Brazilian Government

Executive Committee for Electronic Government

gov.br

e-PING

MAIS GOVERNO, MAIS CIDADANIA.

e-PING
Electronic Government Interoperability Standards

Reference Document

Version 4.0

16 December, 2008

TABLE OF CONTENTS

Introduction

The e-PING – Electronic Government Interoperability Standards – architecture defines a minimum group of premises, policies and technical specifications that regulate the use of Information and

Communication Technology (ICT) in the interoperability of Electronic Government Services,

establishing conditions for them to interact with the remaining Branches and spheres of government and with society in general.

The areas covered by e-PING are segmented in:

- Interconnectivity;
- Security;
- Means of Access;
- Organization and Exchange of Information;
- Areas for Electronic Government Integration.

Components were assigned for each one of these segments, for the further establishment of standards.

The entire content of the document of reference is in line with the guidelines set out by the Executive Committee for Electronic Government, created by the Decree of 18 October, 2000, and is published in a specific site on the Internet (http://www.eping.e.gov.br), in order to assure public access to information that is of general interest, and the transparency that is intrinsic of the initiative.

The Brazilian government is committed to guaranteeing that these policies and specifications remain in line with society's needs, and follow the evolution of the technology market.

The e-PING document of reference contains:

- the basis/grounds for the e-PING conception, implementation and administration, listing the benefits expected from the work, defining the limits of the e-PING architecture coverage, and highlighting the premises and the policies established;
- the e-PING management model, describing responsibilities, criteria for the verification of conformity, change management, dissemination and guidelines for capacity-building;
- the policies and technical specifications set out for every component in each one of the e-PING segments;
- glossary of referenced technical terminology;
- list of the participants and collaborators of this version of the document.

The content of this document pertains do public domain, there being no restriction on its reproduction or in using of the information therein contained. Reproduction may be carried in whichever media, without needing specific authorization. Inappropriate use of the material for unlawful ends will be subject to the appropriate legal measures, by the Brazilian Government, holder of its copyrights.

The complete or partial use of this document for commercial purposes is prohibited.

Part I – e-PING Overview

1. Introduction

The starting point to offering better services, appropriate for citizens' and business' needs, at lower costs, is the availability of an Information and Communication Technology (ICT) infrastructure to stand as a pillar for the creation of these services. A modern, integrated and efficient

Government demands equally modern, integrated and interoperable systems, working fully, safely and in line with the public sector.

In such context, the interoperability of technology, processes, information and data is mandatory in order to provide quality services, therefore it becomes a premise for governments all over the world, as basis for the concepts of electronic governments - the e-gov. interoperability allows us to rationalize investments in ICT, by sharing, re-using, and exchanging technological resources.

Governments such as in North America, Canada, Britain, Australia and New Zealand strongly invest in ICT, setting up structures that are dedicated to providing interoperability, with the purpose of offering better services at lower costs.

The Brazilian government is strengthening the e-PING architecture – "Electronic Government Interoperability Standards," which aims at being the paradigm for the establishment of policies and technical specifications to allow for the rendering of quality electronic services to society.

What is interoperability?

In order to achieve the e-PING objectives, it is important to clearly define what we understand by *interoperability*. To follow, we present four concepts that underline the Brazilian government's understanding on the matter:

"The coherent exchange of information and services between systems. It must allow for the replacement of any component or product used in the interconnectivity points, for another one of a similar specification, without compromising the systems functionalities." (Government of the United Kingdom);

"The ability of transferring and using information in a uniform and efficient manner, among various organizations and information systems (Government of Australia);

"Ability of two or more systems (computers, means of communications, networks, software and other information technology components) to interact and exchange data, according to a defined method, in as to achieve expected outcomes." (ISO);

"Interoperability defines if two components of a system, developed through different tools, from different suppliers, may or may not work together." (Lichun Wang, European Bioinformatics Institute – CORBA Workshops);

Interoperability is not only an Integration of Systems, not only an Integration of Networks. It is not only about data exchange between systems. It does not only address the meaning of technology.

It is, actually, the sum of all of these factors, also considering the existence of a legacy of systems, platforms, Hardware and Software implemented. It comes from principles that deal with the diversity of components, with the use of different products, from different suppliers. Its goal is to understand all of the factors so that the systems may perform cooperatively, establishing the norms, the policies and the standards needed to achieve these objectives.

For interoperability to be achieved, the people shall be engaged in a continuous effort to assure that systems, processes and cultures in an organization are managed and directed to maximize opportunities to exchange and reuse information.

2. Scope

Clearly defined policies and specifications for the interoperability and management of information are important to provide government connection, both internally, as well as in terms of contact with the society, and greater coverage level, with the rest of the world – other governments and companies performing in the world market. e-PING is conceived as a basic structure for the electronic government strategy – Executive Branch, without any restriction against the participation of the other branches and government tiers, by adhering to it voluntarily.

The government's information resources are valuable economic assets. While guaranteeing that the government information may be quickly located and exchanged between the public sector and the society, still maintaining its obligations concerning privacy and security, the government helps it making the most use of this asset, propelling and encouraging the country's economy.

The e-PING architecture covers the exchange of information between the federal government – Executive Branch systems, and the interactions with:

- Citizens;
- Other government tiers (state and municipal);
- Other Branches (Legislative and Judiciary) and the Federal Prosecutor's Office;
- International Organizations;
- Governments from other countries;
- Companies (in Brazil and worldwide);
- Third Sector.

The following figure represents that relationship.

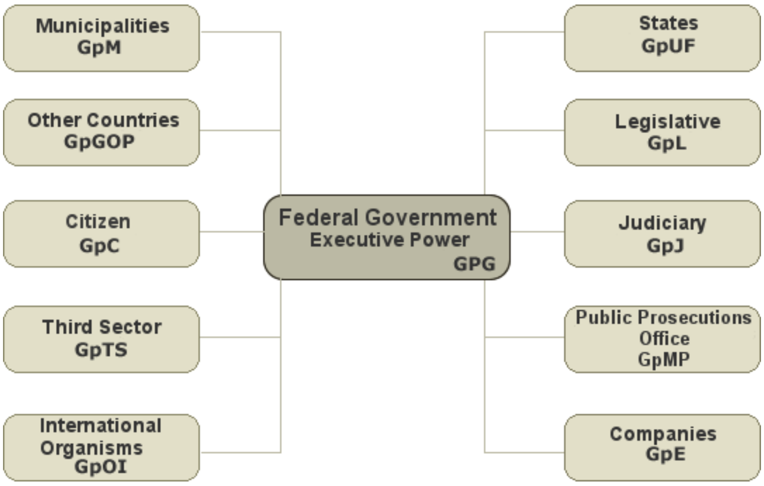

Figure 1 – Relationships in the Federal Government.

2.1. Adopting the e-PING

The adoption of e-PING standards and policies cannot be imposed over the citizens and the different government tiers, inside and outside of the country. The Brazilian government, however, sets out such specifications as the standard selected and accepted, in other words, these are the standards based on which it wishes to interoperate with entities outside of the federal government – Brazilian Executive Branch. These entities shall join the e-PING voluntarily, and without any interference by the e-PING coordination staff.

Within the federal government – Brazilian Executive Branch, adoption of the e-PING Standards and policies is mandatory.

The “federal government – Brazilian Executive Branch" includes:

- entities that make up the Direct Administration: Ministries, Secretariats and other government entities having the same legal structures, direct or indirectly connected to the Presidency of the Republic of Brazil
- autarchies and foundations.

Within the above mentioned entities, the specifications contained in the e-PING are mandatory for:

- all of the new information systems to be developed and implemented in the federal government and that are within the scope of interaction, inside the federal government and with society in general;
- previous information systems that are subject to implementations involving the provision of electronic government services or interactions among systems;
- other systems that are included in the goal of making electronic government services available.

Adhesion to the e-PING shall take place gradually, and according to the implementation plan designed by the agency itself, which will take into account the situation of the institution regarding the conditions needed to meet the e-PING specifications and recommendations.

For the government information systems that are not obligated to join the e-PING, we recommend that those responsible for them do consider adopting e-PING standards whenever significant updating efforts are planned.

All federal government – Executive Branch procurement and hiring aimed at the development of electronic government services and updating the systems in place must comply with the specifications and policies set out in this document.

e-PING encourages the participations of all parties interested in continuously developing and updating the specifications and recommendations of the architecture. e-PING management foresees this participation through the Internet (http://www.eping.e.gov.br), as the preferred means of contact between e-PING managers and the society.

2.2. Focus on interoperability

e-PING will not cover all matters related to the area of Information and Communications Technology (ICT). It will only deal with specifications that are relevant to assure interconnection of the systems, data integration, access to electronic government services and content management. e-PING covers the issues related to segmentation, as described under topic 4 of this document.

2.3. Subjects not addressed

e-PING does not intend to standardize the way in which the information on electronic government is presented, and is limited to defining the requirements concerning data exchange and the conditions of the availability of these data to access devices.

Information on guidelines and policies related to the presentation and accessibility of gateways and sites to the electronic government are available in the Brazilian electronic government gateway at (http://www.governoeletronico.gov.br).

3. General Policies

Each of the e-PING segments has a set of technical policies that drive the establishment of the specifications of its components. These specific sets relating to each segment are based on the following general policies:

Alignment with the INTERNET: all the information systems in the public administration must be in line with the main specifications used in the Internet and the World Wide Web.

Adoption of XML as the primary standard to exchange data throughout all the systems in the public sector.

Adoption of Browser as the main means of access: all government information systems shall be accessible, preferably through technology based on browser; other interfaces are allowed in specific situations, such as for updating routines and data collection, whenever there is no technological alternative available based on browser.

Adoption of metadata for government information resources.

Development and adoption of an Electronic Government Metadata Standard – e-PMG, based on internationally accepted standards (http://www.eping.e.gov.br).

Development and maintenance of the Government List of Subjects: Browsing taxonomy (LAG), which addresses the subjects related to the government's performance, organized in a directory structure (http://www.eping.e.gov.br).

Market Support: all of the e-PING specifications consider solutions that are widely supported by the market. The purpose here is to reduce costs and risks in conceiving and producing services within the government information systems.

Scalability: the specifications chosen must be capable of meeting the system's changes in demand, such as, changes in data volume, amount of transactions, and amount of users. The standards set out cannot be a limiting factor, and must be capable of supporting the development of servers to address from small specific needs, involving small volumes of transactions and users, to nationwide demands, dealing with large amounts of information and involving a greater number of users.

Transparency: the e-PING documents are available to society, via Internet, and there shall be mechanisms to disseminate it, and receive and evaluate suggestions. In that regard, deadlines and commitments for the implementation and management of a dedicated site on the Internet (http://www.eping.e.gov.br) shall be defined – and disseminated for public acknowledgement.

Preferred Adoption of Open Standards: e-PING sets out that, whenever possible, open standards will be adopted in the technical specifications. Proprietary standards shall be accepted, temporarily and during transitions, however keeping in mind the aim to replace them as soon as there are conditions to migrate. Without dismissing those goals, situations that demand that information security and integrity requirements be reviewed, shall be respected. Whenever available, Free Software solutions are preferred, in accordance to the policy set out by the Executive Committee for Electronic Government (CEGE).

e-PING is totally compatible with the government initiatives in the field of ICT. As an example, we refer to the Brazilian Government Guide on Free Software Migration. (http://www.governoeletronico.gov.br).

Ensuring information privacy: all agencies responsible for offering e-gov services must provide the conditions needed to conserve information privacy of citizens, companies and government agencies, respecting and complying with the legislation that establishes the restrictions on access and dissemination.

4. Segmentation

The e-PING's architecture was divided into five parts, with the purpose of organizing the definition of Standards. For each of the **segments**, a working group was created, made up of professionals, specialists in each area, from federal, state and municipal government entities. These groups were responsible for designing this version of the architecture, which is the basis to establish the Brazilian government interoperability standards.

The five segments – "Interconnectivity", "Security", "Means of Access", "Organization and Exchange of Information" and "Areas for Electronic Government Integration" – were subdivided in **components**, for which policies and technical specifications to be adopted by the federal government were set out. The components that make up each of the five segments are described below.

4.1. Interconnectivity

The segment for "Interconnectivity" sets out the conditions needed for the government agencies to InterConnect, plus it establishes the conditions for interoperation between government and society.

This segment established specifications for:

- Messaging;
- Network Infrastructure;
- Network Services.

4.2. Security

This segment addresses ICT security aspects to be considered by the federal government.

It provides standards for:

- IP Security;
- Electronic Mail Security;
- Encryption;
- System Development;
- Network Services;
- Wireless Networks;
- Collection, Treatment and Filing of Evidence.

4.3. Means of Access

The segment "Means of Access" explains the issues related to the standards of the devices to access electronic government services. This version addresses the policies and specifications for work stations, smart cards, tokens and other cards, digital television and mobility. Future versions will address other devices. This segment is made up of four subgroups, related to the following components:

Standards for access via work stations:

- Browsers;
- Character sets and Alphabets;
- Hypertext interchange formats;
- Document file types;
- Spreadsheet file Types;
- Presentation file Types;
- Database file types for Work Stations;
- Graphical/still image information exchange;
- Vector Graphics;
- Specification of Animation Standards;
- Audio and Video Files;

- General purpose files and Compression;
- Geographic Information Files (Shapefiles).

Smart Cards / Tokens / Others:

- Data Definition;
- Applications (including multi-applications);
- Electric Components;
- Communication Protocols;
- Physical Interface Standards;
- Security;
- Terminal Infrastructure.

Mobility:

- Definition;
- Transmission Protocol;
- Browser;
- Hypertext Standard;
- Extended programming;
- Messaging;
- Video and Sound Files;
- Image Files;
- Office Files;
- PDF Reader.

Digital TV:

- Definition;
- ABNT Rules;
- Specification of Standards.

4.4. Organization and Exchange of Information

It addresses the aspects related to the treatment and transfer of information in the electronic government services. Includes standard for the structure of government subjects and metadata, covering the following components:

- Language for data exchange;
- Language for data transformation;
- Defining the data to be exchanged;
- Government List of Subjects: Browser Taxonomy (LAG);
- Government Metadata Standard (e-PMG).

4.5. Areas for Electronic Government Integration

This segment establishes the use or construction of technical specifications based on the XML standard in order to support the exchange of information in fields that cross over those of the government's activities.

The tools to support the segment are:

- Data Standard Catalogue (CPD);
- XML *Schemas* Catalogue;
- Interoperable Service Catalogue (Web Services).

5. e-PING Management

This topic covers the aspects of the e-PING architecture management, describing how the Brazilian government intends to achieve and strengthen the implementation of policies and technical specifications as effective Standards adopted both internally, by the agencies that make up the Federal Public Administration, as well as in it interoperation with outside entities, represented by other government tiers, by the private sector, by institutions in the third sector, and by the citizen.

5.1. Background

The e-PING architecture aims at being the interoperability paradigm for the federal government, beginning in the scope of the Executive Branch. The initiative of setting up this architecture came from three agencies in the federal tier:

- Ministry of Planning, Budget, and Management, through its Secretariat of Logistics and Information Technology (SLTI/MP);
- National Institute of Information Technology, of the Presidency of the Republic (ITI);
- Federal Data Processing Service (SERPRO), a public enterprise linked to the Ministry of Finance.

These agencies organized a Seminar involving several federal government entities, during which they created an interdepartmental steering committee – called the Constituent Committee - to drive the initial efforts of assembling the e-PING architecture. After it became institutionalized, through Administrative Ruling no. 5, of 14 July, 2005, it started being called the e-PING Coordination. In addition to these three organizers, the following agencies were part of the group: Presidency of the Republic, Ministry of External Relations, Ministry of Health, Bank of Brazil, Federal Savings Bank (CAIXA), DATAPREV and the Brazilian Association of Information and Communication (ICT) State Entities (ABEP).

The Committee set out the following work program:

- To define the initial format to design and manage the e-PING architecture;
- To define the segmentation of the topics to be covered by e-PING;
- To create five working groups responsible for the initial definition of policies and technical specifications for each one of the segments;
- To establish a work timetable with the purpose of creating and disseminating the first version of the architecture, called version 0;
- To hold public consultation and public hearings in the states of RS, SP, DF, RJ, MG and PE, in order to gather contributions from the general public, regarding the content suggested for version 0;
- To publish version 1, along with the e-PING institutionalization resolution, in the scope of the APF – Executive Power;
- To publish version 1.5, containing the updates and revision of the technical specifications and of the general overview on e-PING. Versions 1.1 to 1.4 are being discussed by the working group and the e-PING coordination;
- To hold public consultation and public hearings in order to gather contributions from the society in general, at each new version of the reference document;
- To publish the annual version, containing the updates and the revision of the technical specifications and of the general overview on e-PING.

Similar experiences developed by governments of other countries are constantly being researched. The e-GIF – Government Interoperability Framework – belonging to the British government was used as basis for the creation of the Brazilian government's interoperability architecture. The e-PING management follows the format implemented by the government of the United Kingdom, in operation since 2000, and is currently at a maturity state that is internationally acknowledged as reference.

5.2. Implementation Strategy

The dissemination of the Standards and specifications set out by the Brazilian government uses the version control system. The design of an annual version is foreseen, as well as intermediate publications of updates whenever significant changes are made.

This version solidified the work of the groups set up for the five segments. All its content was put available for Public Consultation, with the purpose of obtaining contributions to the proposals of standards published in version 3.9.

5.3. Management Model

This topic provides the ways to manage the e-PING architecture, and lists management's main duties and how to implement such activities within the government structural organization.

5.3.1. Duties

E-PING management embraces the performance of both activities that are administrative in nature as well as technical activities.

Within the **activities that are administrative in nature**, we highlight:

- To define the government strategic and management objectives regarding the establishment of Standards;
- To administrate the Brazilian government's interoperability architecture, providing the management infrastructure necessary for its correct administration, and assuring it will be updated, taking into account: government priorities and goals, society's needs, and the availability of new mature technologies that are supported by the ICT market;
- To be a coordination center for the e-PING architecture, seeking to align interoperability efforts, and to assure the coherence of the initiatives put forth by the government agencies;
- Specifically for the Interoperability segments, to administrate the relationship among the federal government – Executive Branch – and the other tiers defined under topic 2 - Scope;
- To manage and to make operational the dissemination of e-PING standards, considering:
  - The creation and administration of a site on the Internet for the e-PING (http://www.eping.e.gov.br);
  - Coordination of the public consultation processes;
  - Coordination of the process to receive and evaluate proposals of amendment and others;
  - Coordination of the process to request suggestions for e-PING;
  - Publication of e-PING updated versions and intermediate updates;
- To manage the interaction with initiatives having the same purpose, led by other governments in the country and abroad;
- To encourage capacity-building for the federal government's staffs, working jointly with the agencies, both at considering e-PING within the specific training plan of each one of them, as well as in holding corporate events aimed at disseminating the e-PING standards;
- To set out, implement and disseminate indicators to follow up on the outcomes obtained by the e-PING implementation;
- To manage the interaction with the entities responsible for setting out standards (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Ruling Institutes for specific segments, such as ABNT, INMETRO, ISO, NIST, etc). These bodies shall be chosen at the e-PING coordination's discretion, taking into account their international acknowledgement, capacity and the establishment of open standards.
- To manage the interaction with national and international development agencies, in order to concentrate resources, to meet e-PING creation needs, and promote research and development;
- To allow for the implementation, and to manage the process for the approval of the standards to be set out by the government;
- To allow for the implementation, and to manage hearing processes carried out with the purpose of verifying how much of the e-PING recommendations and specifications have been adopted;
- To perform cooperatively, with the support or government agencies, in carrying out the processes needed to adjust to the e-PING standards; to study the possibility of sponsoring broader programs to promote intensive use of the standards proposed.

Within the **activities that are technical in nature**, we highlight:

- To establish procedures for the design and maintenance of the policies and technical specifications that make up e-PING, taking into account:
  - Identification, creation, and management of specific working groups;
  - Establishment of agreements and definition of government institutions to be responsible for the policies and technical specifications of specific components of the interoperability segments;
  - Identification and implementation of alternative technical management procedures regarding the matters addressed within the scope of the e-PING;
- To coordinate development and maintenance, in the scope of the federal government – Executive Branch, of:
  - Government Metadata Standard (e-PMG);
  - Government List of Subjects: Browsing Taxonomy;
  - Data Standard Catalogue (CPD);
  - XML Schemas Reference Catalogue;
  - Other Standards for Organization and Exchange of Information;
  - Interconnectivity Standards;
  - Security Standards;
  - Standards on Means of Access to government electronic services;
  - Standards for the use of Smart Cards, Tokens and other types of cards;
- To assure that all of those responsible for the technical segments defined for e-PING will adopt the same conceptions, concepts, definitions and establishment of standards.

5.3.2. Responsibilities

The government structure created for the e-PING administration is shown in the simplified diagram below.

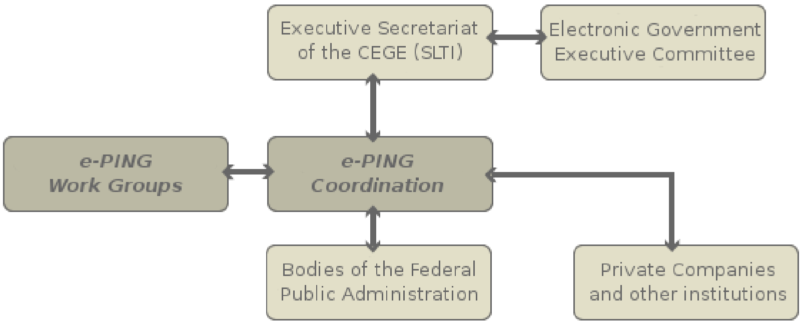
Executive Secretariat of the CEGE (SLTI)
Electronic Government Executive Committee
e-PING Work Groups
e-PING Coordination
Bodies of the Federal Public Administration
Private Companies and other institutions

Figure 2 – e-PING Administration.

The SLTI/MP, through instrument of the System for Administration of Information and Computer Science Resources, created by Decree 1.048, of 21 January 1994, is the one responsible for institutionalizing and defining the legal structure of the e-PING Coordination.

The activities of the e-PING Coordination will be led by the following:

- e-PING architecture implementation, providing the activities needed to solidify the current version and the dynamics of its evolution;
- e-PING architecture management;
- Setting out and managing the rules, and the institutional and legal instruments that assure that e-PING recommendations and specifications will be put in effect;
- Assuring maintenance and updating the various e-PING catalogues;
- Managing processes for the Communication and Dissemination of standards, decisions and e-PING activities, including the publication of new versions and intermediate updates;
- Creating an e-PING stamp and administrating the process to certify a certain service or product's adhesion to the e-PING;

- Providing criteria and subsidies for the design of the federal government's Annual Budget Law;
- Manage processes to hire services and to establish agreements to help carry out the duties needed to solidify the standards, such as, for example, the evaluation of e-gov proposals and projects, directed to the Federal Public Administration;
- Administrating Working Groups, defining their composition and determining the guidelines, based on technical, general, and specific policies, on the government needs, and on the monitoring of the technological scenario.

The e-PING Working Groups, made up by representatives appointed by the various APF agencies and by representatives from institutions in other government tiers, are responsible for:

- Addressing the subjects that make up the e-PING segments;
- Systematically monitoring the market, specifically the segments under its responsibility, with the purpose of identifying needs for technological update of policies and technical specifications;
- Subsidizing the e-PING Coordination activities, in performing its administrative and technical duties.

The Working Group coordinators shall have seats in the e-PING Coordination.

5.4. Additional Activities

In addition to the administrative and technical duties needed for the implementation and evolutionary maintenance of the e-PING architecture, other activities will be under the responsibility of the e-PING coordination.

5.4.1. Selection and Accreditation of Technological Standards

The technical policies in this document are the basis for the e-PING standards, and are reference in selecting the components for which technical specifications will be set out.

E-PING foresees an analysis of the standards that are being considered to be part of the architecture. This process includes the selection, accreditation and classification of the specifications selected, according to five levels defining situations that characterize the degree of compliance to the general and specific technical policies of each segment.

The Five levels are the following:

- **Adopted (A):** topic adopted by the government as an e-PING architecture standard, having been submitted to a formal accreditation process carried out by a government institution, or by any other institution formally appointed to carry out the process. It is also considered accredited when based on a proposal duly substantiated by the segment's coordination, and published on the site and approved by the e-PING coordination;
- **Recommended for consideration (R):** a topic that fulfills e-PING's technical policies, is acknowledged as a topic that should be used in the scope of government institutions, but has not yet been submitted to a formal accreditation process;
- **Undergoing Transition (T):** topic not recommended by the government because it does not meet one or more requirements set out within the general and technical architecture policies; it is included in the e-PING due to its significant use in government institutions, and tends to be deactivated as soon as another component, from one of the previous situations, presents conditions to replace it. It may eventually be considered a "recommended" component, as long as it adjusts itself to all the technical policies established. It is worthwhile to note that the development of new services or the recreation of significant parts of those already existing services may prevent the use of components that are classified as being transitional ;
- **Under Review (E):** a component that is being examined and will be placed in one of the situations above, as soon as the evaluation process is concluded;
- **For Future Consideration (F):** a component that has not yet been evaluated and will be subject to future studies.

The processes of choosing the components adopted by e-PING and their classification in the situations mentioned above, are the responsibility of the Working Groups, made up of specialist professionals working within the government and in institutions with which some kind of agreement or contract has been made specifically for that end.

The selection is made starting from formalized suggestion, internal demands from government agencies, the Executive Power, and researches carried out by the Working Groups.

However, the accreditation must be subject to a more profound study carried out by the e-PING managers. Due to the major variety of components dealt with by the architecture, it will be necessary to design an accreditation system that addresses from processes that dismiss the presentation of physical characteristics of certain components (Smart Cards, for example) to others, that require the study of aspects that involve the use of the component in developing and building services (organization and exchange of information and security, for example). In that case, the government shall establish agreements or accredit institutions to design conformity tests, always defining which criteria shall be submitted to accreditation processes, and the criteria used to evaluate the outcomes, and the conditions to carry out the procedures.

Complete definition of the selection and accreditation process, considering the specificity of the segments, will be under the responsibility of the e-PING coordination.

5.4.2. Auditing and Conformity

The federal government – Executive Branch's compliance with the specifications and recommendations is a critical factor in succeeding on the implementation of the e-PING. The e-PING managers will recommend that auditing process be carried out, in order to verify the compliance with architectural specifications and policies.

Responsibilities may be assigned to staffs especially set up for such purpose, made up of technicians in the government with experience in those types of procedures.

The preferred way of carrying out this procedure, however, is by using the structures of the agencies responsible for the systems' auditing themselves. The e-PING coordination works with the purpose of suggesting basic criteria to be followed by the agencies. For that matter, and through the administrative ruling no. 8 of 31 October, 2008, of the SLTI/MP, a Working group was created to study, analyze and suggest an auditing model related to the adherence to e-PING standards. This proposal will also address the e-PING maturity model.

5.4.3. Site Creation and Maintenance

All processes for information exchange on e-PING with users, collaborators and other persons concerned shall be carried out preferably through the Internet, at http://www.eping.e.gov.br. In its most advanced operational stage, the e-PING site shall have the following main functionalities:

- Total dissemination of documentation related to the architecture: official versions and their respective updating, versions for public consultation, supporting technical documentation, and related legal and institutional documentation;
- Availability of the recommendations, determinations, technical and policy specifications for validation, accreditation and receipt of comments and suggestions coming from the society;
- Publication of requests for comments related to the specification of architecture components;
- Availability of electronic means to receive suggestions;
- Availability of links for documents, standards, rules, or any type of reference within the e-PING.

5.4.4. Legal and Institutional Follow-up

e-PING will count on constant support from the Legal Advisory staff of the Ministry of Planning, Budget and Management, in order to assure that the content of the documents that make up its architecture complies with the rules and legal instruments in effect in the country.

In addition to that, this advisory staff will also be responsible for preparing all the institutional aspects needed to assure that the e-PING's recommendations and adjustments are included in the set of ICT legal instruments of the country.

The e-PING Coordination may work in the direction of establishing a way to cooperate with some other government agency that can provide its legal support structure to carry out this activity.

5.4.5. Dissemination

Total publicity will be given to the e-PING content. The main means of dissemination foreseen, in addition to the site on the Internet, are:

- Carrying out specific dissemination events, such as Seminars, Workshops and presentations in general;
- Participating in government events in the field of ICT and correlated areas;
- Participating in events directed to specific audiences;
- Publishing all of e-PING's versions as well as the intermediate updates;
- Exchanging information and experiences with other government tiers and branches, with public institutions and the third sector and with governments of other countries.

5.4.6. Capacity-building

Initiatives for capacity-building will be part of the e-PING implementation and management agenda. The intensive use of Distance Learning is also foreseen.

The e-PING coordination will design and publish a minimum training curriculum, so that every APF agency may have subsidies to plan and estimate the investments needed to train the professionals involved in the process of adjusting to the e-PING recommendations.

Each government agency shall observe the e-PING definition of standards while setting up its own capacity-building plans, in order to assure appropriate training for its technical staffs.

5.5. Relationship with Government and Society

This topic addresses e-PING's relationships with government entities and society.

5.5.1. Federal Government Organizations – Executive Branch

In the scope of the Executive Branch, the participation of all hierarchical levels of the Federal Public Administration, its agencies and regulating bodies, and public enterprises and institutions, is very important to promote and solidify interoperability in the public sector.

Although the general guidelines are controlled by the e-PING Coordination, each institution itself will be responsible for managing and assuring the use of e-PING standards. Among those tasks, we highlight:

- To contribute to continuous development and improvement of the e-PING;
- To assure that it's ICT organizational strategies make sure that all systems integrated to the electronic government under its responsibility are in compliance with the e-PING recommendations.
- To have a plan to implement and adjust the organization's ICT structure to the e-PING architecture;
- To assure that the institution's staffs withhold the abilities to set and use the specifications required for interoperability, thus providing training support whenever necessary;
- To appoint a person of contact in the institutions, for the exchange of information and needs together with the e-PING Coordination;
- To set aside and supply resources to support adjustment to the e-PING;
- To take advantage of the opportunity to rationalize processes (as a result of the increase in interoperability) in as to improve quality and reduce costs of providing e-gov services.

5.5.2. Other Government tiers (other Federal Branches, State and Municipal Governments)

Adoption of the e-PING is mandatory for the agencies and entities of the federal government – Executive Branch. For the other Branches (Judicial, Legislative) and other government tiers (state and municipal) its adoption is optional.

The e-PING coordination acts proactively aiming at getting the entities of the other tiers and branches to adopt the e-PING, given the importance of information exchange among tiers and branches to improve efficiency and effectiveness of government performance, and to build electronic services directed to the society, and especially to the citizen.

In order to make e-PING adoption by state governments easier, ABEP is part of the e-PING coordination, working in collaboration to build a matrix of federal interests for information exchange.

5.5.3. Private Sector and Third Sector Organizations

e-PING foresees interaction with the Private Sector and with the Third Sector through mechanisms of Public Consultation, Requesting Comments, and Welcoming Suggestions.

All entities of that nature that participate in the bidding processes to provide products and services to the Federal Executive Branch shall meet e-PING specifications and recommendations.

Other ways for these institutions to participate in e-PING may be considered, provided that criteria be established to assure transparency and equal opportunities.

5.5.4. Citizen

Electronic government means, essentially, that the government will better meet the citizens' needs by using Technology, Information, and Communication resources. The e-PING architecture makes integration possible and makes services available in a complete, safe, and coherent manner, allowing the government to achieve higher levels of efficiency.

Government shall encourage society to express its opinion, to comment on, and to contribute with suggestions of innovations that may help to improve access to information and the rendering of its services. All e-PING dissemination and inter-relationship processes foresee active participation of the citizen and of society in general, in the process of building and managing the architecture.

Part II – Technical Specification of e-PING components

6. Interconnectivity

6.1. Interconnectivity: Technical Policies

The technical policies for interconnectivity are the following:

6.1.1. The APF agencies shall Interconnect by using IPv4, and plan their further migration to IPv6.

New hiring of services and network updates shall foresee support for the coexistence of IPv4 and IPv6 protocols, and for products that handle both protocols.

6.1.2. The e-mail systems shall use SMTP/MIME to carry messages. For the access of messages, POP3 and/or IMAP protocols shall be used, and the use of web interfaces is encouraged for electronic mail, also addressing, when necessary, security aspects.

6.1.3. The APF agencies must obey the federal government's policy on domain names, set out in Resolution no. 7, which may be accessed at the following electronic address:

https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm.

6.1.4. The DNS must be used to translate Internet domain names, converting them into IP addresses, and, inversely, converting IPs in domain names.

6.1.5. The FTP and/or HTTP protocols must be used to transfer files, addressing their functionalities to recover interruptions and security whenever necessary. To transfer files coming from Internet sites or pages, HTTP is preferred.

6.1.6. Whenever possible[1], web-based technology shall be used to replace previous stand-alone applications.

6.1.7. Web Service Technology is recommended to be used as the e-PING interoperability standard, therefore the Simple Object Access Protocol (SOAP) is adopted for interconnectivity in decentralized and/or distributed architectures.

6.2. Interconnectivity: Technical Specifications

Table 1 – Specifications for Interconnectivity – Messaging[2]

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Electronic mail boxes addresses	The rules applicable to electronic mail boxes names are set out in the document called "Individual-Work Mail Boxes in the federal government" available at: http://www.e.gov.br/correios/cp_individ.htm	**A**	
Electronic message delivery	To use electronic messaging products that use SMTP/MIME interfaces to send messages. Co-related RFCs: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 3676; RFC 2047; RFC 2231 (RFCs 2045, 2047 and 2183 updates); RFC 2183; RFC 4288; RFC 4289; RFC 3023 and RFC 2049.	**R**	

[1] There are products that can provide access to the legacy systems via browser, without needing to change these systems; usually, these products can provide direct access to the legacy screens or may be replaced by graphical interfaces (GUIs). One must pay attention if any such use has effect on security.

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

Component	Specification	Current Situation	Observations
Access to the mail box	Unless security requirements demand otherwise, the mail programs that offer easy access to mail shall, at least, handle POP3 for remote access to mail. Co-related RFC: RFC 1939 (updated by RFC 1957 and RFC 2449).	**T**	
	When additional features are needed, unless security requirements demand otherwise, mail programs that offer advanced access options to mail shall use IMAP - for remote access to the mail box. Co-related RFCs: RFC 2342; RFC 2910 (updated by RFC 3510); RFC 2971; RFC 3501; RFC 3502 and RFC 3503.	**R**	
Real Time Messaging	Instant Messaging and Presence Protocol (IMPP) models and requirements are set by RFC 2778 and RFC 2779.	**T**	
	Extensible Messaging and Presence Protocol (XMPP) model and requirements are set by RFC 3920 and RFC 3921.	**R**	
Short Message Service	The Short Message Service (SMS) must use the SMPP protocol, as set out by the SMS Forum http://www.smsforum.net	**R**	

Table 2 – Specifications for Interconnectivity – Network Infrastructure

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Delivery	TCP (RFC 793)	**A**	
	UDP (RFC 768) whenever necessary, subject to security limitations.	**A**	
LAN/WAN Intercommunication	IPv4 (RFC 791)	**A**	
	IPv6 (RFC 2460)	**E**	
Advanced traffic	Whenever necessary, network traffic may be optimized by using MPLS (RFC 3031), but it must have at least four classes of service.	**A**	
Quality of the service	Adopting architecture for differentiated services by using the Diffserv (RFC 2475).	**F**	
Metropolitan wireless network	IEEE 802.16, as set out by the WiMax Forum (http://www.wimaxforum.org) and in compliance with Anatel rules (http://www.anatel.gov.br).	**E**	
Local wireless network	IEEE 802.11 b/g, as established by the Wi-Fi Alliance (http://www.wi-fi.org) and in compliance with Anatel rules (http://www.anatel.gov.br).	**R**	

Table 3 – Specifications for Interconnectivity – Network Service

Component	Specification	Current situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Hypertext transfer protocol	To use HTTP/1.1 (RFC 2616).	**A**	
File transfer protocol	FTP (RFC 959 and RFC 2228) (data recovery and control connection) and HTTP (RFC 2616) for file transfer.	**R**	
Directory	LDAP v3 shall be used for general access to the directory, according to RFC 4510.	**A**	
Time synchronization	RFC 1305 IETF - Network Time Protocol - NTP version 3.0. RFC 4330 IETF - Simple Network Time Protocol - SNTP version 4.0.	**R**	
Domain Name Services	The DNS must be used to translate Internet domain names, according to RFC 1035. Yet, the Brazilian government's guidelines on domain names can be found in Resolution no. 7, of the Executive Committee for Electronic Government, at https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm In addition to those guidelines, the Brazilian Internet Steering Committee decided that domain names must comply with the guidelines set out by the Ministry of Planning, Budget, and Management, which is responsible for managing the GOV.BR domains. The singularities regarding the other tiers of government, such as the domains of the governments of the Federation Units, that include the state's acronym in the address, are addressed at http://registro.br/faq/faq1.html#12	**A**	
Signalling protocols	The use of the Session Initiation Protocol (SIP), defined by RFC 3261, to control the application layer (signalling) to create, change, and end sessions with one or more participants.	**R**	
Network management protocols	Use the SNMP, defined by the RFCs 3411 and 3418, for network management.	**F**	
Structured information exchange protocol on a decentralized and/or distributed platform	SOAP v1.2, as defined by the W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ SOAP protocols specifications can be found at http://www.w3.org/TR/soap12-part0/	**A**	

6.3. Electronic Message (E-mail)

The e-PING will adopt the following concepts:

Electronic Message Transfer

Electronic message transfer is defined as the interface between two mail systems.

Mail Box Access

Mail box access is defined as the interface between an e-mail client and an e-mail system.

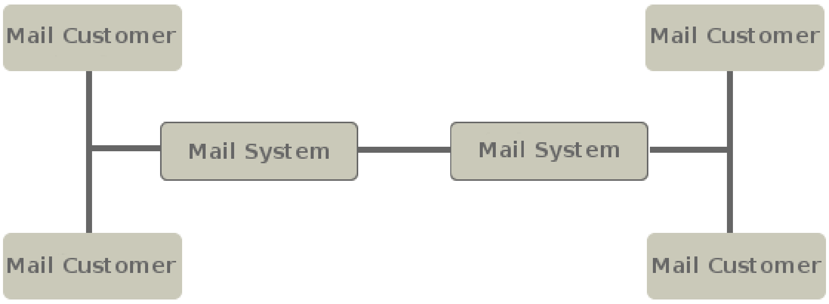

Figure 3 – Interfaces between E-mail clients and systems.

6.4. VPN

Virtual Private Network (VPN) is a private tunnel built on a private or public network infrastructure. Instead of using WAN, the Internet infrastructure is usually used.

Such usage as an infrastructure to connect private network hosts, is a good solution in terms of costs, but not in terms of privacy, for the data in transit can be read by any equipment, however needing the use of a VPN.

The virtual tunnels carry encrypted data over public or private networks, creating a safe virtual channel through these networks. In order to do so, tunneling protocols are used.

The devices responsible for the VPN management must be capable of assuring privacy, integrity and data authenticity.

The specifications for the VPN are presented under the segment on security.

6.5. Peer-to-peer Networks

Peer-to-Peer (P2P) are distributed systems that consist of interconnected nodes, capable of self-organizing themselves in network topologies, with the purpose of sharing resources, such as processing, storage and band width, capable of adjusting to flaws and to accommodate transitioning populations of nodes, while maintaining connectivity and acceptable performance, without depending on intermediation or support from a central authority (server).

Although P2P systems can contribute to the sharing of resources and broad scale collaboration, with decentralized control and loose coupling, they are still susceptible to various security problems, thus making it impossible to systematically use P2P networks. This topic will be addressed later.

7. Security

7.1. Security: Technical Policies

7.1.1. Government data, information and information systems must be protected against threats in order to reduce risks and assure integrity, confidentiality and availability.

7.1.2. The data and information must be kept with the same degree of protection, regardless of the means in which they are being processed, stored, or transferred.

7.1.3. Sensible information moving through insecure networks, including the wireless networks, must be encrypted appropriately, according to the security components specified in this document.

7.1.4. Security requirements for information, services and infrastructure must be identified and treated according to the classification of the information, levels of service as defined, and the outcomes of risk analyses.

7.1.5. Security must be approached in a preventive manner. For systems that support critical processes, continuity plans shall be designed, to address the residual risks and aiming at meeting the minimum levels of production.

7.1.6. Security is a process that must be included in all stages of the cycle of developing a system.

7.1.7. The systems must maintain historical records (logs) for purposes of audits and legal evidence, and it is very important to adopt a centralized time synchronism system, and mechanisms to guarantee authenticity of the stored records should be used, with a digital signature, if possible.

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

7.1.9. For metropolitan wireless networks we recommend that random figures be adopted for the security codes, as well as different identifications for each service, and limitation on the life span of the authorization keys.

7.1.10. The use of cryptography and digital certification to protect traffic, data storage, access control, digital signature and code signatures, must comply with the rules set out by the ICP-Brazil.

7.1.11. The documents regarding the systems, security controls and environment topologies must be kept updated and protected.

7.1.12. The users must know about their responsibilities towards security and must be trained to carry out the necessary tasks, and to correctly use the means of access.

7.1.13. The APF agencies, with aim at improving security, must refer to rules: NBR ISO/IEC 27002:2005 - Code of practice for information security management, BR ISO/IEC 27001:2006 – Information Security Management System, NBR ISO/IEC 15999-1:2007, and 15999-2:2008 – Business Continuity Management, and NBR ISO/IEC 27005:2008 – Information Security Risk Management.

7.2. Security: Technical Specifications

Table 4 – Security Specifications– IP

Component	Specification	Current situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Data transfer on insecure networks through protocols HTTP, LDAP, IMAP, POP3, Telnet.	TLS – Transport Layer Security, RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt). If necessary, the TLS v1 protocol can emulate the SSL v3. HTTP on TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) And being able to implement the following encryption algorithms: - Algorithms to exchange session keys during handshake: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - Algorithms to set the encryption key: RC4, IDEA, 3DES, AES; - Algorithms to implement the hash functions to set MAC: SHA-256 or SHA-512. - Type of digital certification - X.509 v3 - ICP-Brasil, http://www.iti.gov.br SASL - Simple Authentication and Security Layer, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt).	**R**	
Network security IPv4	IPSec Authentication Header RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) and RFC 4835 (http://www.ietf.org/rfc/rfc4835.txt) to authenticate the IP encapsulation. IKE – Internet Key Exchange, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), to be used whenever needed to negotiate security associations between two entities to exchange key material. ESP – Encapsulating Security Payload, RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) Requirement for VPN – Virtual Private Network.	**A**	
IPv4 network security for application protocols	O S/MIME v3,RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) shall be used when deemed appropriate to secure general government messages.	**A**	

Component	Specification	Current situation	Observations
IPv6 network security on the network layer	IPv6 as described in RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt) represents native security implementations to the protocol. The IPv6 specifications referred to two security mechanisms: AH *Authentication Header* RFC 4302 (http://www.ietf.org/rfc/rfc4302.txt) or IP authentication, and IP encapsulation security, ESP (Encrypted Security Payload) RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt).	**R**	

Table 5 – Security Specifications – Electronic Mail

Component	Specifications	Current Situation	Observations

	A = Adopted
	R = Recommended for consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Mail Box Access	The access to e-mail boxes shall be through the electronic mail software client that is being used, because of the native security features. Whenever the specific client cannot be used or it is necessary to access the mail box through insecure networks (Internet, for example), the HTTPS shall be used, according to the security standards described in RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), that addresses the use of TLS with IMAP, POP3 and ACAP.	**A**	
E-mail content	The S/MIME V3 shall be used whenever deemed appropriate for the security of general government messages. That includes RFC 3369 (http://www.ietf.org/rfc/rfc3369.txt), RFC 3370 (http://www.ietf.org/rfc/rfc3370.txt), RFC 2631 (http://www.ietf.org/rfc/rfc2631.txt), RFC 3850 (http://www.ietf.org/rfc/rfc3850.txt), RFC 3851 (http://www.ietf.org/rfc/rfc3851.txt) and RFC 3852 (http://www.ietf.org/rfc/rfc3852.txt).	**A**	
E-mail transfer	Use SPF (Sender Policy Framework) as set out in RFC 4408 (http://www.ietf.org/rfc/rfc4408.txt).	**R**	
Signature	Use the ICP-Brasil (PKI) standard certificate for e-mail signatures, whenever required, in accordance with Decree 3.996 of 31 October, 2001.	**A**	

Table 6 – Security Specifications – Encryption

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Encryption algorithm	3DES or AES	**R**	
Signature/hashing algorithms	SHA-256 or SHA-512	**R**	The systems must be capable of supporting hash MD5 algorithm with RSA, to assure compatibility with previous implementations.
Signature/hashing algorithms	SHA-224 or SHA-238	**E**	Considering that they were included in the Final Report of the Encryption Working Group I, created by the Cabinet for Institutional Security of the Presidency of the Republic, however, have not yet become a rule within the Federal Public Administration.
Encryption content/session transport key	RSA	**A**	
Encryption algorithms over elliptic curve	ECMQV and ECDH, both for key agreement, ECDSA, for digital signatures and ECIES for encryption and secure encryption key transport. The use of these algorithms is still subject to regulation and normatization by ICP-Brasil regarding its security requirements.	**E**	

Component	Specification	Current Situation	Observations
Security requirements for encryption modules	FIPS 140-2 – Minimum requirements for private key and digital certificate storage solutions issued under the scope of ICP – Brasil, that use both software as well as hardware devices, like a token or smart card. To adopt the standard: a. Follow, at least, the standard's security rules set out for level 1 or 2; b. Follow, at least, the security rules set out for level 2, of the FIPS 140-1 or 2 standard, for tamper evidence verification.	**R**	

Table 7 – Security Specifications – System Development

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

XML Signatures	XML (XMLsig) signature Syntax and Processing as set out by the W3C http://www.w3.org/TR/xmldsig-core/	**A**	
XML Encryption	XML (XMLenc) Encryptions Syntax and Processing, as set out by W3C http://www.w3.org/TR/xmlenc-core/	**R**	
XML Signature and Encryption	Decryption Transform for XML Signature as set out by the W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Main XML managements when using a PKI environment	XML – Key Management Specification (XKMS 2.0) as set out by the W3C http://www.w3.org/TR/xkms2/	**R**	
XML Access authentication and authorization	SAML – as set out by OASIS when using an ICP environment http://www.oasis-open.org/committees/security/index.shtml	**R**	
Identity verification	WS-Security 1.1 – set of Standards to provide message integrity and confidentiality to SOAP messaging. (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf). WS-Trust 1.3 defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and for broker trust relationships. (http://docs.oasis-open.org/ws-sx/ws-trust/200512).	**R**	The previous component (SAML) maybe combined to this one after Under Review.
Browser	Only use cookies upon the user's agreement. Resolution no. 7 of the Executive Committee for Electronic Government (Chapter II, Art.7).	**A**	

Table 8 – Security Specifications – Network Services

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Directory	Administrative Ruling No. 2, of 3 October, 2002 – Published in the Official Gazette, on 4, October, 2002. Section 1, Page 85. LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt). LDAP v3 extension for TLS RFC2830 (http://www.ietf.org/rfc/rfc2830.txt).	**R**	
DNSSEC	Resolution no. 7 of 07/29/2002 – Executive Committee for Electronic Government. Security Practices for Internet Network Administrators Brazilian National Computer Emergency Response Team – CERT.BR http://www.cert.br/docs/seg-adm-redes/seg-adm-chklist.pdf Version 1.2, 16 of May, 2003.	**R**	
Secure File Transfer	HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt).	**R**	
Secure File Transfer	SSH FTP	**E**	The documents are still in the format of working drafts.
Secure File Transfer	Securing FTP with TLS, RFC 4217 http://www.faqs.org/rfcs/rfc4217.html and RFC 2246 http://www.faqs.org/rfcs/rfc2246.html	**E**	
Instant message	RFC 2778 (http://www.ietf.org/rfc/rfc2778.txt), RFC 3261 (http://www.ietf.org/rfc/rfc3261.txt), RFC 3262 (http://www.ietf.org/rfc/rfc3262.txt), RFC 3263 (http://www.ietf.org/rfc/rfc3263.txt), RFC 3264 (http://www.ietf.org/rfc/rfc3264.txt) and RFC (3265. http://www.ietf.org/rfc/rfc3265.txt).	**E**	
Time Synchronization	RFC 2030 IETF- Simple Network Time Protocol - SNTP version 4.0 (http://www.ietf.org/rfc/rfc2030.txt).	**E**	
Time-stamping	RFC 3628 TSAs - Policy Requirements for Time-Stamping Authorities (http://www.ietf.org/rfc/rfc3628.txt), Time-Stamp Protocol, RFC 3161 ETSI TS101861 (Time-Stamping Profile) (http://www.ietf.org/rfc/rfc3161.txt).	**R**	Time-stamping services must comply with the resolutions and other rules set out by ICP-Brasil.

Table 9 – Security Specifications – Wireless Networks

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

MAN[3] wireless 802.16-2004[4] 802.16.2-2004[5] 802.16e[6] and 802.16f[7]	Use PKM-EAP (Privacy Key Management - Extensible Authentication Protocol) with: • EAP – TLS or TTLS; • AES[8] (Advanced Encryption Standard).	**E**	
Wireless LAN 802.11	Use WPA2 (Wi-Fi Protect Access).	**R**	

Table 10 – Security Specifications – Evidence Collection, Treatment and Archiving

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Under Transition
	E = Under Review
	F = For Future Consideration		

Keep records	Guidelines for Evidence Collection and Archiving, RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt).	**R**	
Security Incident Response	Expectations for Computer Security Incident Response, RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt).	**R**	
Forensic Computer Science	Guide to Integrating Forensic Techniques into Incident Response – NIST - Special Publication 800-86 – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	**A**	

[3] The 802.16 is defined by IEEE as a technological interface for wireless metropolitan area networks or WMAN (Wireless Metropolitan Access Network).

[4] http://standards.ieee.org/getieee802/download/802.16-2004.pdf.

[5] http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf.

[6] http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.

[7] http://standards.ieee.org/getieee802/download/802.16f-2005.pdf.

[8] http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf.

8. Means of Access

8.1. Means of Access: Technical Policies

The technical policies to give access to the federal government electronic services to society in general – citizens, other government tiers, other branches, civil servers, private enterprises and other institutions - are:

8.1.1. The government information systems must be designed in compliance with the Brazilian legislation, and providing accessibility resources to citizens with special needs, minority ethnic groups, and those at risk of social or digital exclusion. The provision of services over the counter must be considered thoroughly, in order to allow that the benefits that originate from the use of electronic government services be extended to the population strand that cannot have direct access to these services through the usual devices.

8.1.2. Information systems that provide electronic government services:

- when using the Internet as a means of communication, and work stations as access devices, they will be preferably developed to provide access to its information by using web communication technologies and protocols based on browser;
- when using other access devices, such as, for example, cellular phones, digital television, and smart cards, they may use other interfaces, aside from the web browsers;
- shall be designed to provide electronic government services to the users through various means of access;
- shall foresee gradual replacement of the “login/password” systematic for user authentication through digital certification, preferably based on smart cards or tokens, according to the standards set out by the ICP – Brasil (reference: http://www.icpbrasil.gov.br/);
- new services shall be created, already with user authentication through the ICP-Brasil digital certificates;
- in this version, e-PING addresses the following means of access:
  - Work Stations;
  - Smart Cards, Tokens, and other Cards;
  - Mobility;
  - Digital TV.

8.1.3. The government information systems created to support a certain access device shall, mandatorily, comply with the specifications published in the e-PING concerning that device.

8.1.4. All government information systems that provide electronic services must be capable of using the Internet as a means of access, either directly or through third party services.

8.1.5. The development of electronic government services shall be aimed at providing service to users that do not have access to the most recent technologies available in the market. On the other hand, the service to those users that have special needs must also be addressed, which demands more sophisticated and specific resources. In order to address all of these needs, the recommendations within the Accessibility Model for e- Gov (e-MAG) shall be considered.[(9)].

8.1.6. Whenever the Internet is used as a means of communication, the government information systems shall be designed to allow that the most amount of information is able to be worked upon based on the browsers that comply with the minimum standards set out by the technical specifications foreseen in section 8.2. In addition, e-PING recommends that every electronic government service clearly specifies, on its home page, the minimum browser versions that support the services. While complying with that standard, exceptions that involve security issues in treating information shall be considered.

8.1.7. Whenever the Internet is used as a means of communication, additional middleware or plug-ins may be used, if there is no other technically feasible alternative, to optimize the browser’s functionality at the work stations. In that case, the additional software shall be offered without having to pay for the license, and must comply with all the technical specifications, as listed in the e-PING. Plus, it must be put available within a secure environment, sustained by the government

[9] BRAZIL. Ministry of Planning, Budget and Management. Accessibility recommendations for the creation and adjustment of the Brazilian Government content to the Internet. Version 2.0. Brasília, 2005. Available: (http://www.governoeletronico.gov.br/emag/). Accessed on: 13/07/2006.

agency responsible for its application.

8.1.8. The electronic government services shall be designed to assure the users with content authenticity by issuing a digital certificate, according to the ICP-Brasil standards. Reference: http://www.icpbrasil.gov.br/. In that regard, all web sites must mandatorily use “https” instead of “http”.

8.1.9. The society’s need, along with the government’s possibility to develop and implement electronic services, shall underlie the definition of technical specifications required by the means of access that are available. Content management techniques and technologies that allow for the adjustment of devices, so that they can bear electronic government services, may be used to ease the access through a minimum standard web browser (according to topic 3. General Policies) and to make the use of public booths, service counters and Customer Service Center feasible (such as Telecenters).

8.1.10. The federal government’s information systems shall foresee, whenever necessary and when technically and economically feasible, the setting up of adapters that allow for web access to the information on electronic services for different environments, with adequate response times and reduced costs.

These adaptors may be used to filter, convert, and reformat dynamically the web content, in as to adapt to the demands and display capacities of the access device. They may, yet, allow a web page content to be changed, based on XML, XSL data protocols, user preferences and network and access devices configuration.

These adapters may also be used as an alternative way to provide access to ethnical minorities and persons visually impaired (for example: by using text translators, bigger fonts and graphs, audio, etc.). Such possibilities are addressed by Resolution no. 7 of the Executive Committee for Electronic Government.

Reference:

https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES07-02web.htm

8.1.11. XML files shall be preferred, in order to ease interoperability among the electronic government services.

8.1.12. The electronic government services that give its users access to documents shall do so by displaying, on the same link that leads to the document, clear information regarding its source, version, publication date and format. Date of publication is to be understood as the date in which the document was published in the official gazette, whenever that is required; and, for others, the date it is made available on the website. Other information regarding the document, such as author, editor, data topica or others that are relevant, shall be available in the field for properties of the document itself.

8.2. Means of Access: Technical Specifications for Work Stations

To prepare drafts or papers that need to be created in collaboration by more than one person and/or agency, the formats foreseen in Table 11 can be used.

However, for the final version of the document, to be sent to other agencies or even digitally filed, use of the pdf/a format is recommended. Documents that require integrity and/or authorship assurance, besides being in a pdf/a format, they shall be digitally signed by their author, using the ICP-Brasil certificate.

Referring to the documents that generate the format of the files cited in Table 11 has the sole purpose of identifying a **minimum reference** based on which e-gov services shall exchange information, to be prepared to receive or send files in **the same or in later versions.**

Table 11 – Specifications on Means of Access – Work Stations

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Browsers	See topic 3. General Policies.	**E**	
Character sets and alphabets	UNICODE standard version 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	**R**	
Hypertext interchange format	HTML version 4.01 (.html or .htm), generated according to W3C[10] specifications.	**A**	
	XHTML versions 1.0 or 1.1 (.xhtml), generated according to W3C[11]specifications.	**A**	
	XML versions 1.0 or 1.1 (.xml), generated according to W3C[12]specifications.	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl ou .mht)[13].	**T**	
Document file types	XML versions 1.0 or 1.1 (.xml), or in XSL (.xsl) format (optional) generated according to W3C[14] specifications.	**R**	
	Open Document (.odt), generated according to ISO/IEC 26300[15]standard specifications.	**A**	
	OpenOffice.org XML (.sxw), generated in OpenOffice version 1.0 format.	**T**	
	Rich Text Format (.rtf).	**T**	
	PDF (.pdf) generated in 1.3 version format	**T**	
	PDF open version PDF/A[16].	**R**	
	Pure text (.txt).	**A**	
	HTML version 4.01 (.html or .htm), generated according to W3C specifications.	**R**	
	Microsoft Word document (.doc), generated in MS Office format up to version 2000.	**T**	

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

[11] *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/.

[12] *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-xml11-20040204/.

[13] *Mime Enscapsulation of Aggregate HTML Documents*.

[14] *Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001*. Available at: http://www.w3.org/TR/xsl/.

[15] *Open Document Format for Office Applications (OpenDocument)* v1.0 -ISO/IEC 26300 Standard. Available at: http://www.iso.org/.

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

Component	Specification	Current Situation	Observations
Spreadsheet file types	Open Document (.ods), generated according to ISO/IEC 26300 Standard specifications.	**A**	
	OpenOffice.org XML (.sxc). generated in Open Office version 1.0 format.	**T**	
	MS Excel spreadsheet (.xls), generated in MS Office format up to version 2000.	**T**	
Presentation file types	Open Document (.odp), generated according to ISO/IEC 26300 standard specifications.	**A**	
	OpenOffice.org XML (.sxi), generated in Open Office version 1.0 format.	**T**	
	HTML (.html or .htm), generated according to W3C specifications.	**R**	
	MS Power Point Presentation (.ppt), generated in MS Office format up to version 2000.	**T**	
“Database” file types for work stations	XML versions 1.0 or 1.1 (.xml)	**R**	For plain text (txt) and csv, the layouts of the fields must mandatorily be included, to allow it to be treated.
	MySQL Database (.myd, .myi), generated in MySQL formats, version 4.0 or higher.	**R**	
	Pure Text (.txt)	**A**	
	Pure text (.csv) – comma-separated values	**A**	
	Base files (.odb), generated in the BrOffice.org (or OpenOffice.org) format version 2.0 or higher.	**R**	
	MS Access file (.mdb), generated in the MS Office format, up to version 2000.	**T**	
Exchange of graphic information and static images	PNG (.png), generated according to W3C[17] specifications – ISO/IEC 15948:2003 (E).	**A**	
	TIFF (.tif)[18].	**R**	
	SVG (.svg), generated according to W3C[19] specifications.	**R**	
	JPEG File Interchange Format (.jpeg, .jpg or .jfif)[20].	**R**	
	Open Document (.odg), generated according to ISO/IEC 26300 standard specifications.	**A**	
	OpenOffice.org XML (.sxd), generated in Open Office format version 1.0.	**T**	
	XCF (.xcf), generated in GIMP version 1.0 or higher.	**R**	
	BMP (.bmp).	**T**	
	GIF (.gif), generated according to GIF87a and GIF89a[21] specifications.	**T**	
	Image Corel Photo-Paint (.cpt), generated in Corel Draw suite format up to version 7.	**T**	
	Photoshop Image(.psd), generated in Adobe Photoshop format up to version 4.	**T**	

[17] *Portable Network Graphics (PNG) Specification (Second Edition). W3C Recommendation 10 November 2003.*

Component	Specification	Current Situation	Observations
Vector graphics	SVG (.svg), generated according to W3C specifications.	**R**	
	Open Document (.odg), generated according to ISO/IEC 26300 Standard specifications.	**R**	
	OpenOffice.org XML (.sxd), generated in Open Office format version 1.0.	**T**	
	Corel Draw Graphics (.cdr), generated in format up to version 7.	**T**	
	MSX (.msx), generated in Corel Draw suíte format up to version 7.	**T**	
	MS Visio Graphiscs.vss or .vsd), generated in format up to version 2000.	**T**	
	Windows Metafile (.wmf).	**T**	
Specification of Animation Standards	SVG (.svg), generated according to W3C files.	**R**	
	GIF (.gif), generated according to GIF89a specification.	**T**	
	Shockwave Flash (.swf), generated in Macromedia Flash up to version 4, ofMacromedia Shockwave version 1.	**T**	

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/. Access on: 7 December, 2005.

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

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

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

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

Component	Specification	Current Situation	Observations
Audio and video type files	.mpg	**R**	
	Audio and video MPEG-4, Part 14 (.mp4)[22]	**R**	
	MIDI (.mid)[23]	**R**	
	Audio Ogg Vorbis I (.ogg)[24]	**R**	
	Audio-Video Interleaved (.avi), with Xvid coding.	**R**	
	Audio-Video Interleaved (.avi), with divX coding.	**T**	
	Audio MPEG-1, Audio Layer 3 (.mp3)[25]	**T**	
	Real Media (.rm or .rmm), generated in Real Audio Media Player applications, up to version 8.	**T**	
	Real Audio (.ra or .ram), generated in Real Audio Media Player applications, up to version 8.	**T**	
	WAVE (.wav)	**T**	
	Shockwave Flash (.swf), generated in Macromedia Flash format, up to version 4 or in Macromedia Shockwave, version 1.	**T**	
	Windows Media Video (.wmv), generated in Windows Media Player format, up to version 6.4.	**T**	
	Windows Media Audio (.wma), generated in Windows Media Player format, up to version 6.4.	**T**	
	QuickTime (.mov), generated in Apple Quicktime format, up to version 6.	**T**	
	QuickTime (.qt), generated in Apple Quicktime format, up to version 6.	**T**	
Compressing files of general use	ZIP (.zip).	**R**	
	GNU ZIP (.gz).	**R**	
	TAR (.tar) package.	**R**	
	Compressed TAR package (.tgz or .tar.gz).	**R**	
	BZIP2 (.bz2).	**R**	
	Compressed TAR package with BZIP2 (.tar.bz2).	**R**	
	MS Cabinet (.cab).	**T**	

[22] *ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file format.*

[23] Musical Instrument Digital Interface, according to the specification *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., Nov. 2001. Available at: http://www.midi.org/about-midi/specinfo.shtml. Access on: 30 May. 2007.

[24] Xiph.Org Foundation. Specification available at: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.

[25] *ISO/IEC 11172-3:1993 - Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5Mbit/s - Part 3: Audio.*
ISO/IEC 11172-3:1993/Cor 1:1996.

Component	Specification	Current Situation	Observations
Geospatial information – file standards for exchange among work stations	GML version 1.0 or higher[26].	**A**	Indicated for complex vectorial structures, involving geographic references, such as polygons, points, lines, surfaces, collections and numerical or text features with no limit on the number of characters.
	ShapeFile[27].	**A**	Indicated for vectorial structures limited to lines, points and polygons, which text features are not more than 256 characters. It may also store M and Z dimensions.
	GeoTIFF[28].	**A**	Indicated for matrix structures limited to pixel matrixes.
	SFS.	**E**	SFS (Simple Features Interface Standard) is an OGC standard (http://www.opengeospatial.org/standards/sfa) that defines how the applications will store (create, update and exclude) and access geographic features In relational or object-relational databases. OpenGIS Simple Features are spatial features described using data elements, such as points, lines and polygons.
Extended programming (Plug-ins)	Subjects for further consideration.	**F**	

[26] *Geography Markup Language*. Specifications available at: http://www.opengeospatial.org/standards.

[27] *ESRI Shapefile Technical Description*. Available at: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.

[28] *GeoTIFF Format Especification*. Available at: http://remotesensing.org/geotiff/geotiff.html.

8.3. Means of Access: Technical Specifications for Tokens, Smart Cards and Cards in General.

The first specifications on smart cards and tokens were added on to by the conclusions of the ICP-Brasil Working Group (Administrative Ruling no. 33, of 08 April, 2003), based on the ISO/IEC (7816 parts 1 to 6) family.

The group's conclusions were also used to prepare the ITI's Manual on Technical Conducts, documents that sets out the technical requirements to be complied with in the accrediting processes of smart cards and cryptographic tokens, within the scope of ICP-Brasil. The specifications contained in those manuals were also used to design this reference document, specifically regarding cryptographic devices.

The accreditation of digital certification systems and equipments in the scope of ICP-Brasil was created by Resolution 36 of the ICP-Brasil Steering Committee, of 21 October, 2004; whereas the National Institute for Information Technology (ITI) was made responsible for driving the process, while the Laboratories for Studies and Auditing (LEA), created by Resolution 36 were responsible for the conformity trials.

According to that Resolution, the media that store the digital certificates and the respective readers, plus the systems and equipment needed to carry out digital certification, shall follow minimum standards and technical specifications, in order to assure interoperability and reliability of the information security resources used by them.

According to the regulation, the following are subject to accreditation: media, such as cryptographic tokens and smart cards; systems, such as for electronic signature, signature authentication, certifying authorities and records; and equipment, such as the HSM, time synchronization and time-stamp, among others. For the products accredited through this process, a conformity report will be issued, and an accreditations stamp, plus the corresponding identification number will be placed on them.

It is important to note that the data stored in a certain smart cards or tokens cannot be protected by any type of licensing the doesn't allow it to be read by another software, aside from that of the supplier of that smart card or token.

Standardization of these devices will make it easier for Brazil to be part of international agreements related to digital certification, in addition to complying with the Electronic Government Interoperability Standards – e-PING and helping to expand the use of certification for, among others, it may help to reduce the price of this technological solution.

Within the e-PING context, other standards were also assessed: a ISO/IEC 7810, which defines the physical properties, such as flexibility, resistance to temperature, and dimensions for three different types of card format (ID-1, ID-2 and ID-3); the PC/SC Workgroup standard, and the FIPS-140 standardization for security, from the National Institute of Standards and Technology (http://www.nist.gov).

These basic standards were used by the ICP-Brasil Working Group with the purpose of obtaining better interoperability within the universe of access devices such as smart cards and tokens, in other words, devices that handle digital certificates. In addition, the ISO rules for magnetic traditional cards and more fancy expensive optical cards.

For future e-PING versions, a minimum agenda shall be established, to revise the whole set of specifications and map/identify, within the federal government, the government plans and activities using any type of smart card, and that, consequently, must be addressed. An exhaustive research shall be carried out to provide subsidies to include, or not, in e-PING, the standards of the cards effectively used by the government agencies. For example, we may refer to the embossed smart cards (ISO/IEC 7811) that are not addressed in this version. In case this research finds that there is intensive use of that type of device, the feasibility of including it into the e-PING set of specifications will be assessed.

Also, for future version, the standards typically directed to the European community will be deeply analyzed. Such as the e-Europe, the *Open Smart Card Infrastructure for Europe* – version 2" that assimilates the technology of contactless cards, present in ISO/IEC 14443. The same goes for the CALYPSO standard (Fourth European Research and Technological Development Framework Program) for contactless card (or ticket) systems, used in public transportation. Standardizations, patent systems and licensing that may eventually exist shall be evaluated.

Table 12 – Specifications on Means of Access – Intelligent Cards, Tokens, and Cards in general.

Component	Specification	Current Situation	Applicability	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration			

Data definition	ITI Technical Conduct Volumes – Volume 1 (http://www.lea.gov.br/).	**A**	All cards and tokens that handle digital certificates.	
	Identification Cards **ISO/IEC 7816-6**. Integrated Circuit Cards with contacts Part 6: Interindustry data elements.	**A**	All card types.	According to the choice of the ICP-Brasil Working Group.
	Identification Cards **ISO/IEC 7812-1**. Identification of Issuers Part 1: Numbering system.	**R**	All card types.	
	Financial Transaction Cards **ISO 9992-2**. Messages between the integrated circuit card and the card accepting device Part 2: Functions, messages (commands and responses), data elements and structures.	**F**	All card types.	
	Identification Cards Systems. **BS EN 1546-3** – Inter-sector electronic purse - Part 3: Data elements and Exchange. Identification Cards Systems **BS EN 1546-4** – Inter-sector electronic purse - Part 4: Data objects.	**F**	All card types.	The current edition was published in July, 1999. The current edition was published in August, 1999.

Component	Specification	Current Situation	Applicability	Observations
Applications, including multi-applications	Identification cards **ISO/IEC 7816-4** Part 4: Interindustry commands for interchange.	**A**	Integrated circuit(s) cards with contacts.	This sets out the file structures, secure messaging for file access, card application startup, and logical channels for use where the card can have more than one virtual communications channel active. Application specific commands are not described, and therefore the standard treats command codes as application specific where they are not defined in this part.
	Identification Cards **ISO/IEC 7816-5** Part 5: Numbering system and registration procedure for application identifiers.	**R**		
	ISO/IEC 7816-7 Part 7: Interindustry commands for Structured Card Query Language (SCQL);	**R**		According to the choice of the ICP-Brasil Working Group. The current edition was published in June, 1994. There is also an amendment ISO/IEC 7816-5/AM1 Registered Application Provider Identifiers (RDIs) published in December, 1996.
	ISO/IEC 7816-11 Part 11: Structure for dynamic handling of multiple applications in integrated circuit cards.	**R**		
	Identification Cards **ISO/IEC 7813** – Financial Transaction Cards.	**R**	Financial Cards.	
	Identification Cards – identification of issuers **ISO/IEC 7812-2** Parte 2: Application and registration procedures.	**R**	All card types.	
	Identification Cards **ISO/IEC 15693-4** – Contactless integrated circuit(s) cards {Vicinity Integrated Circuit(s) Cards (VICC)} Part 4: Application/issuers registration.	**R**	Proximity integrated circuit cards.	
	Identification card systems - **EN 1332-1**:1999 – Man-machine interface – Part 1: Design principles for the user interface. Identification card systems **EN 1332-4:**1999 – Man-machine interface – Part 4: Coding of user requirements for people with special needs.	**R**	All card types.	

Component	Specification	Current Situation	Applicability	Observations
Electrical	Identification Cards **ISO/IEC 7816-10** – Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards. **ISO/IEC 7816—12** Part 12: USB Interface.	**R**	Integrated circuit(s) cards with contacts.	
	Identification Cards **ISO/IEC 14443-2** – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface.	**R**	Proximity integrated circuit cards.	This part defines the radio frequency interface, and contains two quite different modulation techniques (Types A and B) for data communication between card and terminal. Type A is based on the Philips Mifare technology (widely licensed to other manufacturers). Type B is a new concept. These two types run in parallel through this part of the standard and through Part 3. In addition, some Type A specific items appear in Part 4.
	Identification Cards **ISO/IEC 10536-3** Contactless integrated circuit(s) cards {Close Coupling Integrated Circuit(s) Cards (CICC)} Part 3: Electronic signals and reset procedures.	**F**	Close Coupling Integrated Circuit(s) Cards.	
	Identification Cards **ISO/IEC 15693-2** Contactless integrated circuit(s) cards. Proximity Cards {Vicinity Integrated Circuit*(s)* Cards (VICC)}: Part 2: Air interface and initialization;	**R**	Contactless proximity integrated circuit cards.	
Communication Protocols	Identification Cards **ISO/IEC 7816-3** Part 3: Electronic signals and transmission protocols.	**R**	Integrated circuit(s) cards with contacts.	According to the choice of the ICP-Brasil Working Group.
	Identification Cards **ISO/IEC 14443-3** - Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anti-collision.	**R**	Proximity integrated circuit cards.	This part continues the Type A and Type B duopoly, defining card initialisation, anti-collision procedures and basic communications protocols. Anti-collision procedures are the methods used to identify and select one card when several cards are active within the RF field of the terminal.
	Identification Cards **ISO/IEC**			This contains higher level

Component	Specification	Current Situation	Applicability	Observations
	14443-4 – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission Protocols.			(message level) data transmission protocol information, equivalent to ISO/IEC 7816's T=1 protocol, and is a bridge across to ISO 7816-4. For Type A cards only, ISO/IEC 14443-4 includes a protocol initialization procedure.
	Identification Cards **ISO/IEC 15693-3** – Contactless integrated circuit(s) cards – Vicinity cards - Part 3: Anti-collision and transmission protocol.	R	Contactless proximity integrated circuit cards.	
	Financial Transaction Card Originated Messages - **ISO 8583** – Interchange message specifications.	F	All card types.	
	Financial transaction cards **ISO 9992-1** – Messages between the integrated circuit card and the card accepting device -- Part 1: Concepts and structures; ISO 9992-2 Part 2: Functions, messages (commands and responses), data elements and structures.	F	All card types.	
	Financial transaction cards **ISO 10202-2** Security architecture of financial transaction systems using integrated circuit cards -- Part 2: Transaction process; ISO 10202-6 **Part 6: Cardholder verification.**	R	All card types.	
	Identification Cards **ISO/IEC 10536-4** Contactless Integrated Circuit(s) Cards {Close Coupling Integrated Circuit(s) Cards (CCIC)}. Part 4: Answer to reset and transmission protocols.	F	Close Coupling Integrated Circuit(s) Cards.	
Physical - Physical and interface standards cover the card dimensions; location and layout of contacts. Location and layout of contacts.	**Physical characteristics** Identification Cards **ISO/IEC 7810**	R	All contact and combination cards	To ensure that they can be read in a standard reader, all cards should be in ID-1 format as defined in this standard.
	Magnetic Card **ISO/IEC 7811**, parts 2, 4 and 5: define the magnetic stripe's position and coding.	R	All cards with magnetic stripe.	
	Optical memory cards **ISO/IEC 11693** and **11694.**	F	Optical cards.	Cards capable of holding many megabytes of data.
	Identification Cards **ISO/IEC 7816-1** Part 1: Physical characteristics Identification Cards	A	Integrated circuit(s) cards with contacts.	This part supplements ISO/IEC 7810, setting out the particular physical characteristics of IC

Component	Specification	Current Situation	Applicability	Observations
	ISO/IEC 15693-1 - Contactless integrated circuit(s) cards – Vicinity cards - Part 1: Physical characteristics. Identification Cards **ISO/IEC 7816-2** – Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts.			cards with contacts. According to the choice of the ICP-Brasil Working Group and the ITI Manual on Technical Conducts – Volume I.
	Identification Cards **ISO/IEC 14443-1** – Contactless integrated circuit (s) cards -- Proximity cards -- Part 1: Physical characteristics.	**R**	Proximity integrated circuit cards.	This part adds on to the physical characteristics defined in ISO/IEC 7810.
	Identification Cards **ISO/IEC 15693-1** – Contactless integrated circuit (s) cards -- Proximity cards -- Part 1: Physical characteristics. This part of the **ISO/IEC 15693** foi was published on 07/15/2000.	**R**	Contactless proximity integrated circuit cards.	This part of the **ISO/IEC 15693** was published on 07/15/2000.
	Identification Cards **ISO/IEC 10536-1** – Contactless integrated circuit (s) cards Part 1: Physical characteristics; **ISO/IEC 10536-2** Part 2: Dimensions and location of coupling areas.	**F**	Close Coupling Integrated Circuit(s) Cards.	
	Tactile identifiers. Identification card systems **BS EN 1332-2** – Man- machine interface Part 2: Dimensions and location of a tactile identifier for ID-1 cards.	**F**	Where embossing is not used and there is a requirement for the user to present the card in a particular orientation, a tactile identifier should be provided as an aid to those with impaired vision.	Certain card personalization equipment, unless modified, may have difficulty processing cards with tactile identifiers of the 'notch' type. Agreement must therefore be reached with the personalization service provider to use such cards.

Component	Specification	Current Situation	Applicability	Observations
Security	Identification Cards **ISO/IEC 7816-8** – Integrated circuit(s) cards with contacts Part 8: Security inter industry commands ISO/IEC 7816-9 Part 9: Additional inter industry commands and security attributes. Identification Cards **ISO/IEC 7816-11** – Integrated circuit (s) cards with contacts - Part 11: Personal verification through biometric methods. Identification Cards **ISO/IEC 7816-15** – Integrated circuit (s) cards with contacts - Parte 15: Cryptographic information application on IC cards.	**A**	Integrated circuit(s) cards with contacts.	
	Financial transaction cards **ISO 10202** Security architecture of financial transaction systems using integrated circuit cards Part 1: Card life cycle; Part 2: General principles and overview; Part 3: Cryptographic key relationships; Part 4: Secure application modules; Part 5: Use of algorithms; Part 6: Cardholder verification; Part 7: Key management .	**F**	All card types.	

Component	Specification	Current Situation	Applicability	Observations
Terminal infrastructure	Identification card systems - Man-machine interface – Part 3: Keyboards.	**R**	All card types.	
	PC/SC Standards. Consortium standards PC/SC Workgroup Interoperability Specification for ICCs and Personal Computer Systems. Part 1. Introduction and Architecture Overview. Part 2. Interface Requirements for Compatible IC Cards and Interface Devices. Part 3. Requirements for PC-Connected Interface Devices. Part 4. IFD Design Considerations and Reference Design Information. Part 5. ICC Resource Manager Definition. Part 6. ICC Service Provider Interface Definition. Part 7. Application Domain/Developer Design Considerations. Part 8. Recommendation for Implementation of Security and Privacy ICC Devices.	**A**	All card types	For general use in PCs.
	ITI Manual on Technical Conducts – Volume I.	**A**	Cards capable of handling digital certificates.	
	FIPS-140-2 Standard.	**A**	All card types.	According to topic 1 of the ICP Brasil Working Group: to follow at least the FIPS-140-2 Security level 1 rules. To follow at least the FIPS-140-2 Security level 2 rules on hardware violation verification.

8.4. Means of Access: Technical Specifications on Mobility

Mobile telephone equipment has already outnumbered the amount of landlines, thus becoming a broad communication channel with the citizen. Furthermore, the availability of personal computer with mobile resources, at more accessible prices, is growing day by day, pushed by government incentives and reduction in production costs. Therefore, it becomes a major challenge for the government to provide society access to the electronic government products and services, based on mobile devices, usually portable ones, such as notebooks, cellular phones, smartphones and others.

Table 13 – Specifications on Means of Access – Mobility

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Transmission Protocol		**F**	
Browser		**F**	
Hypertext Standard		**F**	
Extended Programming		**F**	
Messaging		**F**	
Video and Sound Files		**F**	
Image Files		**F**	
Office Files		**F**	
PDF Reader		**F**	

8.5. Means of Access: Technical Specifications for Digital TV

Considering the amount of television receivers in Brazilian households, and the eminent implementation of the Brazilian Digital TV System, which allows interaction with spectators; this therefore becomes a channel that has a great potential for relationships between government and society. Therefore, based on the new Digital TV equipment, new possibilities of access to electronic government products and services arise. The digital TV offers much more than just a quality signal, it provides interactivity and access to commercial services, such as shopping, games, and access to banks, as well as Social Services, such as consultations to pension funds, the social integration program, government social programs, distance education, among others, making the citizens go from an essentially passive activity to a participative activity.

The Digital TV provides a communication standard in different perspective, such as: technological, with analog to digital system migration; economic, with new services and business opportunities; social, by offering a diverse range of content, as well as digital inclusion when the Internet is accessed through the television set; political, with the possibility of encouraging the discussion of a new regulatory frame work; and behavioral, when it allows the participations of audiences through different levels of interactivity.

In order to address the technical issues, the Brazilian Technical Standards Association – ABNT set out various standards, as listed below:

Table 14 – ABNT Standards on Digital TV

Reference	Title
ABNT NBR15601	Digital Terrestrial Television – Transmission system.
ABNT NBR 15602-1	Digital Terrestrial Television – Video coding, audio, and multiplexing – Part 1: Video coding.
ABNT NBR 15602-2	Digital Terrestrial Television – Video coding, audio, and multiplexing – Part 2: Audio coding.

Reference	Title
ABNT NBR 15602-3	Digital Terrestrial Television – Video coding, audio, and multiplexing – Part 3: Signal multiplexing system.
ABNT NBR 15603-1	Digital Terrestrial Television – Multiplexing and service information (SI) – Parte 1: SI for digital broadcasting systems.
ABNT NBR 15603-2	Digital Terrestrial Television – Multiplexing and service information (SI) – Part 2: Data structure and definitions of basic information of SI.
ABNT NBR 15603-3	Digital Terrestrial Television – Multiplexing and service information (SI) – Part 3: Syntaxes and definition of extended information of the SI.
ABNT NBR 15604	Digital Terrestrial Television – Receivers.
ABNT NBR 15605	Digital Terrestrial Television – Security issues.
ABNT NBR 15606-1	Digital Terrestrial Television – Data coding and transmission specifications for digital broadcasting – Part 1: Data coding.
ABNT NBR 15606-2	Digital Terrestrial Television – Data coding and transmission specifications for digital broadcasting – Part 2: Ginga-NCL for fixed and mobile receivers – XML application language for application coding.
ABNT NBR 15606-3	Digital Terrestrial Television – Data coding and transmission specifications for digital broadcasting – Part 3: Data transmission specifications.
ABNT NBR 15606-5	Digital Terrestrial Television – Data coding and transmission specifications for digital broadcasting – Part 5: Ginga-NCL for portable receivers – XML application language for application coding.
ABNT NBR 15607-1	Digital Terrestrial Television – Interactivity channel – Part 1: Protocols, physical interfaces and software interfaces.
ABNT NBR 15608	Digital Terrestrial Television – Operational guidelines.
ABNT NBR 15609	Digital Terrestrial Television – Testing suit (under development).
ABNT NBR 15610	Digital Terrestrial Television – Testing for receivers (under development).

Table 15 – Specification on Means of Access – Digital TV

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Middleware		**F**	
Audio Coding		**F**	
Video Coding		**F**	
Transport Layer		**F**	
Transmission		**F**	

9. Organization and Exchange of Information

9.1. Organization and Exchange of Information: Technical Policies

The technical policies for the organization and exchange of information and data are:

9.1.1. Use of XML for data exchange.

9.1.2. Use of XML Schema and UML (whenever such case) to define exchange data.

9.1.3. Use of XSL for data transformation.

9.1.4. Use of a metadata standard to manage electronic contents.

9.2. Information Organization and Exchange: Technical Specifications

Table 16 – Specifications on the Organization and Exchange of Information

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended For Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Data language	XML (Extensible Markup Language) as defined by the W3C http://www.w3.org/XML	**A**	
Data transformation	XSL (Extensible Stylesheet Language) as defined by the W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) as defined by the W3C http://www.w3.org/TR/xslt	**A**	
Data Exchange defintion	XML Schema as defined by the W3C: - XML *Schema Part 0: Primer* http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ - XML Schema Part 1: Structures http://www.w3.org/TR/xmlschema-1/structures - XML Schema Part 2: Datatypes http://www.w3.org/TR/xmlschema-2/datatypes UML *(Unified Modeling Language)* as defined by the OMG http://www.omg.org/gettingstarted/specsandprods.htm/	**A**	
Data description	RDF (Resource Description Framework) As defined by the W3C.	**F**	
Metadata elements for content management	e-PMG – Metadata Standard for Electronic Government.	**E**	
Browser Taxonomy	LAG - • Government List of Subjects, Version 1.0. As defined at: http://www.eping.e.gov.br	**A**	

Component	Specification	Current Situation	Observations
Identifier and resolution services	Handling system (http://www.handle.net).	E	

9.3. Observations on XML and Middleware

Not all systems need to be able to communicate directly in XML, as described in Figure 5. Whenever appropriate, the use of middleware, according to the illustration in Figure 6, is accepted.

Although the settings below represent potential solutions, the direct XML model (Figure 5) is preferred, although it is possible to use the indirect model, as presented in Figure 6, in situations that justify its use.

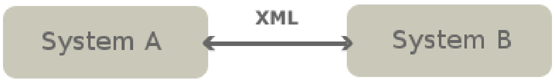

Figure 4 – Direct XML Model – Direct Transaction

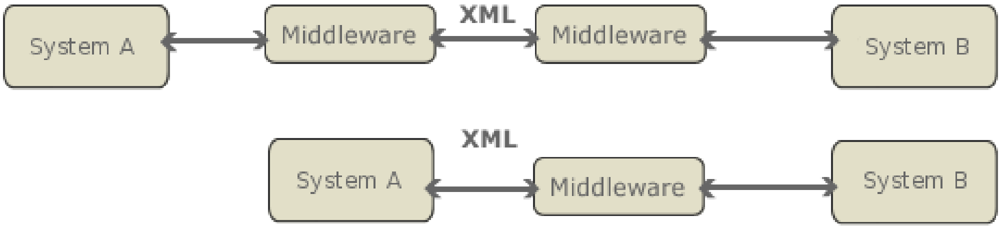

Figure 5 – Transaction via middleware

In specific cases, such as those that require the transaction of a major volume of data between systems in a short period of time, and in transactions in which the response time is critical, adopting XML as an Exchange language can be gradual.

9.4. Observations on the use of UML

To describe complex data, and aiming at the best explanation and description, and whenever appropriate, the use of UML class diagrams is recommended.

10. Areas for Electronic Government Integration

10.1. Areas for Electronic Government Integration: Technical Policies

10.1.1. The technical guideline for information systems integration recommends gradual adoption of the Service Oriented Architecture (SOA), using as reference for its implementation the **“Referential Architecture of Electronic Government Interoperability Standards (RA)**” initiative, which is a Service Oriented Architecture, adjusted to the reality of the Federal Government IT Systems, and that is available at http://i3gov.softwarepublico.gov.br/i3gov/.

10.1.2. The e-PING - Electronic Government Interoperability Standards architecture recommends using XML, and developing XML Schemas as the basis for electronic government integration and interoperability.

10.1.3. The **Government Service Interoperability Guide** is available in the Electronic Government gateway, in order to guide the use of tools and technologies produced by the segment.

10.1.4. This segment deals with the components related to fields that cross over those of the government’s activities, and which the standardization is important in order to achieve interoperability among Electronic Government services, such as Processes and Geographic Information.

10.1.5. Regarding the necessary data and XML Schemas for the applications directed to the fields in which the government operates, the segment will seek to identify, follow up on production, and analyze contents that are of interest to the Public Administration, through articulation with government and society representative groups, and further reporting to the competent levels in regards to prioritization.

10.1.6. Data Standards Catalogue, and the XML Schemas Catalogue are closely interconnected. Therefore, one should be aware to the compatibility among its topics. We do not recommend the addition of a component, isolated, that is present in only one of the catalogues.

10.1.7. The Data Standards, XML Schemas Catalogue and Interoperable Services (Web Services) catalogues are available in the e-PING website.

10.1.8. Data that is of broad interest to the government shall be available in the Data Standards, and XML Schemas Catalogues, according to the rules set out on the use of these tools.

10.1.9. Data Standards Catalogue, and the XML Schemas Catalogue are core elements in the interoperability environment of the Federal Government. Using them is equal to the status of Adopted (A).

10.1.10. The technical specifications referring to XML Schemas within the Organization and Information Exchange Segment must be fulfilled.

10.1.11. The Interoperable Services (Web Services) of general interest must be available in the Service Catalogue; however, one must comply with the rules of utilization on the services that have restricted access, defined by their respective agencies.

10.1.12. The use of Web Services is suggested for integration demands among government information systems. That way, regardless of the technologies upon which they were implemented, an interoperability standard may be adopted, assuring scalability, ease of use, plus allowing it to be updated simultaneously and in real time.

10.2. Areas for Electronic Government Integration: Explanatory Note on the Data Standards and XML Schemas Catalogues

10.2.1. Brief Considerations

The Data Standard and XML Schemas Catalogues are available in the Electronic Government gateway, at http://www.governoeletronico.gov.br/.

The Data Standard Catalogue aims at establishing standards on Data Types and Attributes that apply to the interfaces of the systems within the public sector, and is divided in two documents:

- Volume 1, sets out general principles, that is, reasons, approach, and rules on the application of the standards on Data Types and Attributes; and
- Volume 2, presents the standardized definitions of Data Types and Attributes.

The XML Schemas Catalogue aims at establishing standards for XML Schemas that apply to the interfaces of the systems supporting the Electronic Government services.

The XML Schemas Catalogue contains standards that are accepted, in XML Schemas format, for data exchange within the public sector. These standards can correspond to a single schema, or to a set of XML Schemas, as long as it refers to a same definition within the Integration Area associated.

The publication of XML Schemas does not automatically assure access to its corresponding contents, or services associated, which may be subject to specific rules set out by the respective public manager.

10.2.2. Property and Responsibility

The e-PING Coordination staff is responsible for these Catalogues, particularly for setting out the rules regarding management of the amendment processes, and for encouraging the Standards to be used in future developments.

In that regard, we recommend 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.

10.2.3. Mechanisms to Manage the XML Schemas Catalogue

For new entries to the XML Catalogue:

a) Proposal, followed by accepted content proposal for the Data Standards Catalogue (CPD).
b) Submission, followed by accepted content proposal for the Interoperation Referential Architecture for the Government Information Systems (AR);
c) Submission of content, by a professional linked to the public sector, directly to the XML Schemas Catalogue, through an electronic form available at the e-PING site.

The proposal of XML Schemas registration will be submitted to the analysis of the Working Group on Areas for Electronic Government Integration, through a specific electronic form, available at the e-PING website (www.e-ping.e.gov.br). Only the accepted proposals will be kept in the catalogue, whereas those that are still under review or have been rejected, as well as previous XML Schemas that were accepted, will be kept in a “testing” environment, to be further conceived and implemented in a timely manner.

The evaluation criteria shall include:

- acknowledgment by the user community;
- agreement by the area/subarea public manager (whenever he is not the proponent); and
- compliance with e-PING standards.

In other words, the submission of a certain XML Schema in which the proponent is not the manager of the area is foreseen, but will be additionally subject to the manager’s agreement.

Requests for amendments to already published XML Schemas will be preliminarily analyzed by the Working Group Areas for Electronic Government Integration. The e-ping Central Coordination is responsible for accepting them or not, and may decide to adopt the amendments such as proposed, or submit them to public consultation, through the website http://www.governoeletronico.gov.br.

10.3. Areas for Electronic Government Integration: Technical Specifications

The technical specifications for the Areas for Electronic Government Integration are:

Table 17 – Specifications for the Areas for Electronic Government Integration – Topics that cross-over the fields of government activities.

Topics	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Study
	F = For Future Consideration		

PROCESSES – Business Process Execution Language	BPEL4WS V1.1, as set out by OASIS http://www.oasis-open.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	**R**	The group will follow the evolution of BPEL4WS version 2.0. Studies on future definitions and following specifications will be led by this group
PROCESSES – Process Modeling Notation	BPMN 1.0, as set out by the OMG http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf	**R**	
Financial Information Exchange	XBRL - eXtensible Business Reporting Language http://www.xbrl.org/SpecRecommendations/	**F**	www.xbrl.org
Legislation, Jurisprudence and Legislative Proposals	LexML v. 1.0 http://projeto.lexml.gov.br	**R**	The LexML Project sets out recommendations for identification and structuring of legislative and legal documents.
Strategic Planning	StratML - Strategy Markup Language http://xml.gov/stratml/index.htm	**F**	
Geospatial information - geospatial technology Interoperability	WMS version1.0 or higher http://www.opengeospatial.org/standards	**A**	
	WFS versão 1.0 ou posterior http://www.opengeospatial.org/standards	**A**	
	WCS version1.0 or higher http://www.opengeospatial.org/standards	**A**	
	CAT	**R**	The CAT/CSW - Catalogue Services for the Web – is an OpenGIS standard for metadata exchange based on XML. CSW is mandatory for the implementation of

Topics	Specification	Current Situation	Observations
			metadata exchange networks, plus it fully complies with the e-PING recommendations regarding the use of XML and the availability of free libraries for its implementation.
	WFS-T	**E**	The WFS-T standard (Web Feature Service - Transaction) refers to the optional transaction and Lockfeature operations of the OpenGIS WFS service. The Transaction operation is used to describe spatial data manipulation (create, delete, update features), and the Lockfeature assures consistency of the geometric features in geographic databases.
	WKT/WKB	**E**	The WKT (Well-Known Text or the WKB Well-Known Binary is a text markup language for representing vector geometry objects on a map, spatial reference systems of spatial objects and transformations between spatial reference systems. Geometric objects that can be represented with WKT are: points, lines, polygons, TINs and

Topics	Specification	Current Situation	Observations
			Polyhedrons

Table 18 – Specifications on Areas for Electronic Government Integration – Web Services[29]

Component	Specification	Current Situation	Observations

	A = Adopted
	R = Recommended for Consideration
	T = Undergoing Transition
	E = Under Review
	F = For Future Consideration		

Registry infrastructure	The UDDI v3.0.2 (Universal Description, Discovery and Integration) specification defined by OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	
	ebXML (Electronic Business using eXtensible Markup Language). Specification may be found at http://www.ebxml.org/specs/index.htm	**E**	
Web service description language	WSDL 1.1 (*Web Service Description Language*) as set out by the W3C. Specification may be found at http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (*Web Service Description Language*) set out by the W3C. Specification may be found at http://www.w3.org/TR/wsdl20/	**E**	
Interoperability basic profile	*Basic Profile 1.1 Second Edition*, como definido pela WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	Basic Profile version 1.2 is a working draft, and may be found at http://www.ws-i.org/Profiles/BasicProfile-1.2.html
Remote Portlets	WSRP 1.0 (Web Services for Remote Portlets) as set or by OASIS http://www.oasis-open.org/committees/wsrp	**E**	

[29] Security issues regarding Web Services are addressed in chapter 7.

11. Glossary of Acronyms and Technical Terms [30]

Definitions for the main technical terms used in e-PING.

ABNT – Brazilian Technical Standards Association: publishes rules and standards to direct the preparation and collection of reference material used to produce documents, and to be included in bibliographies, summaries, opinions, and others.

ACAP – Application Configuration Access Protocol: Internet protocol designed to support remote storage and access of program options, configuration and preference information. It's a proposed solution to the problems of client mobility on the Internet.

APF – Federal Public Administration: bodies pertaining to the direct (within the administrative structure of the Presidency of the Republic and Ministries) and indirect administration (Autarchies, Public Enterprises, Government controlled Companies, and Public Foundations) of the Executive Branch. https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm.

BPM - *Business Process Management*: Business processes of an organization approached as a workflow, based on standard modeling notation, execution, and coordination in XML, of which its semantic rigor allows for interoperability between systems in different platforms, therefore it is a basic component to implementing solutions based on service oriented architecture.

Browser: A client application that allows the user to view web contents in another network or personal computer, to follow hypertext links, and transfer files.

XML *Schemas Catalogue*: information directory on XML *Schemas*.

Encryption: information protection technique that consists in encrypting the content of a message or a sign, transforming it into an unreadable text, using complex math algorithms.

CAT – *Catalog Service Implementation Specification*: *OpenGIS* specification defines common interfaces to discover, browse, and query metadata about data, services, and other potential resources. The term most used today for Catalog Service is CSW.

CSW – *Catalog Service Implementation Specification*: *OpenGIS* specification that defines interfaces to publish, access, browse and search metadata about geospatial information.

Device: physical component (work station, mobile telephone, smart card, hand-held, digital television with Internet access).

DNS – *Domain Name System*: The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address. **FTP – *File Transfer Protocol***: it is an application protocol that uses TCP/IP Internet protocols, and is the simplest way of transferring files among computers through the Internet.

GML – *Geography Markup Language*: OpenGIS specification based on XML, and developed to support delivery and storage of geospatial information.

Hand-helds: Hand computer, also know by PDA, pocket PC or palm top. A portable equipment developed to be an access device.

Handshake: In telephone communication, handshaking is the exchange of information between two modems and the resulting agreement about which protocol to use that precedes each telephone connection.

Hashing: Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the

[30] Microsoft Press. IT dictionary. Translator and editorial consultant Fernando Barcellos Ximenes – KPMG Peat Marwick. Campos Ltda. Editing, 1993. ISBN 85-7001-748-0.

Thing, Lowell (ed.). Technology Dictionary. Translation of Bazán Tecnologia e Lingüística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

original value. It is also used in many encryption algorithms.

HELO: variety of parameters that limit the delivery of unsolicited commercial email (UCE). http://www.postfix.org/uce.html.

HTTP – *Hyper Text Transfer Protocol* set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

HTTPS – *Secure Hyper Text Transfer Protocol*: web protocol developed by Netscape and built on to the browser. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. It is simple the use of Netscape Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering.

ICP – Brasil: set of techniques, practices, and procedures to be implemented by the Brazilian government and private organizations, with the purpose of establishing technique and methodological elements for a digital certification system based on a public key. http://www.icpbrasil.gov.br.

IEEE – *Institute of Electrical and Electronics Engineers*: fosters the development of standards that often become national and international standards.

IETF – *Internet Engineering Task Force* the body that defines standard Internet operating protocol s such as TCP/IP.

IMAP – *Internet Message Access Protocol*: is a standard protocol for accessing e-mail from your local server. IMAP is a client/server protocol in which e-mail is received and held for you by your Internet server.

IP – *Internet Protocol*: protocol for communication among devices in the network. Generically, it can be understood as a set of numbers that represent the location of a certain device (usually computers) in a private or public network.

IPSec – *Internet Protocol Security*: IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well.

IPv4 – Internet Protocol Version 4: Internet protocol most widely employed. IPv4 addresses are usually represented in dot-decimal notation (four numbers, each ranging from 0 to 255, separated by dots, e.g. 208.77.188.166). Each part represents 8 bits of the address, and is therefore called an octet. It is possible, although less common, to write IPv4 addresses in binary or hexadecimal. When converting, each octet is treated as a separate number. (So 255.255.0.0 in dot-decimal would be FF.FF.00.00 in hexadecimal.).

IPv6 – Internet Protocol Version 6: the latest version of the IP protocol. IPv6 Node Addresses are 128-bit records represented as eight fields of up to four hexadecimal digits. A colon separates each field (:). Example: 3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344). It is gradually being introduced to the Internet and will probably work side-by-side with the IPv4. In the long run, the IPv aims at replacing the IPv4 that only handles 4 billion (4 x 109) addresses, against 3.4 x 1038 addresses from the new protocol.

LAN – *Local Area Network* : Group of computers and devices that share a same line of communication, and usually the resources of a single processer or Server in a small geographic area. Usually, the server has shared applications and data storage for different users, on different computers.

LDAP – *Lightweight Directory Access Protocol*: software protocol to locate organizations, people, and other resources, such as files and devices on a network, be it on the public Internet, or in a corporative intrante.

Means of Access: set of physical (access devices) and non physical (basic software, applications, etc) components that allow the user to access an electronic government service.

Real Time or Instantaneous Messaging: A type of communication that allows the user to exchange messages with another user that is also connected to the network.

Metadata: also known as data (or information) about data. Metadata describes the structure and attributes of data; metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource; as well as supporting digital identification, filing, and storage.

Middleware: in the computer industry, middleware is a general term for any programming that serves to "glue together" or mediate between two separate and often already existing programs. Typically, middleware programs provide messaging services so that different applications can communicate.

Newsgroup: a newsgroup is a discussion about a particular subject consisting of notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. The users can send messages to existing newsgroups, respond to previous messages and create new newsgroups.

OGC – *Open Geospatial Consortium* : is a non-profit, international, voluntary consensus standards organization that is responsible for the “development of standards for geospatial and location based services that are freely available for general use”.

OWS - OGC *Web Services*: set of OpenGIS® Specifications for interfaces, schemas and encodings that comprise the interoperability framework for development and implementation of standards for geospatial content and services."

Open Standards:
I – allow interoperability among different applications and platforms, both internal and external;
II – are free for all to implement, with no royalty or fee;
III – can be fully and independently implemented by multiple computer program manufacturers, on multiple platforms, and its use is not subject to the payment of any intellectual or industrial property right.

Metadata Standard: sets out a set of metadata elements for a community, including element and coding specifications, to allow interoperability among the systems using the standard.

Plug-in: a separate program that adds capabilities to the main program. Usually, they can easily be installed and used as part of your Web browser. A plug-in application is recognized automatically by the browser and its function is integrated into the main HTML file that is being presented.

POP3 – *Post Office Protocol* 3: is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server.

Gateway: - a network point that acts as an entrance to another network. A website that gathers services, news, and large volumes of information and/or entertainment contents.

Government Network: Gateway entrance to all the federal government’s pages on the Internet. http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm.

Electronic Government Resolution no. 7: sets out rules and guidelines for the Federal Public Administration websites (gov.br and mil.br). It is divided in 7 chapters and addresses: information structure, control and monitoring, interactive element management, organizational model, visual identity and security of government sites on the World Wide Web. http://www.governoeletronico.e.gov.br.

RFC – *Request for Comments*: A Request for Comments (RFC) is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs. RFC is also an abbreviation for Remote Function Call.

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

Government Electronic Service (Electronic Government Services, Electronic Services):

The electronic government can be defined by the use of technology to increase access and improve the delivery of government services to the citizens, suppliers and servers. Generally speaking, the electronic government features are:

1. Electronic delivery of information and services.
2. Regulation of information networks, particularly those related to governance, certification and taxation.
3. Public accountability, transparency and monitoring of budget spending.
4. Distance learning, computer literacy and virtual libraries.
5. Culture dissemination, with emphasis on local identities, fostering and conserving local cultures.
6. e-procurement, that is, procuring goods and services through the Internet, such as electronic public biddings, electronic auctions, Brazilian government electronic market, and other types of digital markets for goods procured by the government.
7. Encouraging e-business, by creating safe transaction environments, specially for small and médium enterprises. http://www.governoeletronico.gov.br/r1.

Federal Government Information Systems: systems that support the following duties:

- government management: Planning, Budget, Budget Spending, Financial Administration, Human Resources Administration, Administration of General Services, Management of Documents and Information, Administrative Organization and Modernization, Information Resources, and Information Technology, and Internal Control;
- Activities that are of government department responsibilities: end activities of the different agencies from the government structures, such as: infrastructure, (transportation, communications, energy, natural resources administration) agriculture, health, etc.

Reference: http://www.redegoverno.gov.br/projetos/reg_gestao.asp.

SFS – Simple Features Specification for SQL: OpenGIS specification that define a standard SQL schema that supports storage, retrieval, query, and update of geospatial information.

Smart Cards: A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.

S/MIME – *Secure Multi-Purpose Internet Mail Extensions*: is a secure method of sending e-mail that uses the RSA (Rivest-Shamir-Adleman) encryption system. S/MIME describes how encryption information and a digital certificate can be included as part of the message body.

SMTP/MIME – *Simple Mail Transfer Protocol/Multi-purpose Internet Mail Extensions*:SMTP is a TCP/IP protocol used to send and receive e-mails. MIME is an Internet standard that extends the format of e-mail to support the transfer of different data files through the Internet.

SOA - *Service Oriented Architecture*: is a paradigm for the organization and use of distributed capabilities that are controlled by different proprietary domains. The SOA architecture is used for interoperability among systems through a set of loosely coupled service interfaces, in which the services do not require the technical details of the other services' platforms in order to exchange information.

SOAP – *Simple Object Access Protocol*: an XML-based protocol to let applications exchange information over HTTP. SOAP message delivery is used to allow the exchange of a variety of XML information. It is responsible for delivering service requests and replies between users and service suppliers.

Free Software: a computer program available through its source code and allowing anyone to use it, copy it and distribute it, be it in its original format or modified, either freely or upon payment of a fee. Free software is necessarily non- proprietary software, but it is important not to confuse free software with freeware.

SPAM: Spam is unsolicited e-mail on the Internet. (E-mail that is wanted is sometimes referred to as ham.) From the sender's point-of-view, spam is a form of bulk mail, often sent to a list obtained from a spambot or to a list obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail.

SSL – Secure Sockets Layer: are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet.
Browser Taxonomy: it is a controlled vocabulary of hierarchically organized and structured

expressions and sentences, based on natural or constructed relationships, to make it easier for website and gateway users to find information.

TCP – *Transmission Control Protocol*: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

Telnet: Telnet is a way to remotely access someone else's computer, given that they have granted permission. Technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers.

TLS – *Transport Layer Security*: is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. protocolo que garante a privacidade entre os aplicativos de comunicação e seus usuários na Internet. Quando um servidor e o cliente se comunicam, o TLS garante que nenhuma outra parte poderá ver ou apanhar a mensagem.

Token: a structured data object or a message that continually circulates between the nodes of a token ring network and describes the network's current status.

UDDI – *Universal Description Discovery and Integration*: registry for businesses worldwide to list themselves on the Internet, enabling companies to find one another on the Web.

UDP – *User Datagram Protocol*: is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.

UML – *Unified Modeling Language*: UML is much more than a standardized notation, that is, it is The Unified Modeling Language offers a standard way to write a system's blueprints, including conceptual components such as business processes and system functions as well as concrete things such as programming language statements, database schemas, and reusable software components. UML can be used for visualizing, specifying and constructing the artifacts of a software-intensive system, as well as for business modeling and other systems, not only software systems.

URI - *Uniform Resource Identifier*: is a string of characters used to identify or name a resource on the Internet. A URI is made up of a name (ex.: file, http, ftp, news, mailto, gopher), followed by a colon character, and then a scheme-specific part, according to RFC 1630. The URI encompasses to URN and URL concepts.

Usenet: Usenet is a collection of user-submitted notes or messages on various subjects that are posted to servers on a worldwide network. Each subject collection of posted notes is known as a newsgroup.

VPN – *Virtual Private Networks*: A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to transfer confidential information. The data transmitted in encrypted. The implementation of a VPN is based on virtual tunnels, through which the information flows, protecting it from unauthorized access.

W3C – *World Wide Web Consortium*: The W3C is an industry consortium which seeks to promote standards for the evolution of the Web and interoperability between WWW products by producing specifications and reference software

WAN – Wide Area Network*:* is a computer network that covers a broad area, such as whose communications links cross metropolitan, regional, or national boundaries.

WCS – *Web Coverage Service Implementation Specification*: OpenGIS standard that defines a standard interface and operations that enables interoperable access to geospatial "coverages" (*GetCapabilities, DescribeCoverage* e *GetCoverage*).

Web Services: software system designed to support interoperable machine-to-machine interaction over a network. Logical and programmable application that provides compatibility among different applications, regardless of their operational system, allowing communication and data exchange among different networks.

WFS – *Web Feature Service Implementation Specification*: OpenGIS standard WFS standard defines interfaces and operations for data access and manipulation on a set of geographic features (*GetCapabilities, DescribeFeaureType, GetFeature, Transaction* e *LockFeature*), through the HTTP protocol. Two classes of services are defined:

- **Basic WFS (WFS):** is only capable of implementing the follow capabilities: *GetCapabilities, DescribeFeatureType* and *GetFeature*. Therefore, it is considered a WMS service only for reading.
- **Transactional WFS (WFS-T):** capable of implementing all WFS basic and transactional operations. Optionally, it may also implement a LockFeature operation.

WMS – *Web Map Service Implementation Specification*: OpenGIS standard that defines interfaces to access and manipulate capabilities on multiple layers of geospatial information containing vectors and/or images.

WSDL - *Web Services Definition Language*: is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

XML – *eXtensible Markup Language*: is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere. XML is "extensible" because, unlike HTML, the markup symbols are unlimited and self-defining.

XML *Schemas*: XML documents also found on the internet, they provide a means for defining the structure, content and semantics of XML documents. in more detail. XML schemas of the same subject must be available on a public site. Softwares could access these documents to validate their own XML documents http://www.uff.br/gdo/htm/tsld106.htm.

XMPP – *eXtensible Messaging and Presence Protocol*: open protocol based on Extensible Markup Language (XML) and intended for instant messaging (IM) and online presence detection.

XSL – *eXtensible Stylesheet Language*: language for creating spreadsheets that described how a piece of information is delivered via Web, by using XML, and how it is presented to the user. XSL is a language for formatting XML documents.

XSLT – *eXtensible Stylesheet Language Transformations*: standard language for transforming XML documents into other XML documents, with another structure. It shall be understood as an extension of the XSL. XSLT shows how XSL documents should be reorganized in another data structure (which may be presented based on an XSL spreadsheet).

12. Participants

e-PING Coordination Staff

Brazilian National Water Agency (ANA)
Sérgio Augusto Barbosa

National Petroleum Agency (ANP)
Roberto Moreira Caldeira
Brazilian Association of Information and Communication (ICT) State Entities (ABEP)
Dayse Vianna

Bank of Brazil (BB)
Ulisses de Sousa Penna

Federal Savings Bank (CAIXA)
Ângela B. Baylo
Paulo Maia da Costa
Rúbia Scrócaro

IT Department of SUS (Unified Health System) - DATASUS
Wilson Moraes Coelho

Technology and Information Bureau of the Brazilian Social Welfare System. (DATAPREV)
Humberto Degrazia Campedelli

Institute for National Artistic and Historical Heritage - (IPHAN)
Carlos Augusto Pessoa Machado

Ministry of Defense – Army Command (MD/CEX)
Linda Soraya Issmael
Roberto Penido Duque Estrada

Ministry of Justice (MJ)
Jorilson da Silva Rodrigues

Ministry of Health (MS)
Eliane Pereira dos Santos
Ernani Bento Bandarra
Márcia Helena Gonçalves Rollemberg

Ministry of External Relations (MRE)
Filipe Carneiro Guimarães

Ministry of the Development, Industry, and Foreign Trade (MDIC)
José Luismar de Campos Larcher

Ministry of the Environment (MMA)
Maurício Dayriell
Paulo Henrique de Assis Santana

Ministry of Planning, Budget, and Management – Secretariat of Logistics and Information Technology (MP/SLTI)
Nazaré Lopes Bretas (Coordinator-General)
Cláudio Muniz Machado Cavalcanti
Corinto Meffe
Ednylton Maria Franzosi
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Leonardo Lanna Guillén
Rogério Santanna dos Santos

Presidency of the Republic (PR)
Macarino Bento Garcia de Freitas
Marcelo André de Barros Oliveira
Roberto Montella Pimenta

Presidency of the Republich – National Institute for Information Technology (ITI)
Mauricio Augusto Coelho
Renato da Silveira Martini

IRS Secretariat – Brazil (RFB)
Edna Pereira Pinto Fernandes

Federal Data Processing Service (SERPRO)
Elói Juniti Yamaoka
Márcio Humberto M. Cammarota

Working Group on Interconnectivity

Leonardo Lanna Guillén (MP/SLTI) – Coordinator
Carlos Bellone Neto (RFB)
Daniel Moreira Guilhon (CGU)
Filipe Carneiro Guimarães (MRE)
Hugo Góis Cordeiro (MinC)
Júlio César Japiassu Lyra (MJ)
Juscelino Kilian (PR/GSI)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Carlos de Oliveira (ECT)
Marco Antonio Silva (ANA)
Marcos Martins Melo (SERPRO)
Nelson Soares de Rezende (IBGE)
Odilon de Freitas Militao Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)
Roberto Moutella Pimenta (ITI)
Rogerio Alencar d´Araujo Couto (EMBRAPA)
Sumaid Andrade de Albuquerque (MTur)
Ulisses de Sousa Penna (BB)
Vanderlei de Jesus dos Santos Marques (ANVISA)

Collaboraters
Diogo da Fonseca Tabalipa (MP/SLTI)

Working Group on Security

Jorilson da Silva Rodirgues (MJ) – Coordinator
Emanuel Alamo Diogenes (ME)
Fábio Abdalla Afonso (CGU)
Filipe Carneiro Guimarães (MRE)
Georgia de Souza Assumpção (IBGE)
Gilberto de Oliveira Netto (SERPRO)
Humberto Degrazia Campedelli (DATAPREV)
Jean Carlo Rodrigues (ITI)
Joel Corrêa (DATAPREV)
Luiz Augusto Barbosa Mozzer (CGU)
Maisa Netto Leidemer (MC)
Márcio Vasconcelos Donato (MEC)
Marcos Gomes Figueira (BB)
Marcos J.C. Euzébio (BACEN)
Renato Navajas (MDIC)
Ricardo Campos dos Santos (SERPRO)
Roberta Rodrigues (ME)
Saulo Medeiros de Araújo (MDA)

Collaboraters
Anderson Claiton Fernandes (MJ)
Cláudia do Socorro Ferreira Mesquita (MP/SLTI)

Ronaldo Íon Miranda do Nascimento (MJ)

Working Group Means of Access

Paulo Maia da Costa (CAIXA) – Coordinator
Artur Emilio de Rezende (MF)
Bruno Pacheco de Assis (SERPRO)
Carlos Bellone Neto (RFB)
Cláudio Muniz Machado Cavalcanti (MP/SLTI)
Danielle de Menezes Maciel Silva (ANVISA)
Denise Barros de Sousa (MEC)
Eliane Aristoteles moreira (DATAPREV)
Frederico Cabral de Menezes (CONAB)
Geancarlo Noronha Vinhal (SERPRO)
Jacob Batista de Castro Junior (PR/GSI)
Jorge Arruda (MP/CGTI)
Juscelino Kilian (PR/GSI)
Márcio F. Viana M. (ME)
Márcio Humberto M. Cammarota (SERPRO)
Marconi Pereira Sodate (RFB)
Mauro Lemes da Silva (CAIXA)
Pedro Paulo Lemes Machado (ITI)
Reinaldo Silva Simão (PR)
Rubia Scrocaro (CAIXA)
Sonia Regina Rodrigues Motta (MEC)
Viviane Regina Lemos Bertol (ITI)
Wagner Ferreira Carneiro Junior (MF)

Collaboraters
André Luís da Silva Gonçalves (MP/SLTI)

Working Group Organization and Information Exchange

Eloi Juniti Yamaoka (SERPRO) – Coordinator
Alisson de Oliveira Rodrigues (MI)
Ângela B. Baylo (CAIXA)
Antonio Celso Xavier de Oliveira (MRE)
Aurélia Dolores Gonçalves Bruner (ELETROBRÁS)
Beatriz Barreto Brasileiro Lanza (CELEPAR)
Brenda Couto de Brito Rocco (AN-CC)
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)
Dayse Vianna (PRODERJ)
Dilma de Fátima Avellar Cabral da Costa (AN-CC)
Eduardo Rafael Miranda Feitoza (MI)
Eliane Pereira dos Santos (MS)
Elizabeth da Silva Maçulo (AN-CC)
Fernanda Hoffmann Lobato (MP/SLTI)
Hilda Pimentel (ANCINE)
João Alberto Lima (Federal Senate)
Ligia Leindorf Bartz Kraemer (UFPR)
Luciana Ferreira Pinto da Silva (INEP)
Márcia Helena Gonçalves Rollemberg (MS)
Márcia Izabel Fugizawa Souza (EMBRAPA)
Márcio Imamura (IBGE)
Margareth da Silva (AN-CC)
Maria Valéria Lins Tenório (Government of the state of Pernambuco / ATI)
Neuza Arantes Silva (MAPA)
Sérgio Silva dos Santos (MAPA)
Siomara Zgiet (MS)
Sylmara Campos Pinho Garcia (ANCINE)
Vicente de Paula Teixeira (CGU)

Virgilio Dantas Lins Filho (ME)
Vivianne Muniz Veras Barrozo (SERPRO)

Collaboraters
Dalva Clementina Luca (MJ)

Working Group on Areas for Electronic Government Integration

Cláudio Muniz Machado Cavalcanti (MP/SLTI) – Coordenador
Adelino Fernando Correia (DATASUS)
Aliomar Mariano Rego (EMBRAPA)
Ananda de Medeiros Macias (SERPRO)
Antônio Campos Monteiro (ANEEL)
Bruno Palvarini (MP/SEGES)
Carlos Bellone Neto (RFB)
Carlos Maranhão (ANS)
Ceres Albuquerque (ANS)
Cláudio Manoel Cordeiro (SERPRO)
Ewerton Luciano Martins (ANVISA)
Frederico Duarte Guerra de Macedo (ME)
José Glaucy Rocha (RFB)
Hesley Py (IBGE)
Maurício Dayrell (MMA)
Marcelo Bastos Brandão (ABIN)
Márcio Humberto M. Cammarota (SERPRO)
Márcio Lúcio Vasconcelos Donato (MEC)
Mônica Maria Lucatelli Dória de Araújo (DATAPREV)
Paulo Henrique Santana (MMA)
Pedro Paulo Cirineo (BB)
Ricardo de Lima (INCRA)
Rogério Werneck (PR/DIRTI)
Tatiana Giachini (SERPRO)
Werangge Custódio (ANVISA)
Wilson de Morais Coelho (DATASUS)

Collaboraters
Cláudia do Socorro Ferreira Mesquita (MP/SLTI)
Luís Carlos Ramos (DATASUS)

Subgroup: ABEP
Dayse Vianna (Governo do Rio de Janeiro / PRODERJ) – Coordinator
Aldecir Paz D´Avila Junior (Government of the state of Acre)
David William Honorio Araujo da Silva (Government of the state of Rio Grande do Norte)
Edinara Maria Ferreira Vale (Government of the state of Acre)
Marcos Ueda (Government of the state of Mato Grosso)
Tarcísio Quirino Falcao (Government of the state of Pernambuco / ATI)

Subgroup: Interoperability Guide for Government Services
Cláudia do Socorro Ferreira Mesquita (MP/SLTI) – Coordinator
Lucio Ribeiro (Government of the state of Pernambuco / ATI)
Tarcísio Quirino Falcão (Government of the state of Pernambuco / ATI)
Rodrigo Henriques Medeiros (SERPRO)

Subgroup: Standards for the Exchange of Spatial Information
Roberto Penido Duque Estrada (MD/CEX/DSG) – Coordinator
Alex Araújo (CAIXA)
Aramis Mota (PR/GSI)
Christian André H. Govastki (MME)
Dêner Lima F. Martins (ABIN)
Ellio Alves de O. Soares (CAIXA)

Eneias Roberto Shüller (CAIXA)
Fernando Gibotti (CAIXA)
Gerson Barrey (MEC)
Gilberto Ribeiro Queiroz (INPE)
Gustavo Araújo (MME)
Hisao Fujimoto (MME)
Jorge D. M. Cerqueira (PR/GSI)
Linda Soraya Issmael (MD/CEX/DSG)
Lúbia Vinhas (INPE)
Lúcia Helena Luz (CAIXA)
Moema José de Carvalho Augusto (IBGE)
Mosar Rabelo Júnior (MMA)
Silmara Ramos (PR/GSI)
Silvio Carlos Heitor Jorge (CAIXA)
Tálsia Garcia Meira (CC)
Valdevino S. Campos Neto (ANA)
Zandhor F. S. Cavalli Pradi (MS)

Collaborators
Carlos Brasileiro (MDS)
Edmar Morett (MMA)
Enos Josué Rose (MCIDADES)
Rafael M. Sperb (UNIVALI)
Wilfredo Pacheco (ANA)
Werner Leyh (MS)

Ilustrations

Hezrai de Souza Cruz (MP/SLTI)