PING that the government units comply with the specifications and recommendations. The e-PING managers will recommend auditing procedures to verify whether the public service abides by the specifications and policies.

There may be delegation of responsibility for that purpose to especially assigned teams of government specialists who are experienced in conducting such procedures.

The preferred way to accomplish those kinds of procedures, however, is to use the extant structures for systems auditing. The e-PING Coordination will be responsible for suggesting the basic criteria that they will use.

The cooperation of government organs active in the area is desirable, and measures are being taken to involve other branches and spheres of government.

5.4.3. Creation and Maintenance of the Internet Site

The whole process of exchange of information between the e-PING staff with the users, collaborators, and other interested parties will be accomplished preferentially by the Internet through the address http://www.eping.e.gov.br . When fully operational the e-PING site will have as its main functionalities:

- Complete dissemination of its documentation - official versions and respective updates, beta versions for public consultations, technical support documentation, and legal / institutional documentation correlates.
- Availability to the public of the recommendations, determinations, and technical and political specifications for validation, approval, and reception of comments and suggestions.
- Publicity of requests for comments on the specifications of components;
- Availability of electronic means for the reception of suggestions.
- Availability of links for documents, standards, norms or any other type of permanent e-PING reference.

5.4.4. Legal and Institutional Support

The e-PING will have the permanent support of the Ministry of Planning legal affairs division to guarantee that the e-PING documents comply with the legal requirements.

This division will have the additional responsibility of ensuring that the e-PING is fully consistent with the Brazilian legal framework as it relates to ICT.

The e-PING Coordination may seek the cooperation of one or more government organs that are in a condition to supply legal support.

5.4.5. Dissemination

Total publicity will be given the whole content of the e-PING. The major means of popularization besides the Internet site are:

- Special dissemination events such as seminars, workshops, and presentations;
- Participation in government events in the ICT area and correlate subjects.
- Participation in events addressed to specific publics.
- Release of all e-PING versions and their intermediate updates;
- Interchange with other spheres and branches of government, public institutions, private and third sector organizations, and foreign governments.

5.4.6. Capacity building

The e-PING implementation and administration calendar will provide for capacity building events, including the intensive use of Internet-based instruction.

The e-PING Coordination will prepare and publish a minimum training grid that each public organ may use to estimate its own necessary investments in staff training to adapt to the e-PING recommendations.

Each government organ should abide by the e-PING standards in setting up their training programs to provide appropriate training to their technical teams.

5.5. Relationship with the Government and the Society

This section disposes on the relationships between the e-PING and the government and society entities.

5.5.1. Federal Government Organizations (Executive Branch)

The participation of all the public service echelons, government agencies, regulatory agencies, public companies and other governmental institutions is essential for the promotion and consolidation of interoperability in the public sector.

Although the general guidelines are managed by the e-PING Coordination, each institution will have its share of responsibility in the administration and enforcement of the e-PING standards. Their attributions in this regard are as follows.

- To contribute to the development and continuous improvement of the e-PING.
- To guarantee that their organizational ICT strategies promote the conversion of their extant systems of electronic government to the e-PING recommendations.
- To have a plan for the implementation and adaptation of their ICT infrastructure to the e-PING architecture.
- To ensure that their staffs have the necessary abilities to define and use the mandatory interoperability specifications and to provide them training support as needed.
- To establish contact points in the institutions for exchange of information and demands with the e-PING Coordination.
- To allocate and supply resources to give support to adaptation to the e-PING.
- To take advantage of the opportunities to rationalize processes deriving from the increase in interoperability to improve the quality and reduce the cost of delivering e-gov services.

5.5.2. Other Governmental Instances (other Federal Branches, and State and Municipal Governments)

In its present stage, the e-PING is meant for the Executive Branch of the Federal Government. Other branches and other spheres of government (States and Municipalities) will be considered as external entities.

It should be kept in mind that the federal government does not determine how the other entities of the society should act, it only specifies the preferential ways in which it intends to interoperate with those entities.

The subscription of other governmental instances is welcome, as it is considered a good strategy to improve the e-PING standards and to consolidate the e-PING architecture as the foremost Brazilian government's interoperability tool.

The e-PING management assigns top priority to the other Federal branches and to the State and Municipal governments and this goal will be pursued as soon as the e-PING standards are firmly established within the Federal Executive Branch through the involvement of the agencies and institutions in the e-PING implementation process.

5.5.3. Private and Third Sector Organizations

The e-PING foresees the interaction with the private and third sectors through the mechanisms of public consultation, requests for comments and reception of suggestions.

All such entities that engage in product and service supply auctions for the Federal Executive Branch should comply with the e-PING specifications and recommendations.

Other forms of participation of these sectors in the e-PING may be considered, and norms will be set down to guarantee transparency to the decisions and equal opportunities.

5.5.4. Citizenry

Electronic government essentially means that the government will deliver better services to the citizens through ICT resources. The e-PING architecture provides for the integration of those services and makes them available in a complete, secure, and consistent way, and enables the government to reach better efficiency levels.

The government should motivate the society to speak up, to comment on, and to contribute suggestions of innovations for improving access to information and service delivery. All of the e-PING popularization and interaction procedures count on the active participation of the citizens and the society in building and managing the architecture.

Part II. Technical Specification of the e-PING Components

6. Interconnection

6.1. Interconnection: Technical policies

The technical policies for interconnection are as follows.

6.1.1. The APF organs will interconnect by use of IPv4, and plan for future migration to IPv6. New network additions and updates should foresee support to the coexistence of protocols IPv4 and IPv6 and to products that support both protocols.

6.1.2. The e-mail systems should use SMTP / MIME for the transport of messages. The access to messages should use the protocols POP3 and/or IMAP. The use of Web interfaces for electronic mail is encouraged, and the necessary security aspects should be observed.

6.1.3. The APF organs should use directory frameworks that are compatible with the Federal Government's Directory Service as available in the electronic address http://www.e.gov.br/correios/dir_redegoverno.htm .

6.1.4. The APF organs should obey the policies for domain nomination as established by Resolution no. 7 of the Chief of Staff Office (*Casa Civil*). (See: https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES0702web.htm).

6.1.5. DNS should be used for the resolution of Internet domain names by converting them into IP addresses and conversely converting IPs into domain names through direct and reverse maps respectively.

6.1.6. The protocols FTP and/or HTTP should be used for file transport, and their functionalities for interruption and security recovery should be kept in mind if necessary. The HTTP should be prioritized for file transport from Internet sites.

6.1.7. Whenever possible[1] Web-based technology should be used for applications developed through terminal emulation.

6.1.8. Web Services technology is recommended as the e-PING interoperability standard.

6.1.9. The Web Services should be registered and located in UDDI compatible directory structures. The access protocol to those structures should be the HTTP.

6.1.10. The SOAP protocol is recommended for the communications between the customers and the Web Services, and the specifications should use the WSDL language (see note on Web Services in item 6.3.).

[1] There are certain products that provide browser access to legate systems with no need to modify such systems. Those products may typically provide direct access to the legate screens, or replace them with graphic interfaces (GUIs). One must pay attention to the implied security risks.

6.2. Interconnection: Technical specifications

Table 1 - Specifications for Interconnectivity[2]

Component	Specifications	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Hypertext transport protocol	Use HTTP/1.1 (RFC 2616) and/or HTTPS (RFC 2660)	**R**
Electronic message transport	Use electronic messaging products that support SMTP/MIME interfaces for message transport. Related RFCs: 2821, 2822, 2045, 2046, 2646, 2047, 2231, 2048, 3023, and 2049.	**R**
Content security of electronic message	S/MIME v3.1 must be used if appropriate for content security of general government messages unless security requirements determine otherwise. Related RFCs: 3852, 2631, 3850, and 3851	**R**
Access to mailbox	Unless security requirements determine otherwise, mail programs that offer access facilities must at least conform to POP3 for remote access to mailbox. Related RFCs: 1939, 1957, and 2449. If additional facilities are needed, and unless security requirements determine otherwise, mail programs that offer advanced facilities of access to mail must conform to IMAP for remote access to mailbox. Related RFCs: 3501, 2342, 2971, 3502, 3503, and 3510.	**R**
Secure access to mailbox	Access to mailbox through non-secure nets must use HTTPS according to secure transport standards. Whenever necessary to use IMAP or POP, it must be done through TLS, according to RFC 2595.	**R**
Directory	Use central directory framework as defined by http://www.e.gov.br/correios/dir_redegoverno.htm . LDAP v3 must be used for general access to directory.	**R**
Domain Naming Services	DNS must be used for Internet domain name resolutions, according to RFC 1035. Brazilian government guidelines for domain naming are found in Resolution no. 7 of the Electronic Government Executive Committee at https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm. Additionally, as decided by the Brazilian Internet Steering Committee domain naming follows directions from the Ministry of Planning, which manages the .gov.br domains. The specifics of other levels of government e.g. State government domains that include the respective abbreviations in their addresses are dealt with at http://registro.br/faq/faq1.html#12.	**R**
Electronic mailbox addresses	Rules for definition of electronic mailbox names must follow the dispositions of "Caixas Postais Individuais-Funcionais no Governo Federal" (Federal Government Personal and Official Mailboxes), available at http://www.e.gov.br/correios/cp_individ.htm.	**R**
File Transport Protocols	FTP with reinitiating and recovery (RFCs 959, and 2228), and HTTP for file transport (RFC 2616)	**R**
Markup Protocols	Use the Session Initiation Protocol (SIP) as defined by RFC 3261 as control protocol of application layer (markup) to create, modify, and terminate sessions involving one or more participants.	**R**
Real Time Messaging	Model and requirements for Instant Messaging and Presence Protocol (IMPP) are defined by RFCs 2778, and 2779.	**R**
Short Messaging Service	Short Messaging Service (SMS) must use SMPP as defined by SMS *Forum* at http://www.smsforum.net.	**R**

[2] RFCs are posted at http://www.ietf.org/rfc.html.

Component	Specifications	Status
LAN/WAN Communications	IPv4 (RFC 791). **Note:** Ipv6 specification presently found as *Draft Standard* RFC 2460.	**R**
Transports	TCP (RFC 793) and UDP (RFC 768) when needed, subject to security limitations.	**R**
Advanced Traffic	When needed, net traffic may be optimized by using MPLS (RFC 3031).	**R**

6.3. Web Services

Web Services software applications identifiable by a URI (Uniform Resource Identifier) whose interfaces and connections are capable of being defined, described and discovered by XML-based artifacts. They additionally support direct integration with other software applications by using as their interoperability standard XML messages encoded in standard Internet application protocols.
The need for integration among a variety of government information systems implemented through disparate technologies, sometimes in a simultaneous way and in real time, implies the adoption of an interoperability standard that will ensure scalability and ease of use.

The Web Services technology is adequate to meet those needs, in addition to being independent in relation to the operational systems and programming languages.

One of their more relevant characteristics relates to their higher level of abstraction as compared to the concept of software components. From a form belonging to a Web page, up to a software component that encodes a complex business rule, all elements can be transformed into Web Services, what renders their use quite flexible.

The use of Web Services contemplates both the document transports between institutions and the requests for execution of remote services.

The XML document structures will be described as XML Schemas for the validation of data types pertaining to business lines.

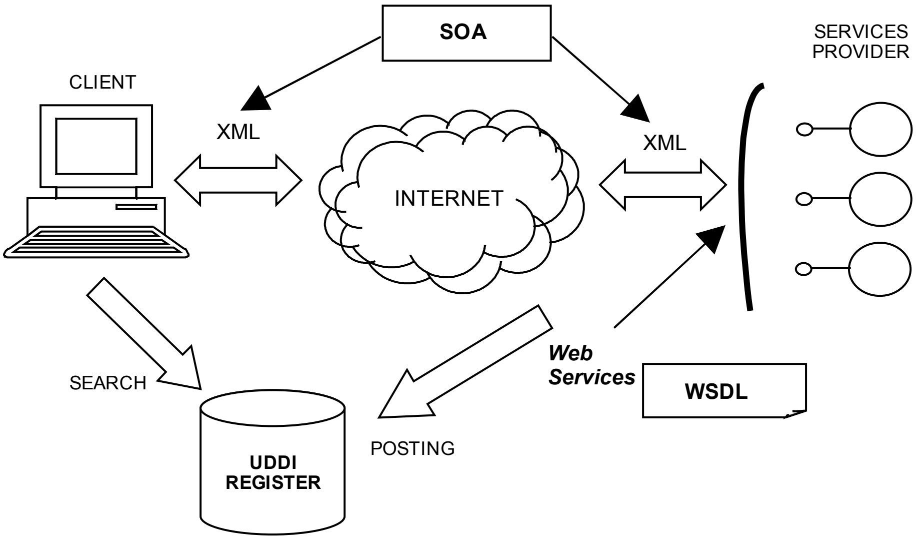

Figure 3 – Overview of Web Services operations

Table 2 - Specifications for Web Services [3]

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Exchange of information protocol	SOAP v1.2 as defined by W3C at http://www.w3.org/TR/soap12-part1/ and http://www.w3.org/TR/soap12-part2/ . SOAP protocol specifications are found at http://www.w3.org/TR/soap12-part0/.	**R**
Registration infrastructure	UDDI v3.0.2 specification *(Universal Description, Discovery, and Integration)* as defined by OASIS at http://uddi.org/pubs/uddi_v3.htm.	**R**
Language for service definition	WSDL 1.1 *(Web Service Description Language)* as defined by W3C. Specification found at http://www.w3.org/TR/wsdl **Note:** WSDL 2.0 specification found as working draft at http://www.w3.org/TR/wsdl20/.	**R**
Basic interoperability profile	*Basic Profile 1.1 Second Edition*, as defined by WS-I at http://www.ws-i.org/Profiles/BasicProfile-1.1.html.	**F**
Remote portlets	WSRP 1.0 (Web Services for Remote Portlets) as defined by OASIS at http://www.oasis-open.org/committees/wsrp.	**E**

6.4. Electronic message (e-mail)

For clarity purpose the e-PING will use the following concepts:

Electronic Message Transport

It is defined as the interface between two mail systems.

Access to Mailbox

The access to a mailbox is defined as the interface between a mail customer and a mail system.

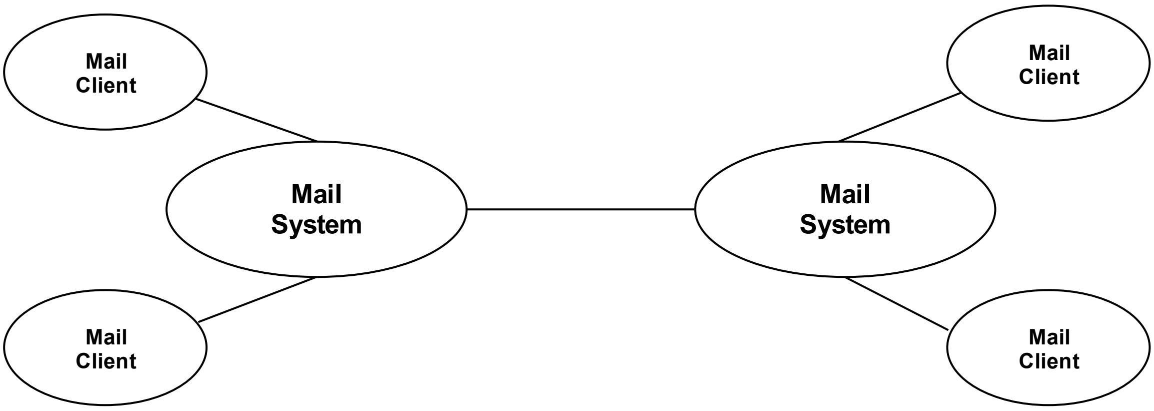

Figure 4 – Mail systems / clients interfaces

[3] Security issues related to Web Services are dealt with in chapter 7.

6.5. Wireless LAN

There is a growing need within the government for mobile computers to allow more flexible work patterns. Wireless LAN solutions based on the pattern series IEEE 802.11 are well accepted by the market. It is recommended to observe the specifications on security, contained in chapter 7 of the present document.

6.6. VPN

Virtual Private Network (VPN), or Virtual Net, is a private net built on the infrastructure of a public net, usually the Internet. Instead of dedicated links or packaged nets to connect with remote nets, the Internet infrastructure is used.

The use of the Internet as connection infrastructure among private net hosts is a good cost solution, but not in privacy terms, because the Internet is a public net where the data traffic may be read by any equipment.

The virtual tunnels enable the traffic of encoded data in the Internet and these devices are capable of understanding the encrypted data, and of superimposing a secure virtual net on the Internet.

The devices for VPN management should ensure the privacy, integrity, and authenticity of the data.

The specifications on VPN will be presented in chapter 7.

6.7. Peer-to-Peer Networks

Peer-to-Peer (P2P) Systems are distributed systems that consist of interconnected nodes capable of self-organizing in network topologies for sharing resources such as processing, storage and bandwidth, can adapt to failures and accommodate transient populations of nodes while maintaining acceptable connectivity and performance without the intermediation or support of a central authority (hub).
Because several security problems still plague the P2P nets their sustained use will be discussed further on.

7. Security

7.1. Security - Technical policies

7.1.1. The data, the information and the government information systems should be protected against threats to reduce risks and to guarantee their integrity, confidentiality, and availability.

7.1.2. The data and information should be maintained at the same protection level, regardless of the media in which they are processed, kept, or transported.

7.1.3. The information going through non-secure nets including wireless LANs should use the appropriate transport layer security controls (IPv4). The security protocols specific to this technology should be used in the special case of wireless LANs whenever necessary. The government information systems should be protected against the security risks involved in connections with those kinds of nets.

7.1.4. The security requirements for the information, the services, and the infrastructure should be identified and treated in accordance to the classes of information, the defined service levels, and the results of the risk analysis.

7.1.5. Security should be treated in preventive ways. Systems that support critical processes should have continuity plans covering the residual risks to ensure minimum levels of operation.

7.1.6. Security is a process that should be present at all of stages of the systems development cycle.

7.1.7. The systems should keep historical records (logs) to allow their auditing and to provide forensic evidence. The adoption of centralized time synchronism systems is indispensable, as well as the use of mechanisms to guarantee the authenticity of the stored registrations, if possible by means of digital signatures.

7.1.8. The XML security services should comply with the W3C specifications.

7.1.9. The use of cryptography and digital certification for the protection of traffic, data storage, access control, and digital and coded signatures should abide by the ICP-Brasil rules.

7.1.10. Documentation on the systems, the security controls, and the environment topologies should be continuously updated and protected.

7.1.11. The users should know their responsibilities for the security and should be qualified for the accomplishment of their tasks and the correct use of the access means.

7.1.12. For the improvement of security the APF organs should refer to the ABNT norm NBR ISO / IEC 17799:2005 - code for information security practices management.

7.2. Security - Technical Specifications

Table 3 - Technical Specifications for IP Security

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Data transport through non-secure nets by the HTTP, LDAP, IMAP, POP3, and Telnet protocols whenever it is possible. Transport layer IPv4 net security.	TLS - *Transport Layer Security,* RFC 2246 at http://www.ietf.org/rfc/rfc2246.txt. If needed, TLS v1 protocol may emulate SSL v3. HTTP over TLS, RFC 2818 at http://www.ietf.org/rfc/rfc2818.txt. It may implement the following cryptographic algorithms: **- Session key exchange algorithms at handshake**: RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA. **- Cipher exchange definition algorithms:** RC4, IDEA, 3DES. **- Hash function for MAC definition**: SHA-1, SHA-256, or SHA-512. **Digital Certificate Type - X.509 v3 - ICP-Brasil**, at http://www.iti.gov.br. **SASL** - *Simple Authentication and Security Layer*, RFC 4422 at http://www.ietf.org/rfc/rfc4422.txt.	**R**
IPv4 Net Security	*IPSec Authentication Header*, RFCs 2402 and 2404 for IP header authentication at http://www.ietf.or/rfc/rfc2402.txt, and http://www.ietf.or/rfc/rfc2404.txt. IKE - *Internet Key Exchange*, RFC 2409 at http://www.ietf.or/rfc/rfc2409.txt must be used whenever needed to negotiate security associations between two entities for the exchange of key material. ESP - *Encapsulating Security Payload*, RFC 2406 at http://www.ietf.or/rfc/rfc2406.txt, requisite for VPN - *Virtual Private Network.*	**R**
IPv4 Net Security for application protocols	S/MIME v3, RFC 2633 at http://www.ietf.or/rfc/rfc2633.txt must be used whenever appropriate for general government message security.	**R**
IPv6 Net Security for net layer	IPv6 as defined by RFC 2460 at http://www.ietf.or/rfc/rfc2460.txt presents native security protocol implementation. IPv6 specifications define two security mechanisms: AH - *Authentication Header*, RFC 2402 at http://www.ietf.or/rfc/rfc2402.txt, and ESP -	**R**
	Encrypted Security Payload, RFC 2406 at http://www.ietf.or/rfc/rfc2406.txt.	
Wireless LAN 802.11 g	Use of WPA - *Wi-Fi Protect Access* with standard 802.11 g specification must be stimulated since the protection offered by the WEP - *Wired Equivalent Privacy* standard presents vulnerabilities.	**R**

Table 4. Technical Specifications for Electronic Mail Security

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Access to mail boxes	Must be done through client of electronic mail software considering the native security facilities of client. If not possible to use the specific client, or if necessary to access mail box through non-secure net such as the Internet, must use HTTPS in accordance to the transport security protocols as described by RFC 2595 that deals with the use of TLS with IMA, POP3, and ACAP, at http://www.ietf.or/rfc/rfc2595.txt.	**R**
E-mail content	S/MIME v3 must be used whenever appropriate for general government message security. This includes RFC 3369 at http://www.ietf.or/rfc/rfc3369.txt, RFC 3370 at http://www.ietf.or/rfc/rfc3370.txt, RFC 2631 at http://www.ietf.or/rfc/rfc2631.txt, RFC 3850 http://www.ietf.or/rfc/rfc3850.txt, and RFC 3851 at http://www.ietf.or/rfc/rfc3851.txt.	**R**
E-mail transport	Reverse check HELO name to guarantee message origin and to minimize SPAM.	**F** [4]
Signature	Use ICP-Brasil standard for e-mail signature if required in conformity with Decree no. 3.996 of 10/31/2001.	**R**

Table 5 - Technical Specifications for Security - Cryptography

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Ciphering algorithm	3DES, AES	
Signature algorithm	SHA-1, SHA-256, or SHA-512 with RSA, and SHA-1, SHA-256, or SHA-512 with DSA. **Note**: Systems must support hashing algorithm MD5 with RSA to guarantee compatibility with previous implementations.	**R**
Hashing algorithm	SHA-1, SHA-256, or SHA-512. **Note**: Systems must support hashing algorithm MD5 to guarantee compatibility with previous implementations.	**R**
Algorithm for content/session code key transport	RSA	**R**
Elliptic-curve-based encoding algorithms	ECMQV and ECDH for key agreement, ECDSA for digital signatures, and ECIES for encoding and safe transport of cryptographic keys. Use of these algorithms is subject to regulations and norms by ICP-Brasil in regard to security requirements	**E**
Security requisites for encoding modules	FIPS 140-2 - Minimum requisites for storage solutions regarding private keys and digital certificates issued by ICP-Brasil that use both software and hardware devices such as tokens and smart cards. Compliance is achieved if a) Level 1 or 2 secure standard rules are obeyed.	**R**

[4] Possible performance implications; possible discharge of valid messages; impossible to deal with multiple domains.

Component	Specification	Status
	b) FIPS 140-1 or 2 secure standard rules for level 2 are at least followed for hardware violation checks (*Tamper Evidence*).	

Table 6 - Technical Specifications for Security - System Development

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

XML signatures	XML syntax and signature processing (XMLsig) as defined by W3C at http://www.w3.org/TR/xmldsig-core/.	**R**
XML ciphering	XML syntax and cipher processing (XMLenc) as defined by W3C at http://www.w3.org/TR/xmlenc-core/.	**R**
XML signature and ciphering	Decoding transformation for XML signature as defined by W3C at http://www.w3.org/TR/xmlen-decrypt.	**R**
XML general management when using PKI environments	XML - Key Management Specification (XKMS 2.0) as defined by W3C at http://www.w3.org/TR/xkms2/	**R**
XML access authentication and permit	SAML as defined by OASIS when using an ICP environment, at http://www.oasis-open.org/committees/security/index.shtml.	**R**
Intermediation and federation of identities	WS-Security 1.1 standards framework to guarantee the integrity and confidentiality of SOAP messages, at http://www.docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security/1.0.pdf. WS-Trust 1.3 extensions for WS-Security standards that define the use of security credentials and distributed trust management, at http://www.docs.oasis-open.org/ws-sx/ws-trust-200512. **Note**: Previous component (SAML) may join the present component after review is completed.	**E**
Navigators	Use connection witnesses of a permanent nature (*cookies*) only by user's agreement as per Resolution no. 7 of the Electronic Government Executive Committee (Chapter II, article 7).	**A**

Table 7 - Technical Specifications for Security - Net Services

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Directories	Normative Act no. 2 of 10/3/2002 published in the Official Federal Journal on 10/4/2002, section 1, page 85. LDAPv3 (RFC 2251) at http://www.ietf.or/rfc/rfc2251.txt. LDAPv3 extension for TLS (RFC 2830) at http://www.ietf.or/rfc/rfc2830.txt	**R**
DNS	Resolution no. 7 of the Electronic Government Executive Committee “Práticas de Segurança para Administradores de Redes Internet” (Security Practices for Internet-based Net Administrators) NIC BR Security Office at http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-chklist.pdf. Version 1.2 of May 16, 2003 Securing an Internet name server, CERT - August, 2002.	**R**
Secure file transfer	FTP (RFC 959) at http://www.ietf.or/rfc/rfc959.txt, and RFC 2228 at http://www.ietf.or/rfc/rfc2228.txt.	**R**

Component	Specification	Status
	HTTPS (RFC 2818) at http://www.ietf.or/rfc/rfc2818.txt. **Note**: SFTP - *Secure File Transfer Protocol* is currently in drafting, and will be dealt with in the future. See: http://www.ietf.org/internet-drafts/draft-ietf-secsh-scp-sftp-ssh-uri-04.txt	
Newsgroup		**F**
Instant messaging	RF2778 at http://www.ietf.or/rfc/rfc2778.txt, RFC 3261 at http://www.ietf.or/rfc/rfc3261.txt, RFC 3262 at http://www.ietf.or/rfc/rfc3262.txt, RFC 3263 at http://www.ietf.or/rfc/rfc3263.txt, RFC 3264 at http://www.ietf.or/rfc/rfc3264.txt, and RFC 3265 at http://www.ietf.or/rfc/rfc3265.txt.	**E**
Time synchronism	RFC 1305 IETF - *Network Time Protocol* - NTP version 3.0 at http://www.ietf.or/rfc/rfc1305.txt. RFC 2030 IETF - *Simple Network Time Protocol* - SNTP version 4.0 at http://www.ietf.or/rfc/rfc2030.txt.	**R**
Time stamping	RFC 3628 TSAs - Policy Requirements for Time-Stamping Authorities at http://www.ietf.or/rfc/rfc3628.txt, *Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) at http://www.ietf.or/rfc/rfc3161.txt. **Note**: The time-stamping service must abide by the resolutions and other norms issued by ICP-Brasil.	**R**

Table 8 - Technical Specifications for Security - Collection and Filing of Evidences

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Records preservation	*Guidelines for Evidence Collection and Archiving*, RFC 3227 at http://www.ietf.or/rfc/rfc3227.txt.	**E**
Incident response	*Expectations for Computer Security Incident Response*, RFC 2350 at http://www.ietf.or/rfc/rfc2350.txt.	**E**

8. Means of Access

8.1. Means of Access: Technical policies

The technical policies on access to the federal government's electronic services for citizens, other governmental spheres, other branches of government, public servants, private companies and other institutions are as follows.

8.1.1. The government information systems should be projected to comply with the Brazilian legislation, and be accessible to the bearers of special needs, minority ethnic groups and those under risk of social or digital exclusion. The delivery of services across the counter should be maintained to extend the benefit of electronic government services to the population without direct access through electronic devices.

8.1.2. The government information systems that supply electronic services should abide by the following guidelines.

- When using the Internet as a means of communications and workstations as access devices they shall be preferentially projected to supply access to the information by the use of Web technologies and communications protocols based on navigators (browsers).
- When using other access devices such as cellular telephones, digital television and smart cards, they may other interfaces besides the Web navigators.
- They should be projected to supply electronic government services through different means of access.
- They should foresee the gradual substitution of the "login / password" system for users' authentication by digital certificates, preferentially through smart cards or tokens, as recommended by ICP-Brasil (see http://www.icpbrasil.gov.br/).
- New services to be created should support users' authentication through digital ICP-Brasil certificates.
- The present version of the e-PING disposes on the following means of access:
    - Work stations that provide users with direct or indirect means of access through over the counter services; and
    - Smart cards, tokens, and other cards.
    - Other means of access such as cellular telephones, handhelds, and digital television will be the object of future study to determine their compliance with federal government approved standards.

8.1.3. Government information systems that are built to support a given access device should comply with the e-PING specifications for such device.

8.1.4. Any government information system that supplies electronic services should be capable of using the Internet as its means of communications, either directly or through third-party services.

8.1.5. The development of government electronic services should provide services to the users who do not have the access to the most recently available technologies. On the other hand, they should consider the need to attend to the bearers of special needs, including the provision of more sophisticated, and user-specific resources. The recommendations contained in the Model of Accessibility of Electronic Government (e-MAG) [5] should be observed in that regard.

8.1.6. Whenever using the Internet for communications the government information systems should be projected so that the maximum information can be obtained through navigators that conform to the minimum standards called for by support of the pertinent technical specifications as stated in section 8.2. Additionally, the e-PING recommends that each electronic government service clearly specify, preferably in its home page, the minimum navigator versions that support the functionalities requested by the associated service.

[5] BRASIL. Ministério do Planejamento, Orçamento e Gestão. Recomendações de Acessibilidade para a construção e adaptação de conteúdos do Governo Brasileiro na Internet: modelo de acessibilidade. Versão 2.0. Brasília, 2005. Available at http://www.governoeletronico.gov.br/emag/.

Compliance with the minimum requirements should allow exceptions to cover the security issues involved in the treatment of information.

8.1.7. Whenever the Internet is used for communications middlewares, or additional plugging may be used if there is no alternate technical way to optimize the navigator's functionality on the workstations. In this case, additional software should be offered free, subject to all of the e-PING technical specifications. It should be also made available in safe repository maintained by the government organ in charge of the application.

8.1.8. Electronic government services should be projected to guarantee content authenticity to the users through digital certificates as recommended by ICP-Brasil (see: http://www.icpbrasil.gov.br/). For that purpose, all of the Web sites should use "https" instead of "http".

8.1.9. The needs of the society together with the government's ability to develop and deliver electronic services will be the bases for the definition of the technical specifications demanded by the available access means. Techniques of content administration and technologies that make possible the adaptation of the devices to support electronic government services shall be used to facilitate the access through the minimum Web navigator standards, as established in item 3 of the General Policies, to enable the use of public stands, service counters, and Citizen Service Centers such as call centers.

8.1.10. The Federal government information systems should foresee, whenever needed, and technically and economically viable, the construction of adapters that allow the Web access to the electronic services information through a plurality of environments at acceptable answer times and reduced cost.

These adapters may be used to speedily filter, convert, and reformat the Web contents to adapt to the display requirements and capabilities of the access devices. They may still make possible the modification of a Web page content through XML and XSL data protocols, user's preferences and net and access device parameters.

These adapters shall also allow their use as alternate ways to make the access possible to the ethnic minorities, to the bearers of visual deficiency for instance, by using text translators, bigger fonts and graphs, audio resources, etc. Such aspects are covered by Resolution 7 of the Electronic Government Executive Committee. (See: https://www.planalto.gov.br/ccivil_03/Resolução/2002/ RES0702web.htm.)

8.1.11. The file types that have XML as their packaging standard will be considered preferential to facilitate the interoperability among electronic government services.

8.1.12. Electronic government services that make documents available to their users should do so by attaching clearly stated information to their own access link to the documents as to their providers, version status, publication date, and format. Publication date means the calendar date the document was published by the official records journal, in case this is legally required, or the date of posting in the site for all other cases. Other information on the document, such as author, editor, issuer, topical data, or other relevant identifiers should be supplied in the "properties" field of each document.

8.2. Means of Access: Technical specifications for work stations

The rough drafts of documents or working paper that need collaborative creation should use the formats presented in Table 8.1.

The final versions of documents to be sent out or digitally filed should use the pdf/a format recommended. Documents that must warrant their integrity and/or authorship, in addition to the pdf/a format, should be digitally signed by their authors by use of the ICP-Brasil certificate.

By mentioning market solutions that generate the file formats mentioned in Table 8.1, the e-PING solely purports to identify **minimum references** for information exchange through e-gov services. Files may be received or sent on the **present or updated versions** of those that are mentioned therein.

Table 9 - Technical Specifications - Work Stations

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Navigators (browsers)	See: Overall Policies item 3	E
Characters and alphabets sets	UNICODE standard version 4.0, latin-1, UTF8, ISBN 0-321-18578-1	R
Hypertext exchange format	HTML version 4.01. (.html)[6] as per W3C specifications	R
	XHTML versions 1.0 or 1.1 (.xhtml) as per W3C specifications[7]	R
	XML versions 1.0 or 1.1 (.xml) as per W3C specifications[8]	R
	SHTML (.shtml).	R
	MHTML (.mhtl or .mht)[9]	T
Document type files	XML versions 1.0 or 1.1 (.xml) or XSL format (optional) as per W3C specifications[10]	R
	Open Document (.odt) as per ISO/IEC standard 26300[11]	R
	OpenOffice.org XML (.sxw) as per OpenOffice version 1.0 format.	T
	Rich Text Format (.rtf).	R
	PDF (.pdf) as per versions up 1.3.	T
	PDF open version PDF/A[12]	R
	Plain text (.txt)	R
	HTML version 4.01 (.html or .htm) as per W3C specifications	R
	Microsoft Word document (.doc) as per MS Office up to version 2000	T
	Star Office document (.sdw) as per Star Office format up to version 5.2.	T

[6] HTML 4.01 Specification – W3C Recommendation 24 December 1999. Available at: http://www.w3.org/TR/html4/.

[7] XHTML 1.0 The Extensible HyperText Markup Language (Second Edition): A Reformulation of HTML 4 in XML 1.0 – W3C Recommendation 26 January 2000, revised 1 August 2002. Available at: http://www.w3.org/TR/xhtml1/.

[8] Extensible Markup Language (XML) 1.0 (Third Edition) – W3C Recommendation 04 February 2004. Available at: http://www.w3.org/TR/2004/REC-xml-20040204/. Extensible Markup Language (XML) 1.1 – W3C Recommendation 04 February 2004, edited in place 15 April 2004. Available at: http://www.w3.org/TR/2004/REC-xml1120040204/.

[9] Microsoft packaging format for Web files (Mime Encapsulation of Aggregate HTML Documents).

[10] Extensible Stylesheet Language (XSL) Versions 1.0 – W3C Recommendation 15 October 2001. Available at: http://www.w3.org/TR/xsl/.

[11] Open Document Format for Office Applications (OpenDocument) v1.0 – standard ISO/IEC 26300. Available at: http://www.iso.org/.

[12] Document management --Electronic document file format for long-term preservation--Part 1: Use of PDF 1.4 (PDF/A -1) – standard ISO 19005-1:2005. Available at: http://www.iso.org/.

Component	Specification	Status
Spreadsheet type files	Open document (.ods) as per ISO/ IEC standard 26300 specifications.	R
	OpenOffice.org XML (.sxc) as per Open Office version 1.0 format.	T
	StarCalc spreadsheet (.sdc) as per Star Office format up to version 5.2.	T
	MS Excel (.xls) as per MS Office format up to version 2000.	T
Presentation type files	Open Document (.odp) as per ISO/ IEC standard 26300 specifications.	R
	OpenOffice.org XML (.sxi) as per Open Office version 1.0 format.	T
	HTML (.html or .htm) as per W3C specifications.	R
	MS Power Point presentation (.ppt) in MS Office format up to version 2000.	T
	StarImpress presentation (.sdd) in Star Office format up to version 5.2.	T
Data bank type files **Note**: Plain text (.txt, and .csv must include box layout to enable handling	.xml	R
	.myd, and .myi as per My SQL version 4.0 or better format	R
	.txt	R
	.csv	R
	OpenDocument (.odb) as per ISO/ IEC standard 26300 specifications.	R
	.sdb in Star Office format up to version 5.2.	T
	.mdb in MS Office format up to version 2000.	T
Exchange of graphic information and static images	PNG (.png), as per W3C[13] specifications – ISO/IEC 15948:2003 (E).	R
	TIFF (.tif)[14].	R
	SVG (.svg), as per W3C[15] specifications .	R
	JPEG File Interchange Format (.jpeg, .jpg or .jfif)[16].	R
	Open Document (.odg), as per ISO/IEC 26300 standard specifications.	R
	OpenOffice.org XML (.sxd) in Open Office version 1.0 format.	T
	XCF (.xcf) in GIMP v. 1.0 or higher format.	R
	BMP (.bmp).	T
	GIF (.gif), as per GIF87a and GIF89a[17] specifications.	T
	Corel Photo-Paint Image (.cpt) in Corel Draw format up to version 7.	T
	Photoshop Image (.psd) in Adobe Photoshop format up to version 4.	T

[13] *Portable Network Graphics (PNG) Specification (Second Edition). W3C Recommendation 10 November 2003. ISO/IEC 15948:2003 (E) – Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification.* Available at: http://www.w3.org/TR/2003/REC-PNG-20031110/. Accessed on 12/7/2005.

[14] *Tagged Image File Format (Adobe Systems).*

[15] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Available at:* http://www.w3.org/TR/2003/REC-SVG11-20030114/. Accessed on 12/7/2005.

[16] *JPEG File Interchange Format (version 1.02) 1 September 1992. Available at:* http://www.jpeg.org/public/jfif.pdf. Accessed on 12/7/2005.

[17] *Graphics Interchange Format (CompuServe/America Online, Inc.).*

Component	Specification	Status
Vector graphs	SVG (.svg) as per W3C specifics.	R
	Open Document (.odg), as per ISO/ IEC 26300 standard specifications.	R
	OpenOffice.org XML (.sxd) in Open Office version 1.0 format.	T
	Corel Draw Graphs (.cdr) in formats up to version 7.	T
	MSX (.msx) in Corel Draw format up to v. 7.	T
	MS Visio Graph(.vss ou .vsd), in formats up to version 2000.	T
	Windows Metafile (.wmf).	T
Animation standards specification	SVG (.svg), as per W3C specifications.	R
	GIF (.gif), as per GIF89a specification.	T
	Shockwave Flash (.swf), in Macromedia Flash format up to v. 4, and Macromedia Shockwave v. 1.	T
Audio and video type files	.mpg	R
	.mp4	R
	.mid	R
	.ogg	R
	.avi, with Xvid coding.	R
	.avi, with divX coding.	T
	.mp3	T
	.rm in Real Audio Media Player format up to v. 8.	T
	.ra in Real Audio Media Player format up to v. 8.	T
	.ram in Real Audio Media Player format up to v. 8.	T
	.rmm in Real Audio Media Player format up to v. 8.	T
	.avi	T
	.wav	T
	.swf in Macromedia Flash format up to v. 4 Macromedia Shockwave v. 1 format.	T
	.wmv in Windows Media Player format up to v. 6.4.	T
	.wma in Windows Media Player format up to v. 6.4.	T
	.mov in Apple Quicktime format up to v. 6.	T
	.qt in Apple Quicktime format up to v. 6.	T
Compacting general use files	ZIP (.zip).	R
	GNU ZIP (.gz).	R
	TAR Pack (.tar).	R
	Compact TAR Pack (.tgz ou .tar.gz).	R
	MS Cabinet (.cab).	T
Geo-referral - filing standards for work stations	Under study	E
Extended programming (plug-ins)	Future consideration	F

8.3. Means of Access: Technical specifications for Tokens, Smart Cards, and Cards in general

The initial specifications on smart cards and tokens were expanded after the conclusions the ICP-Brasil Work Group in Resolution no. 33 of 4/8//2003, which are based on the guidelines issued by ISO / IEC 7816 parts 1 to 6.

The work group's conclusions were also used in the preparation of the ITI Technical Practices Manuals, a set of documents that establishes the technical requirements to be observed in the procedures for approval of smart cards and cryptographic tokens by ICP-Brasil. The specifications that are included in these manuals were also used for the preparation of the present document, specifically in what concerns cryptographic devices.

The approval of systems and equipments of digital certification by ICP-Brasil was instituted by Resolution no. 36 of the ICP-Brasil Executive Committee on 10/21/2004, whereby ITI was made responsible for conducting the actual work, whereas the Study and Audit Laboratories (LEA) created by the same Resolution were put in charge of the conformity tests.

According to Resolution no. 36 medias for storing digital certificates and the corresponding readers as well as the systems and equipments needed to perform digital certifications should obey a minimum set of standards and specifications in order to guarantee interoperability and reliability of the information security resources used.

According to the regulation, such media as cryptographic tokens and smart cards, electronic signature authentication systems, certification and registration authorities, and equipment such as HSM, synchronizers, and time stamps among others are subject to mandatory approval. The products that are ratified through the established process will bear a conformity certificate and use the approval stamp and corresponding identification number.

It is important to note that the data stored in a given smart card or token cannot be protected by any kind of license that would forbid its being read by any other software than their suppliers'.

By standardizing these devices Brazil intends to facilitate its entrance into international agreements governing digital certification, in addition to fostering subscription to the e-PING, and helping to spread the use of certifications, which will contribute to reduce the cost of that technological solution.

The preparation of the present e-PING version took also into consideration ISO / IEC 7810 that defines such physical properties as flexibility, resistance to high temperatures, and dimension of three different kinds of card formats (ID1, ID2 and ID3), the PC/SC Workgroup standards, and the FIPS140 devices security standards of the National Institute of Standards and Technology (http://www.nist.gov). These fundamental standards were used by the ICP-Brasil Work Group to achieve better interoperability of the existing access devices such as smart cards and tokens, which handle digital certificates. Moreover, they absorbed ISO norms for more traditional and low cost magnetic cards, as well as optical cards, which are more advanced and have higher cost.

Future e-PING versions will establish a minimum agenda for the review of all specifications, and to map out the Federal government activities and plans that use some kind of smart card and that therefore should be looked into. Exhaustive research should be conducted to subsidize the decision to include in the e-PING a set of standards cards actually used by the government organs. An example of that are the so-called "embossed smart cards" (ISO / IEC 7811), or high-relief cards, that are not contemplated in the present version. In case it is confirmed by research their extensive use by the government the viability of including them in the e-PING specifications will be analyzed.

Future versions will also analyze in depth the standards that typically apply to the European community devices. Such is the case with the e-Europe, or "Open Smart Card Infrastructure for Europe - version 2" that assimilates the no-contact card technology reviewed by ISO / IEC 14443. The same applies to the CALYPSO standard (Fourth European Research and Technological Development Framework Program) for no-contact card and ticket systems meant for public transportation systems. The standards, licensing systems, and legal property rights should be evaluated if there are any.

Table 10 - Specifications for Means of Access - Smart Cards, Tokens, and Cards in general

Component	Specification	Sit	Applicability

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration		

Data definition	**ITI Technical Conduct Manuals** - Volume 1. See: http://www.lea.gov.br	**A**	All cards and tokens that handle digital certificates.
	ISO/IEC 7816-6 ID Cards – Integrated circuit contact cards. Part 6: Inter-sector data elements. **Note:** As chosen by ICP-Brasil Work Group	**A**	All.
	ISO/IEC 7812-1 ID Cards – Sender identification. Part 1: Numbering system.	**R**	All.
	ISO 9992-2 Financial transactions cards - Messages between the integrated circuit card and the card receiver device. Part 2: Functions, messages (commands and responses), elements, and data structure.	**F**	All.
	BS EN 1546-3 ID Card Systems - *Inter-sector electronic purse* – Part 3: Data exchange elements. **Note:** Present edition released in July, 1999. **BS EN ID Card Systems 1546-4** - Part 4: Data objects. **Note:** Present edition released in August, 1999.	**F**	All.
Applications, including multi-applications	**ISO/IEC 7816-4 ID Cards** Part 4: Inter-sector exchange commands.	**A**	Integrated circuit contact cards.
	ISO/IEC 7816-5 ID Cards Part 5: Numbering system and procedure for registering application identifiers.	**R**	
	ISO/IEC 7816-7 ID Cards Part 7: Inter-sector commands for *Structured Card Query Language* (SCQL).	**R**	
	ISO/IEC 7816-11 ID Cards Part 11: Structure for dynamic handling of multiple applications in integrated circuit cards	**R**	
	ISO/IEC 7813 ID Cards – Financial transactions cards.	**R**	Financial cards.
	ISO/IEC 7812-2 ID Cards Part 2: Procedures for application and registration.	**R**	All.
	ISO/IEC 15693-4 ID Cards– No-contact *Vicinity Integrated Circuit Cards* (VICC). Part 4: Registering applications/ senders.	**R**	Vicinity Integrated Circuit Cards.
	EN 1332-1:1999 ID Card Systems – Man-machine interface – Part 1: Principles of user interface projects.	**R**	All.

Component	Specification	Sit	Applicability
	EN 1332-4:1999 ID Card Systems - Man-machine interface – Part 4: Coding user demands for bearers of special needs.		
Electric	**ISO/IEC 7816-10 ID Cards** – Integrated circuit contact cards – Part 10: Electronic signals and responses for synchronous card reinitiating. **ISO/IEC 7816-12 –** Part 12: USB interface.	R	Integrated circuit contact cards.
	ISO/IEC 14443-2 ID Cards – No-contact integrated circuit cards (vicinity cards) – Part 2: Potency interface and radio frequency signal. **Note:** This part defines the radio frequency interface and contains two very distinct modulations (Types A and B) for data communications between cards and terminals. Type A is based on Philips Mifare technology (widely licensed to other manufacturers). Type B is a brand new concept. The two types are simultaneously processed in this part of the standard and in part 3. Moreover, some specific items of Type A are treated in part 4.	R	Vicinity card.
	ISO/IEC 10536-3 ID Cards - No-contact integrated circuit cards {*Close Coupling Integrated Circuit Cards* (CICC) - Part 3: Electronic signal procedures and reinitialization	F	Close coupling integrated circuit cards.
	ISO/IEC 15693-2 ID Cards - No-contact integrated circuit cards {*Vicinity Integrated Circuit* Cards (VICC) - Part 2: Interface and on air initialization	R	Vicinity cards.
Communications protocols	**ISO/IEC 7816-3** ID Cards - Part 3: Protocols for signaling and electronic transmissions. **Note:**As chosen by the ICP-Brasil work group.	R	Integrated circuit contact cards.
	ISO/IEC 14443-3 ID Cards - No-contact integrated circuit cards - Part 3: Initialization	R	Vicinity cards.

Component	Specification	Sit	Applicability
	and buffering. **Note:** This part gives continuity to Types A and B, and defines initialization and buffering procedures as well as basic communications protocols. Buffering procedures are methods used for identifying and selecting a card when several cards are active within the terminal's RF field. **ISO/IEC 14443-4** ID Cards– No-contact integrated circuit cards (vicinity cards) – Part 4: Transmission protocols. **Note:** This part contains data transmission protocol's high message level information equivalent to the ISO/IEC 7816 T=1 protocol, and bridges over to ISO 7816-4. ISO/IEC 14443-4 includes an initialization protocol procedure, but only for Type A.		
	ISO/IEC 15693-3 ID Cards – No-contact integrated circuit cards (vicinity cards) – Part 3: Buffering and transmission protocol	**R**	Vicinity cards.
	Message originating from **ISO 8583** financial transaction card – exchange message specification	**F**	All.
	ISO 9992-1 – financial transaction cards – Messages between integrated circuit card and card reader – Part 1: Concepts and structures; **ISO 9992-2** - Part 2: Functions, messages (commands and responses), data elements and structures.	**F**	All.
	ISO 10202-2 financial transaction cards – Security architecture for financial transaction systems with integrated circuit cards – Part 2: Transaction process; **ISO 10202-6 -** Part 6: Card bearer verification.	**R**	All.
	ISO/IEC 10536-4 no-contact integrated circuit cards (*Close Coupling Integrated Circuit Cards* - CCIC - Part 4: Response to reinitialization and transmission protocols.	**F**	Close coupling integrated circuit cards.
	Physical characteristics **ISO/IEC 7810 ID Cards** **Note:** To ensure that they are read by standard readers all cards must follow the specified	**R**	All contact and combination cards.
	ISO/IEC 7811 Magnetic Card, parts 2, 4 e 5: They define the properties, location and *coding* of the card's magnetic band.	**R**	All magnetic band cards.
	Optic memory cards **ISO/IEC 11693,** and **11694.** **Note:** Cards that support great volumes of stored *megabytes*.	**F**	Optic cards.
	ISO/IEC 7816-1 ID Cards - Part 1: Physical characteristics **ISO/IEC 15693-1** ID Cards – No-contact integrated circuit cards – Part 1: Physical characteristics.	**A**	Integrated circuit contact cards.

Component	Specification	Sit	Applicability
	ISO/IEC 7816-2 ID Cards - Integrated circuit contact cards – Part 2: Dimensions and locations of contacts. **Note:** This part is a supplement to ISO/IEC 7810, and establishes the physical characteristics which are specific to contact ID cards. Chosen byICP-Brasil work group and ITI Technical Conduct Manual, Volume I.		
	ISO/IEC 14443-1 ID Cards – No-contact integrated circuit cards — Part 1: Physical characteristics. **Note:** This part is a supplement to the physical characteristics defined by ISO/IEC 7810.	**R**	Vicinity cards.
	ISO/IEC 15693-1 ID Cards – No-contact integrated circuit cards - Part 1: Physical characteristics. This part of **ISO/IEC 15693** was released on 7/15/2000. **Note:** This part of **ISO/IEC 15693** was released on 7/15/2000.	**R**	Vicinity cards.
	ISO/IEC 10536-1 ID Cards – No-contact integrated circuit cards – Part 1: Physical characteristics; **ISO/IEC 10536-2 –** Part 2: Dimensions and location of coupling areas	**F**	Close coupling integrated circuit cards.
	Tactile identifiers **BS EN 1332-2** – ID Card systems – Man-machine interface - Part 2: Dimensions and location – Tactile identifier for ID-1 cards. **Note:** Some customized card readers, unless modified, may not properly handle 'notch'-type tactile ident- ifiers. Agreement must be reached with the makers of such equipments to avoid problems.	**F**	If embossed record is not used, and user is requested to fit card in a given way, a tactile identifier must be provided to aid visually impaired users.
Security	**ISO/IEC 7816-8** ID Cards – Integrated circuit contact cards - Part 8: Inter-sector security commands. **ISO/IEC 7816-9 -** Part 9: Additional inter-sector commands and security attributes. **ISO/IEC 7816-11** ID Cards – Integrated circuit contact cards - Part 11: Personal verification through biometric methods. **ISO/IEC 7816-15** ID Cards – Integrated circuit contact cards - Part 15: Cryptographic device information in ID cards	**A**	Integrated circuit contact cards.

	ISO 10202 Financial transaction cards – Financial transaction security architecture through integrated circuit cards.
	Part 1: Card's life cycle;
	Part 2: Principles and overview;
	Part 3: Cryptographic key relationships;
	Part 4: Secure application modules;
	Part 5: Algorithms utilization;
	Part 6: Card bearer verification;
	Part 7: Key management.
		F	All.

Component	Specification	Sit	Applicability
Terminal infrastructure	**EN 1332-3:1999** ID Card Systems–Man-machine Interface – Part 3: Keyboards.	**R**	All.
	PC/SC standards Joint PC/SC work group standards for interoperability specifications for ICCs and personal computer systems - Part 1: Introduction and architecture overview; Part 2: Interface requirements for ID cards and interface devices; Part 3: Requeriments for interface devices coupled with PCs; Part 4: IFC Project consider-ations and reference inform-ation; Part 5: ICC resource manager's definition; Part 6: Interface definition of ICC service provider; Part 7. Considerations on the application's domain/developer project; Part 8. Recomendations on implementation of ICC security and privacy devices. **Note:** For general PC use.	**A**	All.
	ITI Technical Conduct Manual – Volume I.	**A**	Cards with digital certificate management capability.
	FIPS-140-2 Standard. **Note:** ICP-Brasil work group, item 1: follow the minimum rules for security level 1 as per FIPS-140-2. Follow at least security level 2 rules for hardware tampering.	**A**	All.
Java Card types	API (*Application Programming Interface*) Java Card platform.	**A**	Defines classes groups where applet-based Java Card technology may be built.
	Runtime environment specification for Java Card platform.	**A**	Describes the required environment for executing applets based on Java Card.
	Virtual machine specification for Java Card platform. **Note:** Java Card technology version 2.2.1 (October, 2003): http://java.sun.com/products/javacard/	**A**	Defines the required configuration for the card's virtual machine.

9. Organization and Exchange of Information

9.1. Organization and Exchange of information: Technical policies

The technical policies on information organization and exchange systems are as follows.

9.1.1. Use of XML for data exchanges.

9.1.2. Use of XML Schemas and UML whenever the case is for data exchange definition.

9.1.3. Use of XSL for data transformation.

9.1.4. Use of metadata standards to handle electronic content.

9.2. Organization and Exchange of Information: Technical specifications

Table 11 - Specifications for the Organization and Exchange of Information

Component	Specification	Status

	A = Adopted
	R = Recommended
	T = in Transition
	E = under Elaboration
	F = Future consideration	

Language for data exchange	XML (*Extensible Markup Language*) as defined by W3C See: http://www.w3.org/XML.	**R**
Data transformation	XSL (*Extensible Stylesheet Language*) as defined by W3C. See: http://www.w3.org/TR/xsl. XSL *Transformation* (XSLT) as defined by W3C. See: http://www.w3.org/TR/xslt.	**R**
Data definition for exchange	XML *Schema* as defined by W3C: - *XML Schema Part 0: Primer* at http://www.w3.org/TR/2004/REC-xmlschema-0-20041028 - *XML Schema Part 1: Structures* at http://www.w3.org/TR/xmlschema-1/structures - *XML Schema Part 2: Datatypes* at http://www.w3.org/TR/xmlschema-2/datatypes UML (*Unified Modeling Language*) as defined by OMG http://www.omg.org/gettingstarted/specsandprods.htm/	**R**
Data description	RDF (*Resource Description Framework*) as defined by W3C.	**F**
Metadata elements for content management	e-PMG – "Padrão de Metadados para o Governo Eletrônico" as defined at http://www.eping.e.gov.br	**E**
Navigation taxonomy	LAG – "Lista de Assuntos do Governo" as defined at http://www.eping.e.gov.br	**E**
Data definition	Data Standards Catalog as defined at http://www.eping.e.gov.br	**E**

9.3. Notes on XML and Middleware

Not all systems need to have the capability to communicate directly in XML as shown by figure 5. When appropriate it is acceptable to use middlewares as shown by figure 6.

Although the configurations below offer potential solutions the direct XML model on figure 5 is preferred, but it is possible to use the indirect model presented in figure 6 if there is justifiable motive.

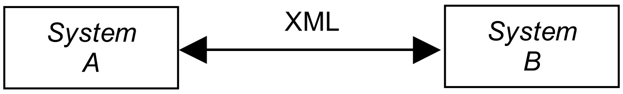

Figure 5 – Direct XML Model – Direct Exchange

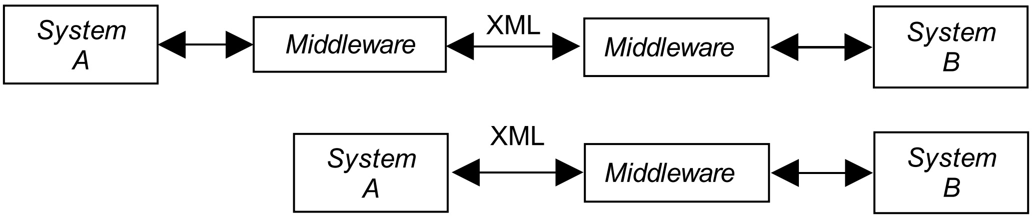

Figure 6 – Exchange through middleware

9.4. Notes on Subjects under Study and Elaboration

List of Government Subject Matters: Navigation Taxonomy (LAG)

Government organs provide information and services through Web portals and sites, but the complexity of the governmental structure can make the information search an arduous task.

The List of Government Subject Matters: Navigation Taxonomy (LAG) is under construction to help people independently find information of the knowledge on the government's structure or of which organ is responsible for the subject.

The mechanisms used in the popular Internet directories are the more familiar examples of classified lists.

Version zero of LAG is in the final elaboration stage.

Metadata Standards for the Electronic Government (e-PMG)
The simplification of the search for information should be a priority goal for governments in the information era. That verification stimulates the creation of Metadata Standards for the Electronic Government (e-PMG), under elaboration.

Metadata are given relative the other data, that is, structured and/or codified data that describe and allow to find, manage, understand, and preserve other data along the time.

The e-PMG will be based on the DCMI (Dublin Colors Metadata Initiative) metadata standards.

10. Electronic Government Integration Areas

10.1. Electronic Government Integration Areas: Technical policies

The guidelines for this segment are as follows.

- The technical specifications under responsibility of the segment include:
  - XML *Schemas* regarding applications for the government performance areas in the organized catalog form, available in the e-PING Internet site with current contents presented in latter topics;
  - The components that are related to issues that cut across the government performance areas, whose standardization is relevant for the interoperability of services of electronic government, such as Geographic Processes and Information.

- In what concerns XML *Schemas* of applications related to the government performance areas, this segment will look for the identification, the attendance of the production and the analysis of contents of interest of the public administration, in articulation with the government's representative groups and of the society, being moderated to the competent instances with respect to the priority assignment.

- The technical specifications for XML *Schemas* in the segment "Organization and Exchange of Information" should be obeyed by their proponents.

- Since the actual use of XML *Schemas* happens through interoperable services it is recommended that
  - the Service Oriented Architecture (SOA) and the technical policies related to the "Interconnection" segment are obeyed by the project and in the implementation of applications based on the referred XML *Schemas*;
  - the segment adopts the Reference Architecture for Government Interoperation Computer Systems, a SOA model adapted to the actual conditions of government computer systems available at http://i3gov.cos.ufrj.br/igov/.

- There is a strong interconnection between the Data Standards Catalog and the XML *Schemas* Catalog and, while considering their specific contents, their general principles and managerial guidelines should be kept compatible.

10.2. Electronic Government Integration Areas: Notes on XML *Schemas* Catalog

10.2.1. Brief considerations

The e-PING architecture favors the adoption of XML and the development of XML *Schemas* as the foundations for the government's integration and electronic interoperability. In this sense, the creation of a repository that allows Electronic Government application managers and planners to consult the consolidated XML *Schemas*, as well as to propose the cataloguing of outlines under their responsibility, undeniably contributes to consolidating good interoperability practices within the government.

10.2.2. Objective

The Catalog purports to establish standards for XML *Schemas* applicable to the interfaces of systems that support the Electronic Government services.

10.2.3. Scope

The Catalog contains the accepted standards in XML *Schemas* format for data exchange in the public sector. Such standards may encompass a single outline or a group of XML *Schemas* if the group refers to an identical issue of the associated Integration Area.

The release of XML *Schemas* does not imply automatic access to the corresponding contents or associated services. The appropriate rules will be defined their respective managers.

10.2.4. Property and Responsibility

The e-PING Coordination is responsible for this Catalog, especially for managing the change processes and fostering the use of the standards in future developments.

In this sense, it is recommended that the released XML *Schemas* be considered in the development or the maintenance of systems that support the Electronic Government services related to the areas and subareas of government performance that are dealt with in the Catalog.

The development and maintenance of this Catalog are incumbent on the "Electronic Government Integration Areas" Work Group, which is made up by participants from different Federal and State government segments.

10.2.5. Managing the XML Schemas Catalog

Inclusions in the XML Catalog may be done through the following situations:

1. Accepted content proposals for the Data Standards Catalog (CPD).
2. Accepted submissions of content proposals for the Reference Architecture for Governmental Interoperations Computer Systems (AR).
3. Submissions by public sector professionals of content proposals for the XML Catalog through the electronic form available at the e-PING Internet site.

In the situations described in the items (b) and (c), the contents will be sent to the "Information Organization and Exchange" Work Group for analysis and evaluation prior to the decision on whether to release the associated data standards.

Proposals for the recording of XML *Schemas* will be submitted to analysis by the "Electronic Government Integration Areas" Work Group through specific electronic form available at the e-PING Internet site (www.eping.e.gov.br). The Catalog will keep only those proposals that are accepted, while proposals under study, rejected proposals, and previous versions of accepted XML *Schemas* will be kept in a “work environment” that will be constructed for that purpose.

The evaluation criteria to be used will include:

- the recognition by the user community;
- the area or subarea manager's agreement (in case he is not the proponent); compliance with the e-PING standards.

The occurrence of XML Schemas submissions made by proponents other than the area manager is foreseen, but their acceptance is conditional to the area manager's agreement, and must be negotiated by their proponents and/or the "Electronic Government Integration Areas” Work Group.

Requests for modifications of XML *Schemas* already released will be firstly analyzed by the "Electronic Government Integration Areas" Work Group. The decision to accept them or not will be made by the Central e-PING Coordination, which may adopt the proposed changes depending on their inclusiveness and impact or submit them to public consultation through the Internet site http://www.governoeletronico.gov.br .

The Catalog’s initial charge as presented later on consists of groups of XML *Schemas* related to initiatives already mapped out by the "Electronic Government Integration Areas" Work Group.

Releasing them has the purpose of giving visibility to the cases of effective use of XML Schemas by the APF and its partners.

The initial load of consolidated contents and their updates can be accessed through the e-PING page (www.eping.e.gov.br).

10.2.6. Format for submitting XML *Schemas*

Each XML *Schema* or group of XML *Schemas* correlates should be documented in accordance with the following format.

PROPOSING ORGAN: Name of upper echelon organ proposing the XML *Schema*, for example Ministry of Agriculture, Ministry of Education, Ministry of the Environment, etc..

RESPONSIBLE PARTY: The name of the professional who is responsible for proposing the XML *Schema*.

BRAZILIAN IRS NUMBER (CPF): The tax number of the professional who is responsible for submitting the XML *Schema*.

UNIT OF WORK: Unit where the person who makes the proposal works. Must show the organ's hierarchical string, for instance GIS / DSI / SLTI / MP.

E-MAIL: The electronic address of the professional in charge of the XML *Schema* proposition.

TELEPHONE 1: Primary contact telephone number of the professional who is responsible for proposing the XML *Schema*.

TELEPHONE 2 (optional): Alternate telephone number of the professional who is responsible for proposing the XML *Schema*.

JURISDICTION: Indicates whether the proponent is responsible for managing the area or subarea that relates to the XML *Schema* by checking one of the options (Yes or No).

MANAGING ORGAN: The organ that manages the area or subarea to which the XML *Schema* is related. It should be filled only if JURISDICTION is checked "No" and the proponent knows what the managing organ is.

NAME OF XML SCHEMA: Usual denomination of the group or of the sole XML *Schema* to be classified.

VERSION: Version of XML *Schema* to be classified.

URL OF XML *SCHEMA*: URL where will be found the XSD file (XML *Schema* definition) and the detailed information on the XML *Schema* or group of *Schemas*.

DESCRIPTION: Brief description of the XML *Schema* or *Schemas* and additional considerations that the proponent considers pertinent.

SUBAREA: Usual denomination inside the government performance area to which the XML *Schemas* are related. It should be informed only if the area identification is not enough to qualify the XML *Schema* topic.

XML SCHEMAS' COMPONENTS: The names of the XML *Schemas* included in the group to be classified.

10.2.7. XML *Schemas* Catalog's Classifications

The XML *Schemas* Catalog will be organized by issue areas of government performance, and will link the catalogued XML *Schemas* according to the first order classifications in the List of Government

Performance Areas as used by the Pluriannual Plan (PPA), which is presented below.

List of Government Performance Areas as used by the Pluriannual Plan (PPA)

1. Social Care.
2. Health.
3. Public Security.
4. Education.
5. Administration.
6. Tax Administration.
7. Housing.
8. Science and Technology.
9. Trade and Services.
10. Foreign Affairs.
11. National Defense.
12. Special Responsibilities.
13. Culture.
14. Environment Administration.
15. Social Welfare.
16. Work.
17. Transportation.
18. Energy.
19. Agriculture.
20. Agrarian Organization.
21. Communications.
22. Judicial Matters.
23. Legislative Matters.
24. Basic Justice.
25. Citizens' Rights.
26. Sports and Leisure.
27. Industry.
28. Sanitation.
29. Urbanization.

The electronic version of the XML *Schemas* Catalog will provide as an alternate search option to the above classification the alphabetical listing of the catalogued XML *Schemas*.

10.3. Electronic Government Integration Areas: Technical Specifications

The specifications for the Electronic Government Integration Areas are listed in tables 12 and 13.

Table 12 - Specifications for the Electronic Government Integration Areas - Traverse Themes to the Government Performance Areas

Themes	Specification	Status	Observations
PROCESSES – Language for Process Execution	BPEL4WS V1.1 as defined by OASIS. See: http://www.oasis-open.org/committees/download.php/2046/BPEL%20V11%20May%205%202003% 20Final.pdf	**R**	The work group will follow on the evolution of BPEL4WS V2.0. Studies on the orchestration and choreography of processes will be done futurely by the group.
PROCESSES – Notation for Process Modelling	BPMN 1.0 as defined by OMG. See: http://www.bpmn.org/ Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf	**R**	

Themes	Specification	Status	Observations
GEORE-FERRAL – Interoperability between geographic information systems	WMS, WFS, WCS, and GML as defined by OGC. See: http://schemas.opengis.net/gml/3.1.1/ http://schemas.opengis.net/wcs/1.0.0/ http://schemas.opengis.net/wfs/1.1.0/ http://schemas.opengis.net/wms/1.3.0/	R	
	SFS as defined by OGC.	E	

Table 13 - Specifications for the Electronic Government Integration Areas - XML *Schemas* Catalog as related to the Government Performance Areas

Area/Subarea	Specification	Notes
ADMINISTRATION - Government Purchases	https://comprasnet.gov.br/xml/aviso.xsd https://comprasnet.gov.br/xml/consultamatserv.xsd https://comprasnet.gov.br/xml/dispinex.xsd https://comprasnet.gov.br/xml/contratoent.xsd https://comprasnet.gov.br/xml/empenho.xsd https://comprasnet.gov.br/xml/resultado.xsd	XML *Schemas* within ComprasNet for Bidding Closure Results, Purchase Commitment, Exemption/Ineligibility of Bidding, Search for Materials via CATMAT, non-SISG entitiy contracts, and Notice of Bidding.
ADMINISTRATION – Government Structures	https://guialivre.governoeletronico.gov.br/igov/	Group of XML *Schemas* relating to APF management.
ADMINISTRATION – Local Network Management/CACIC	https://guialivre.governoeletronico.gov.br/cacic/sisp2/invent/Invent.html	These *Schemas* are a part of the CACIC solution developed by Dataprev, and are used for hardware inventory data transmission. The implementation of these *Schemas* was done in partnership with the Ministry for the Environment.
TAX ADMINISTRATION – Electronic Fiscal Billing	https://200.198.224.29/portal/info/Schemas.htm	XML *Schema* used for issuing legal tender electronic sales receipts instead of printed paper ones. This Project is coordinated by ENCAT (a class organ of fiscal administration professionals), and was developed in

Area/Subarea	Specification	Notes
		partnership with the Federal Revenue Secretariat.
CITIZENS' RIGHTS - Notaries	https://mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd	The Ministry of Justice keeps the National Notary Offices Catalog. This *Schema* uses filters for federated units, municipalities, neighbor-hoods, and notary office attributions. It issues lists of complying entries as desired. It also produces detailed information on any notary office listed.
CITIZENS' RIGHTS – Consumer Protection	https://mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd	This *Schema* allows consulting the consolidated statistics of SINDEC-affiliated PROCONS' (Consumer Rights Offices) service delivery. SINDEC is the National Consumer Defense Information System. Is filters are federated unit, and supplier's name or tax number. Lists are issued according to filter.
CITIZENS' RIGHTS – Consumer Protection	https://mj.gov.br/Schemas/Recall/ConsultaRecall.xsd	This *Schema* allows reasearching the Ministry of Justice's Consumer Protection and Defense Department's data bank to find out whether any given product is the object of mandatory recall actions. It returns lists of manufacturers/models subject to recalls from product, serial number, chassi number, lot number, and other filters.
CITIZENS' RIGHTS	https://mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd	This *Schema* filters the Ministry of Justice's Public Entertainment Indicative Classification Catalog by film or show name, and returns detailed

Area/Subarea	Specification	Notes
		information on the respective classification and the justication for it.
ENVIRONMENT ADMINISTRATION – Licensing/PNLA	https://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_completo.xsd https://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_simples.xsd https://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_totalizadores.xsd	These *Schemas* apply to environmental licensing, and are used by the Ministry of the Environment's PNLA (National Portal for Environmental Licensing) plataform, which consolidates State information through *Web Services.*
JUDICIAL BRANCH – Extrajudicial Notary Services	www.anoregsp.org.br/arquivos	These *Schemas* relate to standardizing research on extrajudicial notary services.

11. Glossary of Acronyms and Technical Terms

ABNT (Brazilian Association of Technical Norms): A private organism that publishes norms for the preparation and compilation of references used for the production of documents and their inclusion in bibliographies, summaries, reviews, compilations and other.

ACAP – Application Configuration Access Protocol: An Internet protocol for remote access to client program options, configurations, and preferential information. It is one of the available solutions for the problem of customers' mobility in the Internet.

APF (Federal Public Administration): The line organs of the direct administration (services under the administrative structure of the Presidency of the Republic and of the Ministries) and indirect administration (Autarchies, Public Companies, Societies of Mixed Economy and Public Foundations) of the Executive Branch of the Brazilian Federal Government. See: https://www.planalto.gov.br/ccivil_03/ decretolei/del0200.htm.

BPM - Business Process Management: An overview of the business processes of an organization such as the flow of services that use XML notation representation, execution, and coordination standards whose semantic rigidity allows its interoperability with systems of different platforms, having become a foundation for implementation of service oriented architecture solutions. When the execution of the services is coordinated by subordination to a master process, generally of the intra-organizational kind, that coordination is called Orchestration. When the coordination is not subject to a master process, generally of the inter-organizational kind, it is called Choreography.

Browser: Web Navigator. A client application that allows the user to read World Wide Web material in another net or in a personal computer, to follow hypertext links, and to transport files.

Catalog of XML *Schemas*: An information directory of XML *Schemas*.

Cryptography: Technique for the protection of information that consists of calculating the content of a message, or a sign and transforming it in illegible text by using complex mathematical algorithms.

Devices: Physical components such as work stations, cellular telephone, smart cards, handhelds, and digital television sets with Internet access, etc.

DNS – Domain Name System: The forms by which the domain names are found, and translated in the Internet protocol addresses. A domain name is a resource easily recalled by reference to an Internet address.

Free software: A computer program available together with its code-source and permission to copy, and distribute it in the original or modified form, either free or for a price. Free software is necessarily non-proprietor, but it is important not to mistake free software with no-cost software.

FTP. File Transport Protocol: It is a protocol application that uses the Internet protocols TCP/IP, and is the simplest way to exchange files between computers in the Internet.

GML. Geography Markup Language: An XML-based OpenGIS specification developed to allow the transport and storage of geographical and space information.

Handhelds: Hand computers, also known as PDA, pocket PC, or palm top. Portable equipment developed to be access devices.

Handshake: In telephone communications, it means exchange of information between two modems and the resulting agreement on what protocol to use before each phone connection.

Hashing: It usually is the transformation of a chain of characters into a smaller value of fixed size, or a key that represents the original chain. It is used to index and recover items in a database because it is faster to find the item by using the smaller transformed key than the original value. It is also used in cryptography algorithms.

HELO: Parameters that limit the delivery of commercial, unwanted e-mails. See: http://www.postfix.org/uce.html .

HTTP. Hyper Text Transfer Protocol: A set of rules for exchanging files such as texts, graphic images, sound, video, and other multimedia files in the World Wide Web.

HTTPS. Secure Hyper Text Transfer Protocol: A Web protocol developed by Netscape and coupled to that navigator. It cryptographs and crypto-analyzes requests and returns of pages by the Web server. HTTPS is the use of Netscape's SSL (Secure Sockets Layer) of as a sublayer under the normal program organization of the HTTP applications.

ICP-Brasil: A set of techniques, practices, and procedures to be implemented by the Brazilian government and private organizations to establish the technical and methodological foundations for a system of digital certification based on public keys. See: http://www.icpbrasil.gov.br .

IEEE. Institute of Electrical and Electronics Engineers: it foments the development of standards and norms that frequently become nationally and internationally accepted.

IETF. Internet Engineering Task Forces: Entity that defines the operational protocol standards of the Internet, like TCP/IP.

IMAP. Internet Message Access Protocol: Standard register for accessing e-mail from a local server. IMAP is a customer/server protocol through which the e-mail is received and kept by the Internet server.

IP. Internet Protocol: method or protocol through which the data are sent of a computer the other in the Internet. Any computer that operates in the Internet has at least one IP address that identifies it to all other computers in the Internet.

IPSec. Internet Protocol Security: development standard related to net layer security or net communications package processing. A great advantage of IPSec is that security dispositions can be handled without demanding changes in the individual users' computers. IPSec supplies two options of security services: AH (Authentication Header), essentially data sender authentication, and ESP (Encapsulating Security Payload), that supports both sender authentication and cryptographic data coding.

IPv4. Internet Protocol Version 4: see "IPv6".

IPv6. Internet Protocol Version 6: last level of IP, today already included as part of IP support in many products, besides the major computer operating systems. Formally, IPv6 is a group of IETF specifications. IPv6 was projected as an evolutionary group of IPv4 improvements. The most significant improvement of IPv6 in relation to IPv4 is that IP addresses increased from 32 bits for 128 bits.

LAN. Local Area Network: group of computers and associated devices that share a same communications line and the resources of a single processor or server in a small geographical area. Usually, the server holds the applications and stores the data that are shared by several users in different computers.

LDAP. Lightweight Directory Access Protocol: software protocol to allow the location of organizations, people, and other resources as files and devices in a net, either in the public Internet or in a corporate Intranet.

Means of access: group of physical (access devices) components and no physical (basic software, applications, etc.) that allows the user to access the electronic government services.

Messaging in Real Time or Instant Messaging: It is a communications type that allows the user to exchange messages in real time with another user also connected to the net.

Metadata: they are necessary additional information to make the data become useful. It is essential information for using the data. In short, metadata are sets of data characteristics that are not usually included in the data themselves. See: http://www.isa.utl.pt/dm/sig/sig20002001/TemaMetadados/trabalho.htm

Middleware: it is a general term that means to mediate two separately existing programs. Different applications can communicate through the *Messaging* services of middleware programs.

Newsgroup: discussion on a certain subject through messages sent to a central Internet site and redistributed by Usenet, a global net of news and discussion groups. The users can send messages to existing news groups, answer previous messages, and create additional news groups.

OGC. Open Geospatial Consortium: has as its mission to "develop specifications for space interfaces that will be made available freely for general use".

Open standard: any technological standard that is established by international organs or business consortia whose specifications are openly available. The PC (personal computer) was created and it is still developed on open standards. So are the Internet specifications and their development. The great majority of the programming languages use open standards.

Pattern of Metadata: A metadata set is a pattern that is defined by a community of users and includes a Vocabulary of descriptive elements and an Outline or rules for coding these elements in computer readable ways. See: http://www.uff.br/gdo/htm/tsld013.htm.

Plug-in: An accessory program that adds capabilities to the main program. In Web applications they usually are programs that can be easily installed and used as part of the navigator. A plug-in application is recognized automatically by the navigator and its functionalities are integrated into the HTML page that is being presented.

POP3. Post Office Protocol 3: more recent version of the standard protocol to recover e-mails. POP3 is a customer/server protocol through which the e-mail is received and kept by the Internet server.

Portal: Internet site that combines services, news, and great volumes of information and/or entertainment contents.

Rede Governo (Government Net): Entrance portal for all of the Federal Government Internet pages. http://www.federativo.bndes.gov.br/destaques/egov/ egov_redegoverno.htm

Resolution no. 7 of the Electronic Government: it establishes rules and guidelines for the Internet sites of the Federal Public Administration (gov.br and mil.br). Divided into 7 chapters, the Resolution disposes on the information structure, control and monitoring, the administration of the interactiing elements, the organizational model, the visual identity and the security of the government sites in the worldwide computer net. See: http://www.governoeletronico.e.gov.br .

RFC. Request for Comments: formal IETF document resulting from models and revisions by concerned parties. The final RFC version became a standard that allows neither comments nor alterations. The alterations can happen, however, through subsequent RFCs that replace or reelaborate previous RFCs. RFC is also an abbreviation for **Remote Function Call**.

RSA. Rivest-Shamir-Adleman: Internet coding and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Services of Electronic Government (related: Electronic government services, Electronic Services). **Electronic Government** may be defined as the utilization of technology to increase the access to, and improve the delivery of government services to citizens, suppliers, and public servants. In general lines, the major functions of electronic government are:

1. Electronic delivery of information and services.
2. Regulation of the information networks, mainly involving governance, certification, and taxation.
3. Public accountability, transparency, and monitoring of budget spending.
4. Nonpresential teaching, computer literacy, and maintenance of virtual libraries.
5. Cultural diffusion with emphasis on local identities, and fostering and preservation of local cultures.

6. *e-procurement*, that is, acquisition of goods and services through the Internet, such as electronic public auctions, electronic proclamations, virtual purchasing and other public types of digital markets for the acquisition of goods for the government.
7. Incentive to e-business through the creation of safe transactions environments especially for small and medium-sized companies. See: http://www.governoeletronico.gov.br/r1

Systems of Information of the Federal Government: systems that support activities of

- Government administration: Planning, Budget, Budget Execution, Financial Management, Human Resources Management, General Services Management, Document and Information Management, Organizational and Administrative Modernization, Information and Computer Resources, and Internal Control;
- Government performance: finalistic activities of the government agencies, such as infrastructure (transport, communications, energy, administration of natural resources), Agriculture, Health, Education, etc. For reference see: http://www.redegoverno.gov.br/projetos/reg_gestao.asp.

Smart Cards: plastic cards approximately the size of a credit card with a built-in microchip that can be loaded with data, used to make phone calls, electronic payments in money and other applications. They are updated periodically to receive additional uses.

S/MIME. Secure Multi-purpose Internet Mail Extensions: safe method for sending e-mail that uses the RSA coding system. S/MIME describes as the encoded information and a digital certificate may be included in the message body.

SMTP/MIME. Simple Mail Transport Protocol/Multi-purpose Internet Mail Extensions: SMTP is a TCP/IP protocol used for sending and receiving e-mails. MIME is an extension of the original Internet e-mail protocol that allows to exchange different types of data files in the Internet.

SOA - Service Oriented Architecture: Architecture aimed at systems interoperability through loosely coupled service interface sets where the services do not need the technicalities of other services' platforms to accomplish the exchange of information.

SOAP. Simple Object Access Protocol: it describes a model for packing XML questions and answers. SOAP messaging is used to allow the exchange of a variety of XML information. The SOAP norm takes on the task of transmitting requests and answers on services between users and service suppliers.

SPAM: unwanted Internet e-mail. From the sender's point of view it is mass messaging to a Usenet discussion group list or people included in a commercial addressing list. For the addressee, spams are usually just plain garbage.

SSL. Secure Sockets Layer: it is a protocol commonly used to manage the security of message transmission in the Internet.

Taxonomy for Navigation: it is a controlled vocabulary of hierarchically organized and structured terms and sentences, which is based on natural or constructed relationships, and aims at facilitating the acess to Internet sites and portals for discovery of information through navigation.

TCP. Transmission Control Protocol: a set of rules that are used with IP to send data to computers in the Internet in the shape of message units. While IP deals with the actual delivery of data, TCP controls the individual data units into which a message is divided for efficient routing through the Internet.

Telnet: the way to access another person's computer, assuming that permission has been given. More technically, Telnet is a user command and subliminal TCP/IP protocol to access remote computers.

TLS. Transport Layer Security: a protocol that guarantees the privacy between communications applications and their users in the Internet. When a server and a customer communicate, TLS guarantees that no other party can see or pick up the message.

Token: a structured data object, or a message that continually loops around the net nodes (token ring) and describes the current net status.

UDDI. Universal Description Discovery and Integration: it is the repository where developers register their available *Web Services* to allow the customers to find and use Extranet and Intranet services.

UDP. User Datagram Protocol: communications protocol that offers a limited amount of services whenever messages are exchanged between computers in a net that uses IP. UDP is an alternate for TCP and, if joined by IP, is referred to as UDP/IP. Such as TCP, UDP uses IP to take a data unit from a computer to another. Unlike TCP, UDP does not supply the service of breaking a message into packages and remounting it on the other end. UDP does not supply the pack sequence of data arrival. That means that the application program using UDP should guarantee that the whole message arrives and is in order. The net applications that want to save on processing time because they have very small data units to exchange may prefer UDP to TCP.

UML. Unified Modeling Language: standard notation of real world object models as the first step in developing an object-oriented design methodology.

URI - *Uniform Resource Identifier*): Standard for coding Internet names and addresses. A URI usually is made up by a name e.g. file, http, ftp, news, mailto, gopher, etc., followed by semicolon, and ending with a path, in compliance with RFC 1630. URI encompasses the URN e URL concepts..

Usenet: collection of notes and messages submitted by users on a variety of topics, and sent to worldwide web servers. Each collection is known as a newsgroup.

VPN – *Virtual Private Networks*): a private network that uses public telecommunications networks' – such as the Internet - infrastructure for transferring confidential information. The transferred data are encrypted, and their implementation is done through virtual tunnels to protect them from access by unauthorized users.

W3C – *World Wide Web Consortium*: industry association to promote standards for the Web's evolution and the interoperability of products that circulate in the Internet. This Consortium produces specification and reference softwares.

WAN – *Wide Area Network*: computer network covering an extensive geographic area such as a State, Country, or Continent.

Web Services**:** logical, programmable applications that make widely differing applications compatible with each other regardless of their operational systems, and allow data communications and transfers among different networks.

WFS – *Web Feature Service*: OpenGIS specification that offers customized acess (entering, updating, excluding, and analyzing) to the Web environment (HTTP).

WMS. Web Map Service: OpenGIS specification that defines 4 protocols (GetCapabilities, GetMap, GetFeatureInfo and DescribeLayer) that allow reading of multiple layers of georeferred information containing vectors and or images.

WSDL - Web Services Definition Language: It is an XML format for description of services Web and their information for access. It describes the functionalities of the services offered by the provider of services, as well as his/her location and access form.

XML. eXtensible Markup Language: It sorts things out flexible to create formats of common information and to share the formats and the data in World Wide Web, in Intranet and anywhere. XML is expandable because unlike HTML its symbols are unlimited and self-defined.

XML *Schemas*: They are XML documents, also found in the Internet, that specify the structure, the number of occurrences of each element, the allowed values, the units, etc., in other words, the syntax of the document. The outlines of a group of XML documents of the same type are available openly in an Internet site so that the programs can have access to them to validate the XML documents in that group. See: http://www.uff.br/gdo/htm/tsld106.htm .

XMPP. eXtensible Messaging and Presence Protocol: open protocol, based on XML for real time messaging.

XSL. eXtensible Stylesheet Language: It describes how data may be organized in the Web by using XML and presented to the user. XSL is a language for formatting an XML document.

XSLT. eXtensible Stylesheet Language Transformations: Standard way to describe, as well as modify the structure of an XML document into another XML document with a different structure. XSLT can be thought of as an extension of XSL. XSLT shows how an XSL document may be reshaped into another data structure to be presented according as an XSL spreadsheet).

12. Bibliography

Câmara Técnica de Implementação do Software Livre. Planejamento Estratégico 2003–2004 - Diretrizes, Objetivos e Ações Prioritárias.

Microsoft Press. Dicionário de Informática. Translation and editorial support of Fernando Barcellos Ximenes – KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 8570017480.

Thing, Lowell (editor). Dicionário de Tecnologia. Translated by Bazán Tecnologia e Lingüística e Texto Digital. São Paulo: Futura, 2003. ISBN 8574131385.

13. Collaborators

e-PING Coordination

Brazilian Association of State-Owned Data Processing Companies (ABEP)
Dayse Vianna
Paulo Cezar Coelho

Bank of Brazil (BB)
Ulisses de Sousa Penna

Federal Savings Bank (CAIXA)
Ângela B. Baylo

Social Security Technology and Information Company (DATAPREV)
Humberto Degrazia Campedelli
José Antônio Borba Soares

Ministry of Justice (MJ)
Jorilson da Silva Rodrigues

Ministry of Planning – Secretariat for Logistics and Information Technology (MP/SLTI)
Leandro Corte (General Coordinator)
Antônio Carlos Alff
Eduardo Favero
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Leonardo Lanna Guillén
Nazaré Lopes Bretas
Rogério Santanna dos Santos
Sylmara Garcia

Presidency of the Republic – The National Institute for Information Technology (ITI)
Mauricio Augusto Coelho
Renato da Silveira Martini
Viviane Regina Lemos Bertol

Federal Data Processing Service (SERPRO)
Antônio Sérgio Borba Cangiano
Catia Gontijo Rezende
Elói Juniti Yamaoka
Geancarlo Noronha Vinhal
Wagner Junqueira Araújo

Interconnection Work Group

Leonardo Lanna Guillén (MP/SLTI) - Coordinator
Carlos Bellone Neto (SRF)
Eder Manoel de Abreu (EMBRAPA)
Flávio Arthur Leal Ferreira (PROCERGSRS)
Júlio César Japiassu Lyra (MJ)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Gonzaga Costa (SERPRO)
Odilon de Freitas Militão Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Ruben César Macedo (CELEPARPR)
Sílvia Aparecida da Cunha (MP/CGTI)
Ulisses de Sousa Penna (BB)
Vicente Eduardo Costa de Paula Pessoa (SRF)
Webster's Gomes Fernandes (MI)

Security Work Group

Jorilson da Silva Rodirgues (MJ) – Coordinator
Alerrandro Luís Augusto Caetano Corrêa (MEC)
Alexandre Almeida Lima (SEORI)
Alexandre Braga (CPqD)
Carlos Eduardo de Santos Souza (CENSIPAM)
Catarina da Matta (ELETROBRÁS)
Clari Dorça Stacciarini (CGU)
Cristiano Sakai (PR)
Daniel Bispo de Jesus (CODESP)
Eloi Juniti Yamaoka (SERPRO)
Ernandes Lopes Bezerra (MP/SLTI)
Etienne César Ribeiro de Oliveira (IBGE)
Humberto Degrazia Campedelli (DATAPREV)
Jailson Mario dos S. Pereira (CORREIOS)
Jean Carlo Rodrigues (ITI)
Joana D'arc Felipe dos Santos (MI)
João Carlos Levy Argel (FUNARTE)
José Ney de Oliveira Lima (MP/SLTI)
Jovino Francisco Filho (MC)
Leonice Tereza Vanni Rangel (CEPROMAT – MT)
Luiz Augusto Barbosa Mozzer (CGU)
Luiz Augusto Vieira de Melo (ANCINE)
Marco Antonio Goes de Oliveira (FNDE)
Marco Aurélio Bonato (CELEPAR)
Marcos Allemand Lopes (SERPRO)
Marcos José da Silva (DATAPREV)
Mônica Vieira Guimarães (MI)
Nilson Carlos de M. Pontes (IBGE)
Renato Navajas (MDIC)
Ronaldo Íon Miranda do Nascimento (MJ)
Ruy Siqueira de Moura (MRE)
Sérgio Carreira dos Santos (IPHAN)
Silvio Márcio Santos Nery (CGU)
Wagner Junqueira Araújo (SERPRO)

Means of Access Work Group

Mauricio Augusto Coelho (ITI) – Coordinator
Renato da Silveira Martini (ITI) – Coordinator
Alessander Florindo da Silva (MS)
Eliane Aristóteles Moreira (DATAPREV)
Eliane Pereira dos Santos (MS)
Eloína Terezinha Domanski (MF)
Geancarlo Noronha Vinha (SERPRO)
Jean Carlo Rodrigues (ITI)
Jorilson da Silva Rodrigues (MJ)
José de Souza Rangel Filho (ATIPE)
Juscelino Ney Carrico (SGIMS)
Márcia Luiza Albertini (MS)
Paulo Édison de Souza (MEC)
Ricardo José Leal dos Santos (PRODERJRJ)
Silvio Melo de Souza (ITI)
Viviane Regina Lemos Bertol (ITI)

Organization and Exchange of Information Work Group

Eloi Juniti Yamaoka (SERPRO) – Coordinator
Ailton Luiz Gonçalves Feitosa (CLDF)

Aline Ramalho Bezerra (MJ)
Ana Lúcia de Medeiros (CORREIOS)
Ana Maria Moura (PRODERJ)
Ângela B. Baylo (CAIXA)
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Cláudia Carvalho Masset Lacombe Rocha (ANCC)
Dalva Clementina Luca (MJ)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (ANCC)
Diogo Arce Moreth (MT)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (ANCC)
Fernanda Hoffmann Lobato (MP/SLTI)
Flávia Lacerda Oliveira de Macedo (TCU)
João Alberto Lima (Senado Federal)
José Gabriel Medef Filho (CGU)
Luciana Ferreira Pinto da Silva (INEP)
Luiz Antônio Nery de Oliveira (DATAPREV)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcia Luzia Albertini (MS)
Márcio Imamura (IBGE)
Marcos Augusto Francisco Borges (CPqD)
Margareth da Silva (ANCC)
Maria Augusta de Oliveira Gomes (MF)
Maria Célia Pelisson Jacon (IBGE)
Maria das Graças Comaru de Oliveira (SERPRO)
Maria de Fátima Porcaro (IPT)
Maria Valéria Lins Tenório (ATIPE)
Nádia Maria F. C. Abrantes Ferrão (MF)
Neuza Arantes Silva (MAPA)
Paulo César Pereira Soares (FUNARTE)
Ricardo Torres Lenzi (INEP)
Rosiane Fonseca (ANCINE)
Samuel Batista dos Santos (IPT)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Taciano Tres (BB)
Vicente de Paula Teixeira (CGU)
Vivianne Veras Barrozo (SERPRO)

Electronic Government Integration Areas Work Group

Nazaré Lopes Bretas (MP/SLTI) – Coordinator
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)
Alexandre Grossi (MD)
André Redivo (PR)
Antônio Carlos Alves Carvalho (MEC)
Caio Nakashima (MDS)
César Cardoso (CORREIOS)
Cláudio Machado (MS)
Dalva Clementina Luca (MJ)
Dayse Vianna (PRODERJRJ)
Edna Paulo Cirineo (SRF)
Edmar Morett (MMA)
Ednylton Maria Franzosi (MP/SLTI)
Eduardo Favero (MP/SLTI)
Efraim Soares dos Santos (CAIXA)
Elisa Torrido Lorensi (IBAMA)
Enos Josué Rose (MCIDADES)
Fábio Borges (DNPM)

Gabriel Mathias (IBICT)
João Lima (SENADO)
Jorge D.M. Cerqueira (PR/GSI)
Jorge Luiz Salomão de Oliveira (CORREIOS)
José Eustáquio Nogueira Guimarães (PR/GSI)
José Ney de Oliveira Lima (MP/SLTI)
Karina Lima de Moura (MP/SEGES)
Leandro Corte (MP/SLTI)
Maria de Fátima (IPT)
Maria Rita Almeida (SRF)
Mauricio Dayrell (MMA)
Moema José de Carvalho Augusto (IBGE)
Mônica Lucatelli (DATAPREV)
Onivaldo Rosa Junior (MEC)
Paulo César Pereira Soares (FUNARTE)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo Torres Lenzi (INEP)
Rodolfo Pinto da Luz (INEP)
Samuel Batista (IPT)
Sandro Araújo (ANA)
Silmara Ramos (PR/GSI)
Sylmara Garcia (MP/SLTI)
Valério Falcão (MP/SLTI).