Brazilian Government

Executive Committee of the Electronic Government

gov.br

e-PING

MAIS GOVERNO, MAIS CIDADANIA.

e-PING
Electronic Government Interoperability Standards

Reference Document

Version 2010

December 11th, 2009

SUMMARY

Presentation

e-PING architecture – Electronic Government Interoperability Standards – defines a minimal of premises, policies and technical specifications, which regulate the use of Communication and Information Technology (CIT) in the interoperability of Electronic Government Services, establishing the conditions of integration with the other Powers and Government Spheres and with the general society.

The areas covered by e-PING are segmented in:

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

For each one of such segments, there were specified components, for which, standards have been established.

The whole content of this reference document is in accordance to the guidelines of the Executive Committee of Electronic Government, created by the October 18, 2000 Order, and is published in specific web site at Internet (http://www.eping.e.gov.br), ensuring quick public access to the information of general interest and intrinsic transparency to the initiative. Brazilian Government is committed in assuring that such policies and specifications remain aligned with the needs of the society and with the gradual development of the market and of the technology.

e-PING reference document contains:

- fundamentals of conception, implantation and management of the e-PING, listing the expected benefits through the work, defining the coverage limits of the e-PING architecture and highlighting the considered premises and policies established;
- the management model of the e-PING, discriminating responsibilities, criteria for the verification of conformity, management of changes, divulgation and orientation for capacitating;
- the policies and technical specifications established for all components of each of the e-PING segments;
- glossary of referenced technical terms;
- relation of the integrants and collaborators of the present version of this document.

This document’s content is of public domain, and there are no restrictions related to its reproduction, nor in respect to the use of the information in it contained. The reproduction may be performed in any media, with no need of specific authorization. The improper use of the material with depreciative purposes will be considered subject to proper juridical subject, by part of the Brazilian Government, owner of the copyrights.

It is not permitted the use of the whole or part of this document with commercial purposes.

Part I – e-PING Overview

1. Introduction

The basis for providing better services, suitable to the citizens and business needs, at lower costs, is the existence of an infrastructure of Communication and Information Technology (CIT), which lends itself as a basis for the creation of such services. A modern, integrated and efficient government requires modern, integrated and interoperable systems also, working in an honest, secure and coherent way in the whole of the Public Service.

In such context, the interoperability of technologies, processes, information and data is a vital condition for quality services providing, becoming premises for governments all over the world, as groundwork for electronic government concepts, the *e-gov*. The interoperability allows rationalizing investments in CIT, by means of sharing, re-using and exchanging of technological resources.

Governments, such as American, Canadian, British, Australian and Neo-Zealander invest strongly in the development of policies and processes in the re-establishment of standards in CIT, assembling structures dedicated to obtain the interoperability, with the aim of providing better quality services, at reduced costs.

Brazilian Government has been consolidating the e-PING architecture – “Electronic Government Interoperability Standards”, which has as purpose to be a paradigm for the establishment of policies and technological specifications, which allow the delivery of quality electronic services to the society.

What is Interoperability?

In order to establish the objectives of the e-PING, it is essential to clearly defining what is understood as *Interoperability.* Next, are presented four concepts, which have substantiated the Brazilian Government acquaintance in respect to the subject:

“Coherent exchange of information and services between systems. It should enable the replacement of any component or product used in the interconnection points, by other of similar specification, without compromising the system functionalities” (United Kingdom Government);

“Capability to transfer and use information in a uniform an efficient manner between various organizations and information systems.” (Australia Government);

“Capability for two or more systems (computers, communication medias, networks, software and other components of the Information Technology) to interact an to exchange data according to a defined method, in order to obtain the expected results” (ISO);

“Interoperability defines whether two components of a system, developed through different tools, from different suppliers, may or not work together.” (Lichtun Wang, European Informatics Institute – CORBA Workshops);

Interoperability is not only integration between Systems; it is not only Integration of Networks. It is not referred solely on data exchange between systems. It does not simply look on definition of technology.

It actually is the sum of all of these factors, considering, also, the existence of a legacy of systems, Hardware platforms and installed Software. It arises from principles, which treat of component diversity, with the use of several products provided by various suppliers. It has as a goal to consider all the factors, in order to the systems to be able to work cooperatively, fixing the rules, the policies and the standards needed for the consecution of such objectives.

In order to interoperability to be reached, people should be engaged in a continuous effort to ensure that systems, process and cultures of an organization, to be managed and oriented to maximize the opportunities of exchange and re-use of information.

2. Scope

Policies and specifications clearly defined for interoperability and management of information are essential to provide the Government connection, both in internal ambit as in the contact with the society, and, in a higher lever of covering, with the rest of the world – other government and companies actuating in world market. e-PING is conceived as a basic structure for the electronic government strategy, initially applied to the federal government – Executive Power, not restricting the participation, through voluntary accession, of other Powers and spheres of government.

The government information resources constitute worthy economic assets. By ensuring that the governmental information can be quickly found and exchanged between the public sector and the society, maintaining the privacy and security obligations, the government helps in the maximum improvement of such assets, impelling and stimulating the economy of the country.

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

- Citizens;
- Other levels of the Govern (state and municipal);
- Other Powers (Legislative, Judiciary);
- International Organizations;
- Other countries Governments
- Companies (in Brazil and worldwide);
- Third Sector.

The following picture represents such relationship.

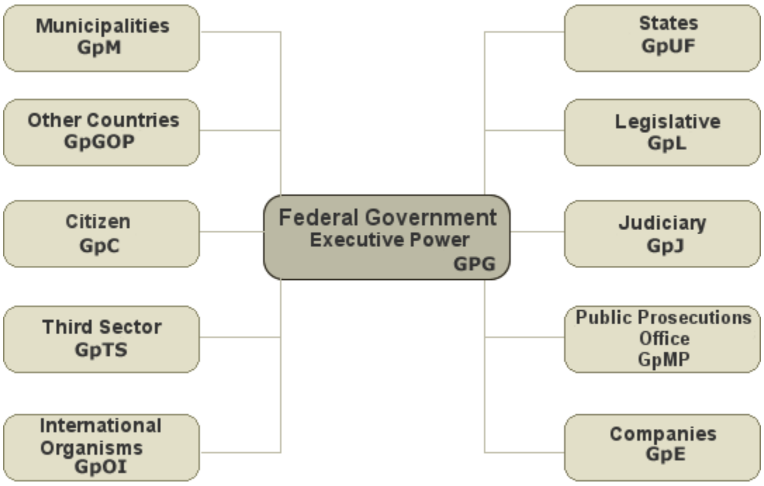

Figure 1 – Relationships of the Federal Government.

2.1. Accession to e-PING

The adoption of the standards and policies contained in the e- EGIS cannot be imposed to citizens and to the various instances of the government, inside and outside the country. Brazilian Government, however, establishes such specifications as standards by it selected and accepted, i.e., the same are the standards in which is desired to interoperate with the entities outside the Federal Government – Brazilian Executive. The accession for those entities will be taken through voluntary means and with no interference by part of the e-PING Coordination.

For organisms of the Federal Government – Brazilian Executive, the adoption of the standards and policies contained in the e-PING is obligatory.

The “Federal Government – Brazilian Executive Power” includes:

- the direct administration organs: Ministries, Secretaries and other governmental entities of the same juridical nature, bond, directly or indirectly to the Presidency of the Republic of Brazil;
- the autarchies and foundations.

In the ambit of the entities aforementioned, are obligatory the specifications contained in the e-PING for:

- all new information systems, which will come to be developed and deployed in the federal government and fall within the scope of interaction, within the federal government and with the general society;
- legacy information systems, which are subject to implementation that involves the provision of services of electronic government or interaction between systems;
- other systems, which are part of the objectives of making available the electronic government services.

The accession will occur in a gradual way, according to the implementation plan elaborated by the organization itself, which will consider the condition of the institution regarding to the conditions to adequate to the specifications and recommendations by e-PING.

The evaluation of the condition of the body in respect to the effective use of the standards will take place based on the Adoption Maturity Model of the e-PING – M-PING, currently in progress.

For information systems of government, which are out of the scope of obligatoriness delimited, it is recommendable that the responsible to consider the adequacy to the standards of the e-PING, every time those significant updating efforts are planned.

All purchases and agreements by the federal government – Executive Power directed to the de development of electronic government services and for updates of the legacy systems will be in consonance to the specifications and policies contained in this document.

The e-PING encourages the participation of all parts interested in the development of continuous updating of the specifications and recommendations integrant of the architecture. The management of the e-PING foresees such participation, by the use of the Internet (http://www.eping.e.gov.br) as a preferential mean for the contact between managers of the e-PING and the society.

2.2. Focus on interoperability

The e-PING will not have as working focus all subjects in the Information and Communication Technology (ICT) area. There will be treated only specifications, which are relevant to ensure the interconnectivity of systems, integration of data, access to electronic government services and management of content. e-PING involves subjects comprised in the segmentation, described in Item 4 of this document.

2.3. Subjects not covered

The e-Egis has not as aim to standardize the presentation form of the services information of the electronic government, restricting itself to the definition of the exchange requirements of data and of the availability conditions of such data for the access devices.

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

3. General Policies

Are listed, next, the general policies used in the construction of the e-PING and, which substantiate the policies and technical specifications of each segment.

3.1. Preferential Adoption of Open Standards

The e-PING defines that, always that possible, open standards will be adopted in the technical specifications. Proprietary standards are accepted, in transitory way, maintaining the perspectives of replacement, as soon as there are conditions for its migration. With no prejudice to such aims, there will be respected the situations in which there is the need of consideration of security requirements and information integrity.

3.2. Public Software and/or Free Software

The implementation of interoperability standards should priorize the use of public software and/or free software, in conformity with the guidelines of the Executive Committee of Electronic Government and norms defined in the ambit of the SISP.

3.3. Transparency

The e-PING documents will be available to the society, via Internet, being foreseen mechanisms of disclosure, receiving an evaluation of suggestions. Accordingly, it will be defined – and disclosure for overall knowledge – terms and commitments for the implantation and management of dedicated web site in the Internet (http://www.eping.e.gov.br).

3.4. Security

The interoperability in services delivery of the electronic government should consider the security level required by the service, with the maximum transparency possible.

3.5. Market Support

All specifications contained in the e-PING regard solutions largely supported by the market. The objective to be reached is the reduction of costs and risks in the conception and production of services in the governmental information systems.

e-PING considers that the interoperability involves technical, semantic and organizational elements, and is general guideline policies of such dimensions:

3.6. Technical dimension

3.6.1. Alignment with INTERNET

All information systems of the public administration should be aligned with the major specifications use in Internet and with the *World Wide Web*.

3.6.2. Adoption of XML

As a primary standard of data exchange, for every systems in the public sector.

3.6.3. Adoption of browsers

As the main way of access: all the government information systems will be accessible, preferentially, by means of technology based on browser, other interfaces are allowed in specific situations, such as in updating routines and data capture, in which there are not technological alternative available based on browsers.

3.6.4. Scalability

The selected specifications should have the ability to meet changes of demand in the system, such as changes in the data amount, quantity of transactions or amount or users. The established standards should not be a restrictive factor, being able to support the development of services, which meet from needs more localized, involving little amount of transactions an users, to national comprehensive demands, through the handling of a great amount of information and the involvement of an elevate contingent of users.

3.7. Semantic Dimension

3.7.1. Development of resources of organization of the information

Aiming to contribute for the simplification of the access to documents and services by Brazilian citizens, such as controlled vocabulary, taxonomies, ontologism and other methods of organization and retrieving of information.

3.7.2. Development and adoption of an Electronic Government Metadata Standard – e-PMG.

Based on standards internationally accepted (http://www.eping.e.gov.br).

3.8. Organizational dimension

3.8.1. Administrative simplification

The application of the e-PING aims to contribute to the changes in the interaction between the government and the society to be performed in a simple and direct way, without prejudice to the current legislation.

3.8.2. Promotion of collaboration between organizations

By means of the integration between institutional objectives and business processes of organizations with different internal structures and processes.

3.8.3. Guarantee of the information privacy

All the organizations responsible for the supply of electronic government services should ensure the conditions for the privacy preservation of the information of the citizens, companies and government organizations, respecting and accomplishing the legislation that defines the access and disclosure restrictions.

4. Segmentation

The e-PING architecture was segmented in five parts, with the finality of organizing the standards definitions. For each one of the **segments**, it was created a workgroup, composed by professionals acting in organs of the federal, state and municipal governments, experts in each subject. Such groups were responsible for the elaboration of this version of the architecture, basis for the establishment of the interoperability standards of Brazilian government.

The five segments – “Interconnection”, “Security”, “Means of Access”, “Organization and Exchange of Information” and “Integration Areas for the Electronic Government” – have been subdivided in **components**, to which were established the policies and technical specifications to be adopted by the federal government. Following, are listed the components that constitute each of the five segments.

4.1. Interconnection

The “Interconnection” segment establishes the conditions for the government organizations interconnect themselves, beyond setting the conditions of interoperation between the government and the society.

In this segment, there are established the specifications for:

- Messaging;
- Network Infrastructure;
- Network Services.

4.2. Security

This segment deals with security aspects of ICT that the federal government should consider.

Are treated standards for:

- Security in Data Communication;
- Security in Electronic Mail;
- Cryptography
- Systems Development;
- Network Services;
- Wireless Network;
- Response to Information Security Incidents.
- Policies and Specifications for smart cards and tokens.

4.3. Means of Access

In “Means of Access” segment, are explicated the questions relative to the standards of the access devices to the electronic government services. In this version, are approached the policies and specifications for workstations, digital television and mobility. In future changes, other devices will be treated. It is composed by three subsets contemplating the following components:

<u>Standards for access via workstations:</u>

- Browsers;
- Characters and Alphabets Set;
- Hypertext Exchange Format;
- Document Type Files;
- Worksheet Type Files;
- Presentation Type Files;
- Database Type Files for Workstations;
- Specification of Exchange of Graphic Information and Static Images;
- Vector Graphics;
- Animation Standards Specification;

- Audio and Video Type Files;
- Compression of General Use Files;
- Georeferencing Files;
- Extended Programming (Plugins).

Mobility:

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

Digital TV

- Definition
- ABNT Norms;
- Standards Specifications.

4.4. Organization and Exchange of Information

Covers the aspects related to the treatment and transference of information in the electronic government services. It includes standards of structure of government affairs and of metadata, comprising the following components:

- Language for Data Exchanging;
- Language for Data Transformation;
- Definition of Data for Exchanging;
- Electronic Government Controlled Vocabulary (VCGE);
- Government Metadata Standard (e-PMG).

4.5. Integration Areas for the Electronic Government

The segment establishes the use or elaboration of technical specifications based on the XML standard to support the information exchange in crosscutting areas of the government action.

The tools, which support the acting of the segment, are:

- Data Standard Catalog (CPD);
- XML Schemas Catalog;
- Interoperable Services Catalog (Web Services).

5. e-PING Management

In this Item, are treated the management aspects of the e-PING architecture, specifying the way by which Brazilian Government intends to consolidate the implantation of policies and technical specifications as effective standards adopted both internally, by the organizations that compose de Public Federal Administration, and in the interoperation with the external entities, represented by other instances of the government, by private initiative, by third sector active institutions and by the citizen.

5.1. Background

The e-PING architecture has as aim to be a paradigm of interoperability for the federal government, initially in the ambit of Executive Power. The initiative of assembling the architecture has been in charge of three organizations in the federal sphere:

- 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);
- Data Processing Federal Service (SERPRO), a company linked to the Ministry of Finance

These three organs have organized a Seminary, with the participation of entities of the federal government, in the ambit of the Executive Power, with the objective of forming an inter-organs committee – named Constituent Committee – to lead the initial works of assembling the architecture.

After its institutionalization, by means of the Normative Regulation n° 5, of July 14 2005, the same become to be named as e-PING Coordination. In addition to the three organizers, the following organizations have participated of such group: Presidency of the Republic, CEF, DATAPREV and the Brazilian Association of Information and Communication Technology State Entities (ABEP)

The committee has established the following work program:

- Definition of the Initial Form of Elaboration and Architecture Management of the e-PING;
- Definition of the segmentation of the subjects to be covered by e-PING;
- Creation of five workgroups responsible for the initial definitions of policies and technical specifications for each one of the segments;
- Establishment of a working schedule with the objective of elaboration and divulgation of the initial version of the architecture, named Version 0;
- Realization of a public enquiry and public audiences in RS, SP, DF, MG and PE (*states of the federation)*, in order to obtain contributions, from the general society, regarding to the proposed content of the Version 0;
- Publication of the Version 1, together with the resolution of institutionalization of the e-PING in the APF ambit – Executive Power;
- Publication of the Version 1.5, containing updates and revisions of the technical specifications and of the overview of the e-PING.
- Realization of a public enquiry and public audiences, in order to obtain contributions, from the general society, by the issuing of each new version of the reference document;
- Publication of annual version, containing the updates and revisions of the technical specifications and of the overview of the e-PING.

Similar experiences developed by governments in other countries are constantly researched. The e-GIF – Government Interoperability Framework – of the British government was adopted as basis for the construction of the interoperability architecture of the Brazilian government. The management of the e-PING is supported in the form implemented by the United Kingdom, in operation since the year of 2000, and, currently found in a maturity level internationally recognized as a reference.

5.2. Implantation strategy

The disclosure of standards and specifications established for Brazilian government follows the versioning scheme. It is foreseen the elaboration of an annual version, with intermediary publications of updates, whenever there are significant changes.

The present version has consolidated the work of groups assembled for the five segments defined. All its content was made available for Public Consultation, with the aim of obtaining contributions to the proposals of standards published in the 2010 draft version.

5.3. Management Model

In this item are specified the forms of management of the e-PING architecture, and lists the main tasks and how to implement these activities in the structural organization of the government.

5.3.1. Attributions

The e-PING management comprises the performance of duties of administrative and of technical order.

Among the **attributions of administrative character**, stand out:

- To define the strategic objectives and management of government for the establishment of the standards;
- To manage the interoperability architecture of the Brazilian government, providing the management infrastructure needed for its correct use and ensuring its updating, considering: the priorities and aims of govern, the needs of the society and the availability of new mature technologies supported by the ICT market;
- To act as a center of coordination of the e-PING architecture, pursuing the alignment of the interoperability efforts, ensuring the coherence of the initiatives carried out by the government organs;
- Specifically for the interoperability segments, to manage the relationship of the federal government – Executive Power – with the other instances defined in item 2 – Scope;
- To manage and make operational the divulgation of the e-PING standards, considering:
    - Creation and management of a site in Internet for the e-PING (http://www.eping.e.gov.br);
    - Coordination of the Public Consultation process.
    - Coordination of the process of receiving and evaluation of the proposals of changes and complementation;
    - Coordination of the process requesting suggestions for the e-PING;
    - Publication of the updated versions of the e-PING and the intermediary updates;
- To manage the interaction with initiatives with the same purpose, conducted by other governments in the country and abroad;
- To encourage the training of teams from the federal government, working together with the organs, both in consideration of the e-PING in the specific training plans of each one, and the implementation of corporative events aimed to disseminate the e-PING standards.
- To establish, implement and disseminate the indicators of monitoring of the results obtained with the implementation of the e-PING;
- To manage the interaction with specification organizations (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Normative Institutes of specific segments, such as ABNT, INMETRO, ISO, NIST, etc.). These organizations are chosen under e-PING coordination criteria, taking into account their notorious international recognition, competence in their acting area and the establishment of open standards.
- To manage the interaction with the national and international fomentation organs in order to channel resources, aiming to meet the needs of creation of infrastructure of the e-PING and promote research and development;
- To facilitate the deployment and manage the process of approval of the standards to be established for the government;
- To facilitate the implementation and to manage auditory processes performed with the purpose of verify the accession level to the e-PING recommendations and specifications.

- To act, cooperatively, as support to the government organs, in the realization of the processes needed for the adequacy to e-PING standards; evaluate the possibility of sponsoring comprehensive programs, which promote the intensive use of the standards proposed.

Among technical nature attributions are:

- To establish the ways for the elaboration and maintenance of the policies and technical specifications, which compose the e-PING, considering:
  - Identification, creation and management of specific Working Groups;
  - Establishment of agreements and definition of government institutions as responsible for the policies and technical specifications of specific components of the interoperability segments;
  - Identification and implementation of alternative forms of technical management of the subjects addressed by the scale of operation of e-PING;
- To coordinate the development and maintenance, in the federal government ambit – Executive Power, of:
  - Metadata Standards of the Government (e-PMG);
  - Controlled Vocabulary for the Electronic Government (VCGE);
  - Data Standards Catalog (CPD);
  - XML Schemas Reference Catalog;
  - Other standards for Organization and Exchange of Information;
  - Interconnection Standards;
  - Security Standards;
  - Standards of Means of Access to electronic government services;
  - Standards of use of Smart Cards, Tokens and other types of cards;
- To ensure the uniqueness of concepts, definitions and establishment of standards by part of the responsible for the technical segments defined for the e-PING.

5.3.2. Responsibilities

The government structure created for managing de e-PING is presented in the following simplified scheme:

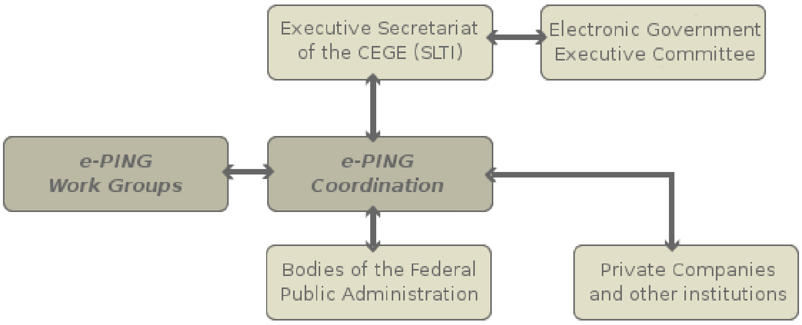
Executive Secretariat of the CEGE (SLTI)
Electronic Government Executive Committee
e-PING Work Groups
e-PING Coordination
Bodies of the Federal Public Administration
Private Companies and other institutions

Figure 2 – e-PING management.

The SLTI-MP, through the Information and Informatics Resource Administration SISP, instituted by the Decree 1048, of January 21, 1994 is in charge of the institutionalization and for the definition of the legal form of the e-PING Coordination.

The role of the e-PING Coordination will be guided by the following points:

- of the e-Egis, providing the activities needed for the consolidation of the current version and the dynamics of it evolution;
- Architecture Management of the e-PING;
- Establishment and management of the rules and of the institutional and legal

instruments, which ensure the effectiveness of the recommendations and specifications of the e-PING;

- Management of the standards seen in the e-PING;
- Guarantee of maintaining the updating of the various e-PING catalog;
- Management of the Communication and Divulgation process of the standards, decisions and of the activities of e-Egis, including the publication of new versions and of the intermediary updates;
- Creation of a e-PING label and management of process, which certifies the accession of a certain service or product to the e-PING;
- Provision of criteria and subsidies for the elaboration of the Annual Budget Law, by the federal government;
- Management of the process of hiring services and of establishment of agreements for the realizations of the attributions needed for the consolidation of the standards, as, for example, the evaluation of proposals of e-gov projects focused on the Federal Public Administration, homologation of the standards and verification conformity.
- Establishment of contact points with the several organs of the Federal Public Administration;
- Management of the Working Groups – WG, defining its composition and determining the working guidelines, based on the general technical and specific policies, in the govern needs and monitoring of the technological scenery.

The Working Groups of the e-PING, constituted of representatives indicated by the various FPA organs and of representatives of institutions from other levels of government, are in charge for:

- Treating the subjects that make up the segments of the e-PING;
- Systematically monitoring the market, specifically for the segments under its responsibilities, with the aim of detecting the needs for technological updates of the policies and technical specifications;
- To subside the actions of the e-PING Coordination, in the development of its administrative and technical attributions.

The Working Groups coordinators will have a seat in the e-PING Coordination.

5.4. Additional activities

In addition to the attributions of administrative and technical character for implementation and the evolutional maintenance of the e-PING architecture, other activities will be under the responsibility of the e-PING Coordination.

5.4.1. Selection and Homologation of the Technological Standards

The technical policies within this document establish the e-PING standards, being useful as a reference in the selection of the components for which the technical specifications are established.

The e-PING foresees an assessment process of the standards candidate to integrate the architecture. Such process covers the selection, homologation and of the specifications selected in five levels of situations, which characterize the accession degree to the technical, general and specific policies for each segment.

These five levels are the following:

- **Adopted (A):** item adopted by the government as standard in the e-PING architecture, and that have been submitted to a formal process of homologation performed by a government institution or by other institution with formal delegation, in order to perform the process. It is also considered approved when based on a proposition dully reasoned by the coordination of the segment, published in web site and approved by the e-PING Coordination;
- **Recommended (R):** item that meets the technical policies of the e-PING, is recognized as an item that should be used in the ambit of the government institutions, but not yet submitted to a formal homologation process;

- **In Transition (T):** item, which the government does not recommend, for not meeting to one or more requirements established in the general and technical policies of the architecture; it is included in the e-PING because of its significant use in government institutions, tending to be disabled as soon as any other component in one of the both aforementioned situations presents complete conditions to replace it. It can become to be considered a "recommended" component, if it would fit all the technical policies established. It should be noted that the development of new services or the reconstruction of significant parts of those already existing should avoid the use of components classified as transitional.
- **Under Study (S):** component, which is under evaluation and can be accommodated in one of the aforementioned situations, as soon as the evaluation process is completed;
- **Future Study (F):** posterior. Component not yet evaluated and that will be subject of further study.

The process of selection of the components selected by e-PING and its resultant classification in the above-indicated situations is in charge of the Working Groups composed by experts professionals with role in the government and in institutions with which is established any type of covenant or agreement.

The selection is made as from formalized suggestions, internal demands of the federal government organs, Executive Power and inquiries performed by the Working Groups.

In what is related to the homologation, this should be subject of more profound study by e-PING managers. In virtue of the large variety of components covered by the architecture, there will be the need of elaborating a systematic of homologation, which covers, since process in which will be indispensable the evaluation of the physical characteristics of determined components (Smart Cards, for example) up to others in which are required the examination of aspects that involve the use of the component in the development and construction of the services (information organization and exchange and security, for example).

In this case, the government will establish covenants or accredit institutions for development of conformance essays, always defining which components should be submitted to homologation processes, the criteria for the evaluation of the results and the conditions for the procedure performance.

The complete definition of the selection and homologation process, taking under consideration the segments specificities, will be in charge of the e-PING Coordination.

5.4.2. Conformity Auditing

Compliance with the specifications and recommendations by the federal agencies – Executive Power, is a critical factor of success in the implementation and consolidation of the e-PING. The managers of the e-PING will recommend the implementation of audit process for checking of the meets to the specifications and policies of the architecture.

There may be delegation of responsibilities to teams specially mounted for such finality, composed by technicians from the government with experience on proceedings of this nature.

The preferred way for the realization of this kind of procedure, however, will be the use of the own structures of the organs responsible for systems auditing. The e-PING Coordination will act in the sense of suggesting the basic criteria to be followed by the organs. To this end, it was constituted, by means of the Ordinance No. 8, October 31, 2008, the SLTI-MP, Working Group to study, analyze and propose the model of auditing regarding to the accession to the e-PING standards. This proposal will also include the maturity model of the e-PING (M-PING).

Other point to be considered will be the collaboration of government organs acting in the area, foreseeing contacts with institutions from other Powers and government levels.

5.4.3. Creation and Maintenance of the Site

The whole process of information exchanges about e-PING and users, collaborators and interested is performed, preferentially, through Internet, in http://www.eping.e.gov.br. In its more advanced stage of working, the e-PING site will have, as major functionalities:

- Full divulgation of the documentation related to the architecture: official versions and the relevant updates of the architecture, versions for public consultation, support technical documentation, correlate legal and institutional documentation;
- Availability of recommendations, determinations, technical specifications and policies for ends of validation, homologation and receiving of comments and suggestions by the society;
- Publication of request for comments related to the specification of components for the architecture;
- Availability of electronic means for receiving the suggestions;
- Availability of links to documents, standards, rules or any other type of reference in e-PING.

5.4.4. Legal and Institutional Follow-up

The e-PING will have constant support of the Juridical Advisory Body of the Ministry of Planning, Budget and Management in order to ensure the accession to the content of the documents that make up the architecture to the rules and legal instruments in force in country.

In addition, this Advisory will also have the responsibility to prepare the full institutional part needed to guarantee that the adequacies and recommendations of the e-PING come to be a set of legal instruments of ICT in country.

The Coordination of the e-PING will be able to act in the sense of establishing a way of collaboration with any other organ of the government, which has conditions to provide its juridical support structure for the realization of this activity.

5.4.5. Divulgation

Will be given full publicity to all content in e-PING. The main ways of divulgation foreseen, beyond the website, are:

- Realization of specific divulgation events , such as Seminaries, Workshops and general presentations;
- Participation in government events in ICT and correlate areas;
- Participation in events targeted to specific audience;
- Publication of all versions of the e-PING and the intermediary updates;
- Exchange with other levels and other Powers of the government, with public institutions, private and from the third sector and with governments of other countries.

5.4.6. Training

Events targeted to training will be part of the agenda for the implementation and management of the e-PING. Also, is foreseen the intensive use of On Distance Learning (ODL).

The Coordination of the e-PING will elaborate and publish a minimum training grade, so that each organ of the FPA to have subsides to plan and estimate investments needed for training professionals involved in the process of adequacy to the e-PING recommendations.

Each government organ will observe the standards definitions in the assembly of their own particular plans of training, ensuring the provision of adequate training to the elements of their technical teams.

5.5. Relationship with Government and Society

In this item are treated the forms of relationship of the e-PING with the entities, which compose the government and the society.

5.5.1. Federal Government Organizations – Executive Power

In the ambit of the Executive Power, the participation of all hierarchical levels of the Federal Public Administration, its agencies and regulatory organizations and the public companies and institutions is essential for the promotion and consolidation of the interoperability in public sector.

Although the overall guidelines are managed by the e-PING Coordination, each particular institution will have its responsibility in the management and guarantee of use of the e-PING standards. Among the attributions of this nature, stand out:

- To contribute for the development and continuous improvement of the e-PING;
- To ensure that their organizational ICT strategies consider that the integrant systems of services of electronic government under their responsibility are adequate to the recommendations of the e-PING;
- To have a plan of implementation and adequacy of the ICT infrastructure of the organization to the e-PING architecture.
- To ensure that the teams of the institution have domain over the abilities to define and use the specifications required for the interoperability, providing training support whenever needed;
- To establish a contact point in the institutions for the exchange of information and needs with the Coordination of the e-PING;
- To allocate and provide resources to give support to their processes of adequacy to the e-PING;
- To take the opportunity to streamline processes (because of the increased interoperability) in order to improve the quality and reduce the costs of the provision of the e-gov services.

5.5.2. Other Instances of Government (such as Federal Powers, State and Municipal Governments)

The adoption of the e-PING is obligatory to the organs and entities of the federal government – Executive Power. For the other Powers (Judiciary, Legislative) and other government levels (state and municipal) the adoption is facultative.

The Coordination of the e-PING acts proactively aiming the adoption of the e-PING by members integrant of other levels and powers, given the relevance of the exchange of information between the levels and powers for the efficiency, efficacy and effectiveness of the governmental acting and for the construction of the electronic government services oriented to the society, in special to the citizen.

To facilitate the adoption of the e-PING by the state governments, the ABEP makes part of the coordination of the e-PING, acting in collaboration with the coordination of the e-PING in the construction of a federative interests array for information exchange.

5.5.3. Private and Third Sector Organizations

The e-PING foresees the interaction with the Private Sector and with the Third Sector by means of mechanisms of Public Consultation, Comments Requests and Suggestions Receiving.

All entities of such nature that participate in bidding processes to provide products and services for the Federal Executive Power will have to meet the specifications and recommendations of the e-PING.

Other forms of participation of these institutions in the e-PING may be considered, establishing criteria that ensure the transparency and equity of opportunities.

5.5.4. Citizen

Electronic Government essentially means the government better serving to the needs of the citizen, using the resources of Technology, Information and Communication. The e-PING architecture enables the integration and makes available the services in a righteous, safe and coherent way, allowing for better levels of efficiency in the government.

The government should encourage the society to opine, comment and contribute with suggestions of innovations, which could help to improve the access to information and the delivery of its services. All the processes of divulgation and of inter-relationship of the e-PING foresee the active participation of the citizen and of the society in general, in the process of construction and management of the architecture.

Part II – Technical Specification of the e-PING Components

6. Interconnection

6.1. Interconnection: Technical Policies

The technical policies for interconnection are:

6.1.1. The FPA organs should interconnect using IPv4 and planning the future migration to IPv6. New network hiring and updates should provide support to the coexistence of the IPv4 and IPv6 protocols and to products that support such protocols.

6.1.2. The email systems should use SMTP/MIME for the transportation of messages. For the access to the messages, the protocols POP3 and/or IMAP should be used, being encouraged the use of web interfaces for the electronic mail, observed, when needed, the security aspects.

6.1.3. The FPA organs should comply with the domain naming policy of the federal government, established in the Resolution no. 7, which can be seen at the electronic address.

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

6.1.4. The DNS should be used for the resolution of domain names in Internet, converting them into IP address and, conversely, converting IPs in domain names, throughout the maintenance of direct and reverse maps, respectively.

6.1.5. The FTP and/or HTTP protocols should be used for transferring files, observing their functionalities for recovering of interruptions and security, when needed. HTTP should be prioritized for the transference of files arising from pages in websites.

6.1.6. Always that possible, it should be used technology based on the web in applications, which used previously Terminal Emulation.

6.1.7. The Web Services technology is recommended as a solution of interoperability of e-PING. It is recommended the use of the *Simple Object Access Protocol* (SOAP) for interconnection in non-centralized architectures and/or distributed for implementation of services in systems of any size. Alternatively, for small size web services, it is considered possible the development of designs based on REST, which uses the HTTP protocol.

6.2. Interconnection: Technical Specification

Table 1 – Interconnection Specifications – Messaging

Component	Specification	Sit	Observations

	A = Adopted
	R = Recommended
	T = In Transition
	E = In Study
	F = Future Study		

Addresses of electronic mailbox	The rules for the definition of mailbox names of electronic mail should follow to the established in the document “Individual-Functional Mailbox in the Federal Government”, available at the electronic address: http://www.e.gov.br/correios/cp_individ.htm	**A**	
Electronic Message Transportation	Use electronic messaging products that support interfaces in conformity with SMTP/MIME for the transference of correlate RFC messages: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 3676; RFC 2047; RFC 2231 (updates of the RFCs 2045, 2047 e 2183); RFC 2183; RFC 4288; RFC 4289; RFC 3023 e RFC 2049.	**R**	

Component	Specification	Sit	Observations
Mailbox Access	Unless security requirements determine otherwise, the mail programs that provide easy access to the correspondence should be, at least, in accordance to the POP3 for remote access to the mailbox. Correlate RFC: RFC 1939 (updated by the RFC 1957 and RFC 2449).	**T**	
	Whenever additional facilities are needed, unless security requirements establish otherwise, the mail programs that provide advanced facilities of access to the correspondence, should be in accordance to IMAP for remote access to the mailbox. Correlate RFCs: RFC 2342; RFC 2910 (updated by RFC 3510); RFC 2971; RFC 3501; RFC 3502 and RFC 3503.	**R**	
Real time messaging	The model and requirements for the Instant Messaging and Presence Protocol (IMPP) are defined by the RFC 2778 and RFC 2779.	**T**	
	The model and requirements for the Extensible Messaging and Presence Protocol (XMPP) are defined by the RFC 3920 and RFC 3921.	**R**	
Short Messages Service	The Short Messages Service (SMS) should use the SMPP protocol, as defined by the SMS Forum http://www.smsforum.net	**R**	

Table 2 – Interconnection Specifications – Network Infrastructure

Component	Specification	Sit	Observations

	A = Adopted
	R = Recommended
	T = In Transition
	E = In Study
	F = Future Study		

Transportation	TCP (RFC 793).	**A**	
	UDP (RFC 768) when needed, subject to security limitations.	**A**	
Intercommunication LAN/WAN	IPv4 (RFC 791).	**A**	
	IPv6 (RFC 2460).	**E**	
Advanced traffic	When needed, the network traffic may be optimized with MPLS (RFC 3031), and should have, at least, a minimum of four service classes.	**A**	
Service quality	Adoption of a differentiated architecture for services by the use of the Diffserv (RFC 2475).	**E**	
Wireless metropolitan network	IEEE 802.16, in conformity with the determination of the WiMax Forum (http://www.wimaxforum.org) and with Anatel rules (http://www.anatel.gov.br).	**E**	
Local wireless network	IEEE 802.11 b/g, in conformity with the determination of the Wi-Fi Alliance (http://www.wi-fi.org) and with Anatel rules (http://www.anatel.gov.br).	**R**	
Access network via electric cabling	Power Line Communication (PLC), according to the Anatel rules (http://www.anatel.gov.br) and Aneel rules (http://www.aneel.gov.br).	**F**	

Table 3 – Interconnection Specifications – Network Services

Component	Specification	Sit	Observations

	A = Adopted
	R = Recommended
	T = In Transition
	E = In Study
	F = Future Study		

Hypertext transference protocol	Use HTTP/1.1 (RFC 2616).	**A**	
File transference protocol	FTP (RFC 959 e RFC 2228) (with re-initialization and retrieving) and HTTP (RFC 2616) for file transference	**R**	
Directory	LDAP v3 should be used for general access to the directory, according to RFC 4510.	**A**	
Time synchronism	RFC 1305 IETF - *Network Time Protocol* - NTP version 3.0. RFC 4330 IETF - *Simple Network Time Protocol* - SNTP version 4.0.	**R**	
Domain Naming Service	DNS should be used for the resolution of domain naming in internet according to RFC 1035. In its turn, the policy of domain naming of the Brazilian government is found in the Resolution no. 7 of the Executive Committee of Electronic Government, at the electronic address https://www.planalto.gov.br/ccivil_03/Resolução/2002/RES0_7-02web.htm. In addition to those policies, by decision of the Internet Management Committee in Brazil, the domain naming complies with the guidelines of the Ministry of Planning, Budget and Management, which is responsible for managing de domain .GOV.BR. The particularities of other government levels, such as, for example, the domains of the governments of the Federation Unities, which include the acronym of UF in the composition of the addresses are covered in the electronic address http://registro.br/faq/faq1.html#12.	**A**	
Signaling protocols	Use of the Initiation Session Protocol (SIP), defined by the RFC 3261, as control protocol in the application layer (signaling) for creating, modifying and terminating sessions with one or more participants.	**R**	
Network management protocols	Use of the SNMP protocol, defined by the RFCs 3411 and 3418, as network management protocol	**T**	Version 2
		R	Version 3
Protocol for the exchange of structured information in decentralized platform and/or distributed	SOAP v1.2, as defined by the W3C http://www.w3.org/TR/soap12-part1/. http://www.w3.org/TR/soap12-part2/. SOAP protocol specifications can be found in http://www.w3.org/TR/soap12-part0/.	**A**	

Component	Specification	Sit	Observations
Network traffic analysis protocol	IPFix	**F**	

6.3. Electronic Message (email)

For purposes of clarity, the e-PING will use the following concepts:

Electronic Message Transportation

The electronic message transportation is defined as an interface between two mail systems.

Mailbox access

The mailbox access is defined as an interface between a mail client and a mail system.

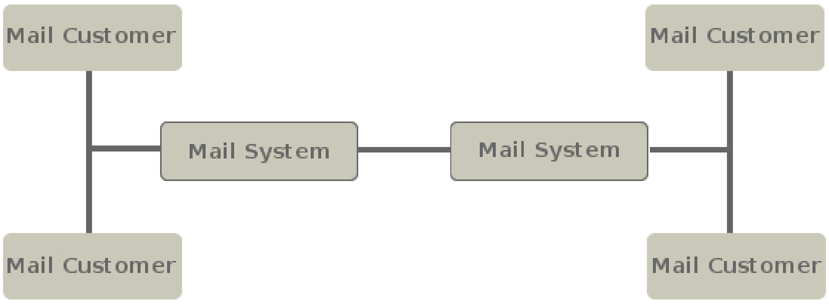

Figure 3 – Interfaces between systems and mail clients.

6.4. VPN

Virtual Private Network (VPN) is a privative virtual tunnel constructed over the infrastructure of a public or private network. Instead of using dedicated circuits or package networks to connect remote networks, it is usually used the Internet infrastructure.

Such use, as connection infrastructure between private network hosts is a good solution in what concerns to costs, but not in terms of privacy, since data in transit may not be read by any equipment, because the use of VPN is needed.

The virtual tunnels carry encrypted data on public or private networks, providing a secure virtual channel throughout such networks. Therefore, protocols are used for tunneling.

The devices responsible for the management of the VPN should be able to guarantee privacy, integrity and authenticity of data.

The VPN specifications are presented in the security segment.

6.5. Peer-to-peer networks

Peer-to-peer systems (P2P) are distributed systems, which consist of interconnected nodes with the ability to self-organize in network topologies, with the objective of sharing resources such as processing, storage and band width, able to adapt themselves to failures and accommodate transient populations of nodes, while keeping acceptable connectivity and performance, not depending on the intermediation or support of a central authority (server).

Although P2P systems can contribute for sharing of resources and collaboration in a large scale, with decentralized control and low coupling, they are still susceptible to several security problems, precluding the systematic use of P2P networks. This subject will be covered in a future time.

7.Security

7.1. Security: Technical Policies

7.1.1. Data, information and systems of information of the government should be protected against threats in order to reduce risks and ensure the integrity, confidentiality, availability and authenticity.

7.1.2. Data and information should be kept with the same level of protection regardless the medium in which they are processed, storage or traveling.

7.1.3. Sensitive information, which travels over insecure networks, including wireless ones, should be encrypted, in an appropriate way, according to the security components specified in this document.

7.1.4. The security requirements for the information, services and infrastructure should be identified and treated according to the classification of the information, defined service levels and result of risk analysis.

7.1.5. Security should be treated as preventive. For systems that support critical processes, there should be elaborated plans of continuity, in which residual risks are treated, aiming to meet the minimum production level.

7.1.6. Security is a process that should be inserted in each step of the development cycle of a system.

7.1.7. Systems should have historic records (logs) in order to allow auditing and material evidences, and it is indispensable the adoption of a centralized time synchronism system, as well as mechanisms should be used, which ensure the authenticity of the stored records.

7.1.8. The XML security services should be in conformity with the W3C specifications.

7.1.9. In metropolitan wireless networks, it is recommended the adoption of random values in the security associations, different identifiers for each service and limiting the lifetime of the authorization keys.

7.1.10. The use of cryptography and digital certification, for traffic protection, data storage, access control, digital signature and code signature, should be in conformity with the ICP-Brazil rules.

7.1.11. The documentation of the systems, of the security controls and environment topologies should be kept updated and protected, maintaining the compatible degree of secrecy.

7.1.12. Users should know about their responsibilities related to security and should be trained for performing their tasks and correct use of the mediums of access.

7.1.13. The FPA organs, aiming the improvement of security, should have as reference the following norms: NBR ISO/IEC 27002:2005 – code of practice for the management of information security; NBR ISO/IEC 27001:2006 – information security management systems; NBR 15999-1:2007 and 15999-2:2008 – business continuity management; NBR ISO/IEC 27005:2008 – information security risk management; Normative Instruction no. 01/2000, Complementary Norm no. 02/2009, 04/2009 and 05/2009.

7.1.14. For specifications about smart cards and tokens, there will should be adopted the requirements contained in the normative ones, which treat of the homologation of equipments and systems in the ambit of the infrastructure of the Brazilian Public Keys – ICP-Brazil (http://www.icpbrasil.gov.br/). These requirements, observed for products approved in the ICP-Brazil, such as medias that store the digital certificates and the respective readers, in addition to the systems and equipments needed for performing digital certification, establish standards and minimum technical specifications, with the purpose of ensure its interoperability and the reliability of the resources of information security used by them. It is important to note that data stored in a certain smart card or token should not be able to be protected by any kind of licensing, which prohibits its reading by any software other than that of the supplier of the smart card or token.

7.2. Security: Technical Specifications

Table 4 – Security Specifications – Data communication

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Transference of data through insecure networks by HTTP, LDAP, IMAP, POP3, Telnet. protocols	TLS – Transport Layer Security, RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt). If it is necessary the TLS v1 protocol, it can emulate the SSL v3. HTTP on TLS, RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt) Able to implement the following encrypted algorithms: - Algorithms for changing session keys during the handshake: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA; - Algorithms for defining encryption keys: RC4, IDEA, 3DES e AES; - Algorithms that implement the hash function to define the MAC: SHA-256 or SHA-512. - Type of Digital Certificate - X.509 v3 - ICP-Brazil, http://www.iti.gov.br SASL - Simple Authentication and Security Layer, RFC 4422 (http://www.ietf.org/rfc/rfc4422.txt).	**R**	
Security of IPv4 networks	IPSec Authentication Header RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) and RFC 4835 (http://www.ietf.org/rfc/rfc4835.txt) for authentication of the IP header. IKE – Internet Key Exchange, RFC 4306 (http://www.ietf.org/rfc/rfc4306.txt), should be used whenever necessary for negotiate the security association between two entities to exchange the keying material. ESP – Encapsulating Security Payload, RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt) Requirement for VPN – Virtual Private Network.	**A**	
Security of IPv4 networks for application protocols	The S/MIME v3 ,RFC 2633 (http://www.ietf.org/rfc/rfc2633.txt) should be used when appropriate for security of general government messages.	**A**	

Component	Specification	Sit	Comments
Security of IPv6 networks in network layer	The IPv6 defined in the RFC 2460 (http://www.ietf.org/rfc/rfc2460.txt) presents native security implementations in the protocol. The IPv6 specifications defined two security mechanisms: the header authentication (HA) RFC 4302 (http://www.ietf.org/rfc/rfc4302.txt) or IP authentication, and the IP encapsulation security, ESP (Encrypted Security Payload) RFC 4303 (http://www.ietf.org/rfc/rfc4303.txt).	**R**	

Table 5 – Security Specifications – Electronic Mail

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Mailbox access	The access to the mailbox will take place through the client of the electronic mail sofware. When it is not possible to use the specific client or it is necessary to access the mailbox through non-secure networks (for example, Internet), HTTPS should be used, according to the standards of transport security described in the RFC 2595 (http://www.ietf.org/rfc/rfc2595.txt), which treats of the use of TLS with IMAP, POP3 e ACAP.	**A**	
Email content	The S/MIME V3 should be used whenever appropriate for the security of general government messages. This 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**	
Email transport	Use SPF (Sender Policy Framework) in the terms of the RFC 4408 (http://www.ietf.org/rfc/rfc4408.txt).	**R**	
Signature	Use the standard certificate ICP-Brazil for email signature, when required. Accordingly, to what disposed in the Provisory Order no. 2200-2, of August 24, 2001 and Decree no. 2996 of October 31, 2001.	**A**	See Resolution no. 65, of July 9, 2009, of the Manager Committee of Infrastructure of Public Keys – ICP-Brazil.

Table 6 – Security Specifications – Cryptography

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Ciphering algorithm	3DES or AES	**R**	
Signature/hashing algorithm	SHA-256 or SHA-512	**R**	The systems should have support for the MD5 hash algorithm with RSA, to ensure compatibility with previous implementations
Signature/hashing algorithm	SHA-224 or SHA-238	**E**	Whereas were included in the Final Report of the Encryption Working Group I, set up by the Institutional Security Office of the Presidency of the Republic, however, still have not become standard in the Federal Public Administration.
Algorithm for transportation of cryptographic key of content/session	RSA	**A**	
Cryptography algorithms based on elliptical curves	ECDSA 256 and ECDSA 512 (RFC 5480 – http://www.ietf.org/rfc/rfc5480.txt). ECIES 256 and ECIES 512 (Resolution no., of July 9, 2009, of the Manager Committee of Infrastructure of Public Keys – ICP-Brazil. ECMQV and ECDH, both for agreement of keys according to RFC 3278. (http://www.ietf.org/rfc/rfc3278.txt).	**A** **E**	ECDSA, for digital signatures and ECIES for ciphering and secure transportation of cryptographic keys. See errata for RFC 5480 in http://rfc-editor.org/errata_search.php?rfc=5480.
Security requirements for cryptographic modules	Homologation of ICP-Brazil NSH-2 and NSH-3; FIPS 140-1 and FIPS 140-2.	**R**	See Resolution no. 65, of July 9, 2009, of the Manager Committee of Infrastructure of Public Keys – ICP-Brazil.

Table 7 – Security Specifications – Systems Development

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

XML Signatures	Syntax and Processing of XML signature (XMLsig) as defined by W3C http://www.w3.org/TR/xmldsig-core/	**A**	
XML Ciphering	Syntax and Processing of XML Ciphering (XMLenc) as defined by W3C http://www.w3.org/TR/xmlenc-core/	**R**	
XML signature and ciphering	Transformation and deciphering of XML signature as defined by W3C http://www.w3.org/TR/xmlenc-decrypt	**R**	
Main XML managements when PKI environment is used	XML – Key Management Specification (XKMS 2.0) (Specification and management of XML key) as defined by W3C http://www.w3.org/TR/xkms2/	**R**	
Authentication and authorization of XML access	SAML – as defined by OASIS when an ICP environment is used http://www.oasis-open.org/committees/security/index.shtml	**R**	
Identity Intermediation or Federation	WS-Security 1.1 – framework of standards to ensure integrity and confidentiality of SOAP messages. (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf). WS-Trust 1.3 – extensions for the WS-Security standard, defining the use of security credentials and trust management distributed. (http://docs.oasis-open.org/ws-sx/ws-trust/200512).	**R**	The previous component (SAML) may join this component after studies.
Browsers	Only use connection witness of permanent character (*cookies*) through user's allowance. Resolution no. 7 Executive Committee of the Electronic Government (Chapter II, Art.7th).	**A**	

Table 8 – Security Specifications – Network Services

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Directory	Normative No. 2, of October 3, 2002 – Published in the Union Official Diary (D.O.) in October 4, 2002, Section 1, page 85 LDAPv3 RFC 2251 (http://www.ietf.org/rfc/rfc2251.txt). LDAP v3 extension to RFC2830 (http://www.ietf.org/rfc/rfc2830.txt).	**R**	

Component	Specification	Sit	Comments
DNSSEC	Resolution no. 7 of July 29, 2002 –Executive Committee of Electronic Government Security Practices for Internet Network Managers Center of Studies, Responses and Treatment of Security Incidents in Brazil – CERT.BR http://www.cert.br/docs/seg-adm-redes/seg-adm-chklist.pdf Version 1.2, May 16, 2003.	**R**	
File transference in secure way	HTTPS RFC 2818 (http://www.ietf.org/rfc/rfc2818.txt).	**R**	
File transference in secure way	SSH FTP	**E**	Documents are still in draft format.
File transference in secure way	Securing FTP with TLS, RFC 4217 (http://www.faqs.org/rfcs/rfc4217.html) and RFC 2246 (http://www.faqs.org/rfcs/rfc2246.html)	**E**	
Instantaneous 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 synchronism	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**	The time stamping time should be in accordance to the Resolution no. 58, of November 28, 2008 and other ICP-Brazil rules.

Table 9 – Security Specifications – Wireless network

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Wireless MAN[1] 802.16-2004[2] 802.16.2-2004[3] 802.16e[4] and 802.16f[5]	Use PKM-EAP (Privacy Key Management - Extensible Authentication Protocol) com: • EAP – TLS or TTLS; • AES[6] (Advanced Encryption Standard).	**E**	

[1] O 802.16 is defined by IEEE as a technological interface for wireless metropolitan access networks (WMAN)

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

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

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

Component	Specification	Sit	Comments
Wireless LAN 802.11	Use specification WPA2 (Wi-Fi Protect Access).	**R**	

Table 10 – Security Specifications – Response to Information Security Incidents

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Record preservation	Guidelines for Evidence Collection and Archiving, RFC 3227 (http://www.ietf.org/rfc/rfc3227.txt).	**R**	
Treatment and response to incidents in computer networks	Expectations for Computer Security Incident Response, RFC 2350 (http://www.ietf.org/rfc/rfc2350.txt). Creation of treatment and response teams for incidents in computer networks according to the Complementary Norm no. 05/09 (http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf).	**R**	
Computer Forensic	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**	

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

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

8. Means of Access

8.1. Means of Access: Technical Policies

The technical policies for allowing access to the electronic services of the federal government to general society – citizens and other levels of government, other Powers, civil servants, private companies and other institutions are:

8.1.1. The information systems of the government should be designed in order to respect Brazilian laws, providing accessibility resources to the citizens with special needs, to minority ethnical groups and to those under risk of social or digital exclusion. The service via counter service should be considered in its whole coverage, in order to enable the benefits of the use of electronic government services are extended to the population that may not have direct access to these services by means of the foreseen precepts.

8.1.2. Information systems of the government that provide electronic government services:

- when using Internet as a means of communication and workstations as access device, will be preferentially designed to provide access to information through the use of web technologies and communication protocols based on browsers;
- when using other access devices, as, for example, cell phones and digital TV, other interfaces can be used, in addition to the web browsers;
- should be designed to provide the users with the electronic government services by means of various means of access;
- in this version, the e-PING treats of the following means of access:
  - Workstations;
  - Mobility;
  - Digital TV.

8.1.3. The information services of the government, made to support a certain access device, should follow, obligatorily, the specifications published in the e-PING for such device.

8.1.4. All information systems of the government, which provide electronic services, should be able to use the Internet as a means of communication, both directly and by means of third party services.

8.1.5. The development of electronic government services should be guided in order to provide services to users that do not have access to the most recent technologies available in market. In other hand, it also should be considered the necessity of serving those users owners of special needs, requirement that involves the use of resources that are more sophisticated and of specific use. In order to conciliate these needs, there should be observed the recommendations of the Accessibility Model of Electronic Government (e-AMG)[7].

8.1.6. When Internet is used as a means of communication, the government information systems should be designed so that the maximum of information can be worked from browsers that meet the minimum standards expressed by the support to the relevant technical specifications foreseen in Section 8.2. In addition, e-PING recommends that all electronic government service to specify, clearly and, preferentially in its home page, the minimum browsers versions, which support the functionalities required by the associate service.

To meet the minimum standard aforementioned must be considered the exceptions that involve security subjects in the treatment of information.

8.1.7. When Internet is used as a means of communication, middleware or additional plug-ins should be used, if there is no alternative technically viable, in order to optimize the browsers functionalities in workstations. In this case, this additional sofware should be offered without payment of license fee and should comply with all relevant technical specifications listed separately in the e-PING. In addition, should be available a secure repository maintained by the governmental agency responsible for the application.

8.1.8. The services of electronic government should be designed in order to ensure for the users, the authenticity of the content, by means of emission of a digital certificate, according to the standards advocated by ICP-Brazil. Reference: http://www.icpbrasil.gov.br/. In this sense, all websites should use obligatorily "https" instead of "http".

8.1.9. The society needs, together with the possibility of the government developing and implanting the electronic services will support the definition of the technical specifications required by the available means of access. Techniques of content management and technologies that enable adaptation of devices to support the electronic government services can be used to facilitate the access by means of the minimum standard of web browsers (according to item 3: General Policies) and to make viable the use of public call-boxes, service counters and Service Centers for the citizens (as, for example, Tele-centers).

8.1.10. Information systems of the federal government should foresee, whenever necessary and when technically and economically viable, the construction of adapters to permit the access to the information of the electronic services in the web for a diversity of environments, presenting acceptable response times and reduced costs.

Such adaptors should be used to filter, convert and re-format, dynamically, the web content, in order to adapt to the requirements and display capabilities of the access device. In addition, they can enable the modification of the content of a web page, based on data protocols, XML, XSL, users' preferences and customization of network and access devices.

These adaptors can also be used as an alternative way to enable the access to ethnical minorities, visual deficiency holders (for example, through the use of text translators, larger graphics and fonts, audio, etc.). Such features are covered by the Resolution no. 8 of the Executive Committee of the Electronic Government. Reference:

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

8.1.11. Will be considered preferential those file types that have “xml” as default marshaling, in order to facilitate the interoperability between the electronic government services.

8.1.12. The electronic government services, which make available documents to their users, should do it using the actual link to access the document, clear information related to its provenance, version, publication date and format. For publication data, it is understood to be the one in which the document was published in an official diary, for cases in which such measure is required, or the date of available in the site, for the other cases. Other information about the document, such as author, editor, issuer, topical date or other relevant ones for its precise characterization should be in the properties field of the document itself.

8.2. Means of Access: Technical Specification for Workstations

For the elaboration of document drafts or works that need to be created collaboratively by more than one person and/or agency, the formats foreseen in Table 11 can be used.

As for the preparation of the final version of the documents, it must be sent to other organs or even digitally filed, and is recommended the use of the pdf/a format. Documents that need integrity and/or authoring guarantee, in addition of being in pdf/a format, must be digitally signed by their author, using the ICP-Brazil certificate.

The mention to products, which generate the file formats cited in Table 11, has as only objective the identification of a **minimum reference** from which the e-gov services should exchange information, being able to receive and send files in **versions equal or posterior** to the ones mentioned.

Table 11 – Specifications for Means of Access – Workstations

Component	Specifications	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Browsers	Should be concerned to the W3C standards and to the items *Browsers Adoption* and *Preferential Adoption of Open Standards*, in General Policies.	**R**	
Characters and alphabets sets	UNICODE standard version 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	**R**	
Hypertext exchange format	HTML version 4.01 (.html or .htm), generated according to the specifications of the W3C[7].	**A**	
	XHTML versions 1.0 or 1.1 (.xhtml), generated according to the specifications of the W3C[8].	**R**	
	XML versions 1.0 or 1.1 (.xml), generated according to the specifications of the W3C[9].	**A**	
	SHTML (.shtml).	**R**	
	MHTML (.mhtl or.mht)[10].	**T**	
Document type files	XML versions 1.0 or 1.1 (.xml), or with formatting (optional) (.xsl), generated according to the specifications of the W3C [14].	**R**	
	Open Document (.odt), generated according to the specifications of the standard ISO/IEC 26300[11].	**A**	
	Rich Text Format (.rtf).	**T**	
	PDF (.pdf).	**T**	
	PDF open version PDF/A[12].	**R**	
	Plain text (txt).	**A**	
	HTML version 4.01 (.html or.htm), generated according to the specifications of the W3C.	**R**	
Worksheet type files	Open Document (.ods), generated according to the specifications of the ABNT NBR ISO/IEC 26300 standard.	**A**	

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

[8] *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 in: http://www.w3.org/TR/xhtml1/.

[9] *Extensible Markup Language (XML) 1.0 (Third Edition) - W3C Recommendation 04 February 2004*. Available in: 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 in: http://www.w3.org/TR/2004/REC-xml11-20040204/.

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

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

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

Component	Specifications	Sit	Comments
Presentation type files	Open Document (.odp), generated according to the specifications of the ABNT NBR ISO/IEC 26300 standard.	**A**	
	HTML (.html or.htm), generated according to the specifications of the W3C.	**R**	
“Database” type files for workstations	XML versions 1.0 or 1.1 (.xml)	**R**	In the options of plain text (txt) and csv, should be included, obligatorily, the fields layout, in order to enable its treatment.
	MySQL Database (.myd, .myi), generated in MySQL formats, version 4.0 or superior.	**R**	
	Plain text (.txt).	**A**	
	Plain text (.csv) – comma-separated values.	**A**	
	Database file (.odb), generated according to the specification of ISO/IEC 26300 standard.	**R**	
Exchange of graphics and static images information	PNG (.png), generated according to the specifications of the W3C[13] – ISO/IEC 15948:2003 (E).	**A**	
	TIFF (.tif)[14]..	**R**	
	SVG (.svg), generated according to the specifications of the W3C[15].	**R**	
	JPEG File Interchange Format (.jpeg, .jpg or .jfif) [16].	**R**	
	Open Document (.odg), generated according to the ABNT NBR ISO/IEC 26300 standards.	**A**	
	BMP (.bmp).	**T**	
	GIF (.gif), generated according to the specifications GIF87a e GIF89a[17].	**T**	
Vector graphics	SVG (.svg), generated according to the specifications of the W3C.	**R**	
	Open Document (.odg), generated according to the ABNT NBR ISO/IEC 26300 standards.	**R**	
Specification of animation standards	SVG (.svg), generated according to the specification of the W3C.	**R**	
	GIF (.gif), generated according to the specification GIF89a.	**T**	

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

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

[15] *Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Disponível em: http://www.w3.org/TR/2003/REC-SVG11-20030114/*. Acesso em: 7 dez. 2005.

[16] *JPEG File Interchange Format (version 1.02) 1 September 1992. Disponível em: http://www.jpeg.org/public/jfif.pdf*. Acesso em: 7 dez. 2005.

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

Component	Specifications	Sit	Comments
Audio type and Video type files	.mpg	**R**	
	Áudio e vídeo MPEG-4, Part 14 (.mp4)[18]	**R**	
	MIDI (.mid)[19]	**R**	
	Áudio Ogg Vorbis I (.ogg)[20]	**R**	
	Audio-Video Interleaved (.avi), with Xvid encoding.	**R**	
	Audio-Video Interleaved (.avi), with divX encoding.	**T**	
	Audio MPEG-1, Audio Layer 3 (.mp3)[21]	**T**	
	WAVE (.wav)	**T**	
Compression of files of general use	ZIP (.zip).	**R**	
	GNU ZIP (.gz).	**R**	
	TAR Package (.tar).	**R**	
	Compressed TAR package (.tgz or .tar.gz).	**R**	
	BZIP2 (.bz2).	**R**	
	Compressed TAR Package com BZIP2 (.tar.bz2).	**R**	
	MS Cabinet (.cab).	**T**	

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

[19] Musical Instrument Digital Interface, conforme a especificação *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., Nov. 2001. Available in: http://www.midi.org/about-midi/specinfo.shtml. Access in: May 30. 2007.

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

[21] *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	Specifications	Sit	Comments
Geo-referenced information – file standards for exchange between workstations	GML version 2.0 or superior[22].	**A**	Indicated for complex vector structures involving geographic primitives, such as polygons, point, lines, surfaces, collections and numerical or textual attributes with no limitation in the number of characters.
	ShapeFile[23].	**A**	Indicated for vector structures limited to lines, points and polygons, whose textual attributes do not overcome 256 characters. Also, can store the M and Z dimensions.
	GeoTIFF[24].	**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 applications will store (create, update and delete) and access geographic features in object-relational database management systems, the data. OpenGIS Simple Features are described using spatial data elements such as points, lines and polygons.
Extended programming (Plug-ins)	Subject for future consideration	**F**	

8.3. Means of Access: Technical Specifications for Mobility

The amount of mobile phone devices has already exceeded the amount of fixed telephony, becoming, thus, a wide channel of communication with the citizen. In addition, the provision of personal computers with mobility resources, at more accessible prices for the citizen, is growing every day, motivated by governmental incentives and reduction in the production costs. Thus, it is a great challenge for the government to enable the access to the society to the products and services of the electronic government, from mobile devices, generally portable, such as notebooks, cell phones, smart phones and similar, aiming the increase in the digital inclusion via mobility.

A concept, which has been consolidated for the users application interface, is the “universal web”, which is supposed to be for everyone, in any place, at any moment, regardless the access device. Such concept must be applied to the services to be making available by means of mobile devices.

[22] *Geography Markup Language*. Specifications available in: http://www.opengeospatial.org/standards/gml.

[23] *ESRI Shapefile Technical Description*. Disponível em: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf.

[24] *GeoTIFF Format Especification*. Available in: http://remotesensing.org/geotiff/geotiff.html.

Table 12 – Specifications for Means of Access – Mobility

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Transmission protocol	Should be adhering to the W3C standards – *Mobile Best Practices* 1.0, available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Browser	Should be adhering to the W3C standards – *Mobile Best Practices* 1.0, available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Hypertext standard	Should be adhering to the W3C standards – Mobile Best Practices available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Extended programming	Should be adhering to the W3C standards – Mobile Best Practices available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Messaging	Should be adhering to the W3C standards – Mobile Best Practices available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Video and Audio files	Should be adhering to the W3C standards – *Mobile Best Practices* 1.0, available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
Image files	Should be adhering to the W3C standards – Mobile Best Practices 1.0, disponíveis no endereço eletrônico: http://www.w3.org/TR/mobile-bp	**R**	
Office files	Should be adhering to the W3C standards– Mobile Best Practices available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	
PDF Reader	Should be adhering to the W3C standards– *Mobile Best Practices* 1.0, available at the electronic address: http://www.w3.org/TR/mobile-bp	**R**	

8.4. Means of Access: Technical Specifications for Digital TV

Given the high level of presence of receivers of television signals in Brazilian homes and the eminent implementation of the Digital TV Brazilian System, which allows interaction with the audience, this comes to be a channel of great potential for the relationship between government and society. Thus, new possibilities arise for the access to the products and services of the electronic government, form the new Digital TV devices.

Its use provides much more than a quality signal, it provides interactivity and accessibility with Commercial Services such as: shops, games and access to banks, and also to Social Services, such as: consultations to the FGTS, PIS, Social Programs of the government, tele-learning among others, making the citizens to turn from an essentially passive activity to a participative activity.

Digital TV becomes a communication standard in different perspectives such as: technological, through the migration from analogical system to digital; economical, with the migration of new possibilities of services and business; social, through the provision of a diversity of contents and digital inclusion by using Internet through the TV device; political, with the possibility of encouraging the discussion of a new regulatory mark and behavioral, with the possibility of active participation by the audience through the use of different levels of interactivity in Digital

TV.

To meet technical subjects, the Brazilian System of Terrestrial Digital TV Forum – SBTVD, published with the Technical Norms Brazilian Association – ABNT, groups several norms in the site: http://www.forumsbtvd.org.br/materias.asp?id=112, in which is referenced a standardized and royalty free set of specifications, named GINGA.

Table 13 – Specifications for Mean of Access – Digital TV

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Transmission	**ABNT NBR 15601** Part 1 – Transmission System.	**R**	
Cryptography	**ABNT NBR 15602** Part 1 –Video encoding. Part 2 –Audio encoding. Part 3 –Signal Multiplexing System.	**R**	
Multiplexing	**ABNT NBR 15603** Part 1 –Broadcasting system information services. Part 2 –Syntaxes and definitions of the IS basic information. Part 3 – Syntaxes and definitions of the IS extended information.	**R**	
Receivers	**ABNT NBR 15604** Part 1 – Receivers.	**R**	
Security	**ABNT NBR 15605** Part 1 – Security topics.	**R**	
Middleware	**ABNT NBR 15606** Part 1 – Data encoding. Part 2 – Ginga-NCL for fixed and mobile receivers– XML application language for encoding of applications. Part 3 –Specification for data transmission. Part 5 – Ginga-NCL for portable receivers– XML application language for encoding of applications.	**R**	
	Part 4	**F**	
Interactivity Channel	**ABNT NBR 15607** Part 1 – Protocols, physical interfaces and software interfaces.	**R**	
Operations guide	**ABNT NBR 15608** Part 1 – Transmission System –Guide for implementation of the ABNT NBR 15601. Part 2 –Video, audio and multiplexing encoding – Guide for implementation of the ABNT NBR 15602. Part 3 –Multiplexing and Information service (IS) – Guide for implementation of the ABNT NBR 15603.	**R**	

9. Organization and Exchange of Information

9.1. Organization and Exchange of Information: Technical Policies

The technical policies for systems of 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 (when appropriate) to define the data for exchange.

9.1.3. Use of XSL for data transformation.

9.1.4. Use of a metadata standard for management of electronic contents.

9.2. Organization and Exchange of Information: Technical Specifications

Table 14 – Specifications for Organization and Exchange of Information

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Language for data exchange	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**	
Definition of data for exchanging	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**	
Description of data	RDF (Resource Description Framework) as defined by the W3C.	**F**	
Metadata elements for contents management	MSEG (Metadata Standard for the Electronic Government).	**E**	
Taxonomy for navigation	LAG - *Lista de Assuntos do Governo* – List of Government Affairs (LGA), Version 1.0. According to definition in http://www.eping.e.gov.br	**A**	In 2010, LAG will become to be named VCGE – Controlled Vocabulary of the Electronic Government

Component	Specification	Sit	Comments
Identifiers resolution systems	Handle system (http://www.handle.net).	**E**	

9.3. Notes about XML and *Middleware*

Not all systems need to be able to communicate directly in XML, as showed in Figure 4. When appropriate, it is acceptable the use of *middleware*, according to the illustration in Figure 5.

Although the configurations below present potential solutions, the direct XML model (Figure 4) is preferential, being possible the use of the indirect model, presented in Figure 5, in cases in which there are fundamental reasons to justify its use.

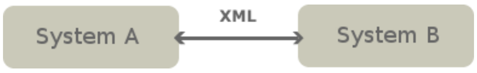

Figure 4 – Direct XML Model – Direct Exchange.

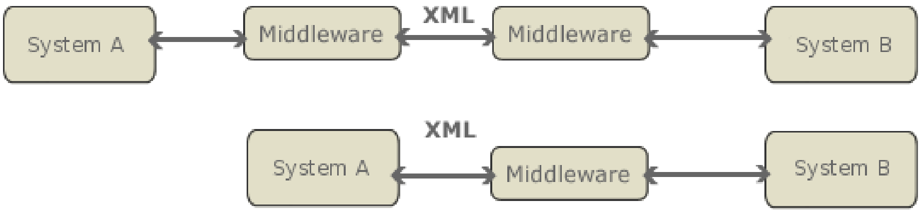

Figure 5 – Exchanges via middleware*.*

In specific cases, such as those needing the transference of a large amount of data between systems in a short time and in the exchanges in which the response time is critical, the adoption of XML as exchange language would occur gradually.

It is important to highlight that XML is adopted in e-PING as a data exchange language. For solution of interoperability (interconnection), observe items 6.1.7 and 10.1.4 with respect to Web Services and SOAP.

9.4. Note about UML use

For description of complex data, aiming a better explanation, it is recommended, when appropriate, the use of the UML classes' diagram.

9.5. Note about LAG

In 2010, LAG will be known as VCGE – Controlled Vocabulary of the Electronic Government.

10. Integration Areas for the Electronic Government

10.1. Integration Areas for the Electronic Government: Technical Policies

10.1.1. this segment, are treated the components related to subjects cross-cutting the Acting Areas of Government, whose standardization is relevant for the interoperability of the Electronic Government Services, such as Processes and Geographic Information.

10.1.2. As a technical guideline for the integration of information systems, it is recommended the gradual adoption of the Services-Oriented Architecture (SOA), having as reference for implementation, the "**Referential Architecture for Interoperability of Computerized Systems of Government (RA)**", which is a model of Services-Oriented Architecture, adapted to the reality of the Computerized Systems of the Federal Government, available in the website: http://www.eping.e.gov.br.

10.1.3. The e-PING architecture – Interoperability Standards of Electronic Government advocates the adoption of XML and the development of XML Schemas as fundaments for the electronic integration and interoperability of the government

10.1.4. It is recommended the use of *Web Services* for integration demands between the information systems of the government. So that, regardless the technologies in which they were implemented, a standard of interoperability may be adopted, which ensures scalability, usability, in addition to enable simultaneous updates in real time.

10.1.5. It is available in the Electronic Government Portal, the **Interoperability Guide of Government Services** to orient the use of tools and technologies produced by the segment.

10.1.6. The segment will act searching the identification, follow-up of the production and analysis of data standards of general interest of the Public Administration, in conjunction with groups representing the government and of the society, reporting to competent instances in respect to the prioritization.

10.1.7. The data format of general interest of the government should be made available in the **Interoperability Catalog**, according to the rules of use of such tool.

10.1.8. The Interoperable Services (*Web Services)* of general interest should be made available in the **Interoperability Catalog**; however, there is the need to observe the rules of use of the restricted access services, defined by the relevant organs.

10.1.9. The **Interoperability Catalog** is a central element in the interoperability environment of the Federal Government. Its use is considered equivalent to the Adopted (A) situation.

10.2. Interoperability Catalog

10.2.1. The Interoperability Catalog is available in the website http://www.eping.e.gov.br and is composed by the Data Standard Catalog (CPD) and by the Interoperable Services Catalog.

10.2.2. The Data Standard Catalog (CPD) has as a goal to establish standards for types and items of data applied to the systems interfaces that are part of the public sector, and are divided into two documents:

- Volume 1, which establishes the general principles, that is, the reasons, approaches and rules for the application of the standards of Type and Items of Data; and
- Volume 2, which represents the Types and Item of Data standardized.

10.2.3. The e-PING Coordination is responsible for the Interoperability Catalog, in special, for the definition of the rules for management of changes processes and for promoting that the standards to be used in future developments.

10.2.4. O The development and maintenance of the Interoperability Catalog is in charge of the Integration Areas of the Electronic Government Group, which has the participation of different segments of the government in federal and state levels.

10.3. Models for documentation of *Web Services* and other forms of data exchange

10.3.1. As a way of documenting of the interoperable services, it is recommended the use, in each case, the documentation model for Web Services and of the documentation model for general services (not Web Services), such as file exchange, FTP, etc. Such models are available in the e-PING website.

10.3.2. The adoption of documentation models has status equivalent to the Recommended (R) situation.

10.3.4. It is solicited to the organs to use the Documentation Models, which send the interfaces documentation to the email: eping@planejamento.gov.br.

10.4. Integration Areas for the Electronic Government: Explanatory note on the Data Standard Catalog and XML Schemas

10.4.1. Initial Considerations

The Data Standard Catalogs and XML Schemas are available in the Electronic Government Portal in the website: http://www.governoeletronico.gov.br/.

The Data Standard Catalog has as objective to establish standards of types and items of data, which apply to the interfaces of the systems that are part of the public sector, and are divided into two documents:

- Volume 1, which establishes the general principles, that is, the reasons, approaches and rules for the application of the standards of Type and Items of Data; and
- Volume 2, which presents the Types and Items of Data standardized.

The XML Schemas Catalog has as a goal to establish the XML *Schemas* standards, which are applied to the interfaces of the systems that support the provision of Electronic Government services.

The XML *Schemas* Catalog contains the accepted standards in the form of XML *Schemas* for exchange of data involving the public sector. Such standards both may constitute in a single scheme and in a set of XML *Schemas*, since the set refers to one same thematic within the associate Integration Area.

The publication of XML Schemas does not automatically imply in guarantee of access to the correspondent contents or associate services, for which specific rules may be defined by the respective manager.

10.4.2. Property and Responsibility

The e-PING Coordination is responsible for these Catalogs, in special for the definitions of the rules for the management of the processes of changes and for promoting the standards to be used in future developments.

In this sense, it is recommended that the development or maintenance of systems, which support the provision of Electronic Government services related to the areas/sub-areas of government operation within the Catalog to consider the XML Schemas published.

The development and maintenance of such Catalogs are in charge of the Integration Areas for the Electronic Government Group, which has the participation of different segments of government in federal and state levels.

10.4.3. Management Mechanisms of the XML Schemas Catalog

The entries in the XML Catalog may be given through one of the following situations:

a) Proposition followed by the acceptance of the proposal of content for the Standard Data Catalog (SDC)

b) Submission followed by the acceptance of proposal of content to the Referential

Architecture of the Government Computerized Systems (RA);

c) Submission, by professional linked to the public sector, of content directly to the XML Schemas Catalog, throughout an electronic form available from the e-PING website.

The proposition of register of XML Schemas will be submitted for consideration of the members of the Integration Areas for the Electronic Government Group by means of specific electronic form, available in the e-PING website (www.e-ping.e.gov.br). Will be maintained in the Catalog only the propositions accepted, and those that are still under study, the rejected ones, as well as the previous XML Schemas versions accepted will be maintained in a "test" environment to be opportunely designed and implemented.

The evaluation criteria used will include:

- recognition by the user community;
- agreement by the area/sub-area manager (in the case in which he himself is not the proponent); and
- accession to the e-PING standards.

That is, the occurrence of submissions in which the proponent of a certain XML Schemas is not the manager of the area is foreseen, but will have as additional condition of acceptance the agreement of the manager, from dialogue performed by the proponent himself and/or by the Integration Areas of the Electronic Government Group.

Solicitations for alteration for XML Schemas already published will be analyzed, preliminary, by the members of the Integration Areas of the Electronic Government Group. The decision of acceptance will be in charge of the Central Coordination of the e-PING, which may adopt the changes proposed according to the coverage and impact, or submit them to Public Consultation, throughout the website: http://www.governoeletronico.gov.br.

For this version of the e-PING document, it was decided to make available the content of the XML Schemas Catalog only in the tool developed for the management, and it was suppressed the publication in the document of the references to the same. This choice is based on the objective of encouraging the use and maintenance of the XML Schemas in the appropriate tool and allowing more flexibility in the management of the XML Schemas.

10.5. Integration Areas for the Electronic Government: Technical Specifications

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

Table 15 – Specifications for the Integration Areas for the Electronic Government – Cross-cutting Themes and Government Acting Areas

Themes	Specifications	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

PROCESSES – Language for the Execution of Processes	BPEL4WS V1.1, as defined by the 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 the BPEL4WS, version 2.0. Studies related to the orchestration of processes and choreography will further conducted by the group.

Themes	Specifications	Sit	Comments
PROCESSES – Notation of Modeling of Processes	BPMN 1.0, as defined by the OMG http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf	**R**	
Exchange of Financial information	XBRL - eXtensible Business Reporting Language http://www.xbrl.org/SpecRecommendations/	**F**	www.xbrl.org
Legislation, Law and Legislative Proposals	LexML v. 1.0 http://projeto.lexml.gov.br	**R**	Project LexML defines recommendations for the identification and structuring legislative and legal documents
Strategic planning	StratML - Strategy Markup Language http://xml.gov/stratml/index.htm	**F**	
GEO-REFERENCED INFORMATION – Interoperability between systems of geographic information	WMS version 1.0 or later http://www.opengeospatial.org/standards	**A**	
	WFS version 1.0 or later http://www.opengeospatial.org/standards	**A**	
	WCS version 1.0 or later http://www.opengeospatial.org/standards	**A**	
	CSW version 2.0 or later http://www.opengeospatial.org/standards/cat	**A**	
	WFS-T version 1.0 or later http://www.opengeospatial.org/standards/wfs	**R**	Observe patterns and security policies set by the GT2, particularly WS-Security.
	WKT/WKB http://www.opengeospatial.org/standards/sfa	**R**	To encrypt coordinates in conventional Web services. The coordinates must be in Lat / Long using the datum SIRGAS2000 or WGS-84. Use GML whenever possible.

Table 16 – Specifications for the Integration Areas for the Electronic Government – Web Services

Component	Specification	Sit	Comments

	A = Adopted
	R = Recommended
	T = In Transition
	E = Under Study
	F = Future Study		

Registration infrastructure	Specification UDDI v3.0.2 (Universal Description, Discovery and Integration) defined by the OASIS http://uddi.org/pubs/uddi_v3.htm	**R**	
	ebXML (Electronic Business using eXtensible Markup Language). The specification can be found in http://www.ebxml.org/specs/index.htm	**E**	

Component	Specification	Sit	Comments
Definition language of the service	WSDL 1.1 (*Web Service Description Language*) as defined by the W3C. Specification can be found in http://www.w3.org/TR/wsdl	**A**	
	WSDL 2.0 (*Web Service Description Language*) as defined by the W3C. The specification can be found in http://www.w3.org/TR/wsdl20/	**E**	
Basic profile of interoperability	*Basic Profile 1.1 Second Edition*, as defined by the WS-I http://www.ws-i.org/Profiles/BasicProfile-1.1.html	**E**	Version 1.2 of the Basic Profile is still in as a Working Draft in http://www.ws-i.org/Profiles/BasicProfile-1.2.html
Remote portlets	WSRP 1.0 (Web Services for Remote Portlets) as defined by the OASIS http://www.oasis-open.org/committees/wsrp	E	

11. Glossary of Acronyms and Technical Terms[25].

In this item are presented the meanings of the main technical terms used in the e-PING.

***ABNT – Associação Brasileira de Normas Técnicas* / TNBA – Technical Norms Brazilian Association:** publishes standards, which provide guidance on the preparation and compilation of references of material used in documents production and for the inclusion of bibliographies, summaries, reviews, census and others.

ACAP – Application Configuration Access Protocol - Internet protocol for access client program options, configurations and preferential information remotely. It is a solution for the problems of client mobility in Internet.

***APF – Administração Pública Federal /* FPA – Federal Public Administration:** put together the organs of the direct administration (services integrated in the administrative structure of the Presidency of the Republic and of the Ministries) and indirect (Autarchies, Public Companies, Societies of Mixed Economy and Public Foundations) of the Executive Power. https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm.

BPM – Business Process Management: overview of business processes of an organization as flow of services using standards of notation representation, execution and coordination in XML, whose semantic rigor permits its interoperability between different platform systems, thus, is a basis for the implementation of solutions based on the architecture oriented to services. When the coordination of the execution of the services is performed with subordination to a master process, in general, intra-organization, such coordination is named as Orchestration. When the coordination is given without the subordination to a master process, in general, inter-organization, it is named Choreography.

Browser: web navigator – A client application that allows the user to view the contents in the *World Wide Web* in other network or user computer, following the hypertext links and transferring files.

XML *Schemas* Catalog: information directory on XML *Schemas*

Cryptography / Encryption: technical protection of information, which consists in ciphering the contents of a message or a signal, turning it into an unreadable text, with complex mathematics algorithms.

CSW – Catalogue Services for the Web: OCG specification that defines interfaces to publish, access, browse and consult metadata in geo-referenced information in Internet (HTTP).

Device: physical component (workstation, cell phone, smart card, hand-held, digital television with access to Internet)

DNS – Domain Name System: how domain names are located and translated in the protocol address in the Internet. A domain name is an easy resource to be remembered when referenced as an address in Internet.

FTP – File Transfer Protocol: applicative protocol that uses Internet TCP/IP protocols, and is the simplest way to exchange files between computers through Internet.

GML – Geography Markup Language: OGC specification based on XML developed to allow the transport and storage of geographic/spatial information.

Hand-helds: portable computer, also known as PDA, pocket PC or palm top. Portable equipment developed to serve as access device.

Handshake: in a communication via telephone, exchange of information between two modems and the resulting agreement about which protocol to use before any telephone connection.

[25] Microsoft Press. Dicionário de informática. Tradutor e consultor editorial Fernando Barcellos Ximenes - KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.

Thing, Lowell (ed.). Dicionário de Tecnologia. Tradução de Bazán Tecnologia e Lingüística e Texto Digital. São Paulo: Futura, 2003. ISBN 85-7413-138-5.

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

HELO: parameters that limit the sending of unsolicited commercial email. http://www.postfix.org/uce.html

HTTP – Hyper Text Transfer Protocol: set of rules for exchanging files (text, images, graphics, sound, video and other multimedia files) in the *World Wide Web*.

HTTPS – Secure Hyper Text Transfer Protocol: web protocol developed by Netscape and coupled to the browser. Encrypts and cryptanalysis solicitations and feedbacks of pages returned by the web server. HTTPS is only the use of Netscape SSL (Secure Sockets Layer) as a sub layer under the normal organization of the HTTP applications programs.

ICP – Brazil: set of techniques, practices and procedures to be implemented by Brazilian government and private organizations, in order to establish the technical and methodological fundaments of a digital certification system based on public key. http://www.icpbrasil.gov.br

IEEE – Institute of Electrical and Electronics Engineers: encourages the development of standards and norms that frequently become national and international.

IETF – Internet Engineering Task Force: entity that defines Internet operational protocols, such as TCP/IP.

IMAP – Internet Message Access Protocol: standard protocol to access emails from the local server. IMAP is client-server protocol in which the email is received and stored by the Internet server.

IP – Internet Protocol: protocol that enables communication between devices in the network. Generally speaking, can be considered as a set of numbers, which represent a location of a particular equipment (usually computers) in a private or public network.

IPSec – Internet Protocol Security: standard of development related to security in the network layer or to processing of communication packages in network. A big advantage of the IPsec is that the security arrangements can be handled without requiring changes in the individual users' computers. IPsec provides two options of security services: Authentication Header (AH), which essentially allows authentication of the sender of data, and Security Payload (ESP), which supports both the sender authentication and the cryptographic encryption of data.

IPv4 – Internet Protocol Version 4: is the IP version protocol most used currently. It is formed by a 32-bit number, written with four octets in decimal format, separated by dots (example: 161.148.1.18). The fist portion of the address identifies a specific network in the inter-network and the second portion identifies an equipment (host) within this network.

IPv6 – Internet Protocol Version 6: is the most recent version of the IP protocol. It is formed by a 128-bity number written in eight fields of four hexadecimal digits separated by colons (example: 3ffe:6a88:85a3:08d3:1319:8a2e:0370:734); and includes network prefix and host suffix. It is being gradually implemented in Internet and should work side by side with IPv4, in a situation technically named “dual stack”, for some time. In the longer term, the IPv6 is intended to replace IPv4, which supports only up to 4 billion (4 x 109) addresses, against about 3.4 x 1038 addresses of the new protocol.

LAN – Local Area Network: group of computers and devices associated, which share the same communication line, and usually the resources of a single processor or server in a small geographic area. Usually, the server has application and storage of data shared by multiple users in different computers.

LDAP – Lightweight Directory Access Protocol: sofware protocol to enable the location of people, organizations and other resources, such as files and devices on a network, whether on the public Internet or a corporative intranet.

Means of Access: set of physical components (access devices) and non-physical (basic sofware, applicative, etc.) that enable to the user the access to an electronic government service

Real Time Massaging or Instantaneous Massaging: is a kind of communication that enables the user to exchange messages in real time with other user also connected to the network.

Metadata: known as “data over data”, metadata are used to register attributes on an informational resource, aiming to facilitate the retrieval, management, interoperability, give support to the digital identification and give support to the archiving and preservation.

Middleware: is a general term that serves to mediate two separate programs and usually already existing. Different applications can communicate via Messaging service, provided by *middleware* programs.

Newsgroup: discussion about a particular subject that consisting of messages sent to a central site in Internet and redistributed by Usenet, a global network of newsgroups for discussion of news. The users can send messages to existing newsgroup, answer previous ones and create novel newsgroup.

OGC – Open Geospatial Consortium: has the mission of “developing spatial interfaces specifications, which will be freely available for general use.

Open Standard:

I - enables the interoperability between several applications and platforms, internal and external;

II - enables application without any restriction or fee payment;

III - can be fully and independently implemented by multiple suppliers of computer programs, in multiple platforms, with no charge relating to intellectual property for the necessary technology.

Metadata Standard: a metadata standard establishes a set of metadata elements for a community, including the specification for each element and encryption schemas to enable the interoperability between systems using the standard.

Plug-in: an accessory program that adds capabilities to the main program. Usually, in web applications, they are programs, which can be easily installed and used as part of the browser. A plug-in application is automatically recognized by the browser and its function is integrated to the HTML page that is being presented.

POP3 – Post Office Protocol 3: most recent version of the standard protocol to retrieve emails. POP3 is a client/server protocol in which the email is received and stored in the Internet server.

Portal: website that aggregates services, news and a great amount of information and/or entertainment content.

Government Network: is the portal to enter in all pages of the federal government in Internet. http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm.

Resolution no. 7 of the Electronic Government: establishes rules and guidelines for the websites of the Federal Public Administration (gov.br and mil.br). Divided into 7 chapters, the resolution treats of the information structure, control and monitoring, management of the interactive elements, organizational models, visual identity and security of the government sites in the worldwide computers network. http://www.governoeletronico.e.gov.br.

RFC – Request for Comments: IETF formal document, resulting from models and revisions of stakeholders. The final version of the RFC has become a standard in which neither comments nor changes are permitted. Changes may occur, however, by means of subsequent RFCs that replace or elaborate in all parts of the previous RFCs. RFC is also the acronym for Remote Function Call.

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

Government Electronic Services (related Electronic Government Services, Electronic Services)

Electronic Government can be defined by the use of technology to increase the access and improve the delivery of government services to citizens, suppliers and servants. In general, the characteristic functions of the electronic government are:

1. Electronic delivery of information and services.
2. Regulation of information networks, especially involving governance, certification and taxation.

3. Public accountability, transparency and monitoring of the budget execution.
4. Distance learning, digital literacy and maintenance of virtual libraries.
5. Cultural diffusion with emphasis on local identities, promotion and preservation of local cultures.
6. e-procurement, that is, purchase of goods and services by means of Internet, as well as electronic public biddings, electronic auctions , virtual public purchase and other types of digital market for goods purchased by the government.
7. Stimulation of e-business, by creating environments for secure transactions, specially for small and medium companies. http://www.governoeletronico.gov.br/r1.

Information System of the Federal Government: systems supporting the following activities:

- government management: Planning, Budget, Budget Execution, Financial Management, Human Resources Administration, General Services Administration, Management of Documentation and Information, Administrative Organization and Modernization, Information and Informatics Resources and Internal Control;
- final performance of government: purposive activities of the various organs of the government structure, such as infrastructure (transports, communication, energy, natural resources administration), Agriculture, Health, Education, etc.

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

SFS – Simple Features Specification for SQL: OGC specification, which defines the customization of the SQL scheme that supports storage, retrieving, consultation and update on geo-referenced information.

Smart Cards: plastic card, with the about size of a credit card, with a microchip embedded that can be loaded with data to be used to perform phone calls, electronic payments in cash and other applications. It is periodically updated to receive additional uses.

S/MIME – Secure Multi-Purpose Internet Mail Extensions: secure method for sending emails, which uses the RSA ciphering system (Rivest-Shamir-Adleman). S/MIME describes as encrypted 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 for sending and receiving emails. MIME is an extension of the original Internet email protocol that enables the exchange of many types of data files through Internet.

SOA – Service Oriented Architecture: is a paradigm for organization and use of distributed competences, which are under control of different owners domains. SOA architecture is used for systems interoperability by means of a set of services interface loosely coupled, where services do not need technical details of the platform of the other services for the exchange of information to be performed.

SOAP – Simple Object Access Protocol: describes a model for packing of XML questions and answers. SOAP sending of messages is used to enable the exchange of a variety of XML information. SOAP rule assumes the task of transmitting requests and answers about services between users and suppliers of services.

Free Software: computer program available throughout its source-code and with permission to anyone to use it, copy it and distribute it, either in its original form or with modification, either free or at cost. A free sofware is necessarily non-proprietary, but it is important not to confuse free sofware with sofware free of charge.

SPAM: unsolicited email. By the point of view of the sender, is a way to provide mass message, usually, to a separate list of inscribed persons to a Usenet discussion group or obtained by companies specialized in creating distribution lists of email. For the receiver, spam is usually considered as trash.

SSL – Secure Sockets Layer: is a protocol commonly used for managing the security of a message transmission in Internet.

Taxonomy for Navigation: is a terms and phases controlled vocabulary, organized, hierarchically structured, according to the natural or presumed relationships, aiming to facilitate to users of websites and portals to find information through navigation.

TCP – Transmission Control Protocol: set of rules used with IP to send data in the form of message unities between computers through Internet. While IP handles the actual delivery of data, TCP controls the individual units of data in which a message is divided for efficient routing through the Internet

Telnet: way of accessing someone else's computer, assuming you have permission. More technically, Telnet is a user command and a subliminal TCP/IP protocol.

TLS – Transport Layer Security: protocol to ensure privacy in the communication between applications and their users in Internet. When a server and the client communicate, TLS ensures no other part is able to see or catch the message.

Token: data object structured or a message that circulates continuously between the nodes of a token ring network and describes the actual status of the network.

UDDI – Universal Description Discovery and Integration: is the repository in which the developers record the Web Services available, which enables to the clients to find and use the services allocated in Extranets and Intranets.

UDP – User Datagram Protocol: communication protocol that provides a limited number of services, when exchanging messages in computers, in a network using IP. UDP is an alternative to TCP and, with IP, is referred as UDP/IP. As well as TCP, UDP uses IP to carry a data unity from a computer to another. Differently of TCP, UDP does not provide the service of dividing a message in packages and reassemble them in the other end. UDP neither does nor provide the sequence of packages in which the data come. This means that the application program that uses UDP should guarantee that the entire message has come and is OK. The network applications that desire to save processing time, for having small data unities to exchange may prefer UDP instead of TCP.

UML – Unified Modeling Language: UML is much more than the customization of a notation, that is, it is a standard-language for the elaboration of the structure of sofware projects, including conceptual aspects, such as business process and functions of the system, in addition to concrete items such as classes written in a particular programming language, database schemas and sofware reusable components. UML can be used for visualization, specification and construction, and the documentation of software systems artifacts, can be used in modeling business and other systems types, and not only sofware ones.

URI – Uniform Resource Identifier: standard for encrypting names and addresses in Internet. A URI is composed by a name (ex, file, http, ftp, news, mailto, gopher), followed by colon, and then, a pathway, standardized by a list of schemas that follows the RFC 1630. URI groups the URNs and URLs concepts.

Usenet: collection of notes and messages submitted by users about various subjects, which are sent to servers in a worldwide network. Each collection of notes sent is known as newsgroup.

VPN – Virtual Private Networks: private network, which uses the infrastructure of a public network of telecommunications, such as Internet, for example, for transmission of confidential information. Transmitted data are encrypted. Its implementation is given by means of virtual tunnels, by which information travels, protecting them from the access of non-authorized users.

W3C – World Wide Web Consortium: industries association aiming to promote the evolution of the web and the interoperability between WWW products by producing specification and reference software.

WAN – Wide Area Network: computers network that covers extensive geographic areas, such as a state, a country or a continent.

WCS – Web Coverage Service: OGC specification that defines the interface of a service to access geo-referenced information, which has values all over the space considered without well-defined borders (geo-fields).

Web Services: logical application, programmable that makes compatible the most different applications, regardless the operational system, enabling the communication of data between different networks.

WFS – Web Feature Service: OGC specification that defines the interface of a service, which enables to access and handle geographic data encrypted in GML in the Internet (HTTP). Two classes of services can be defined:

- **Basic WFS (WFS):** implements read-only operations, which enables to obtain the spatial data
- **Transactional WFS (WFS-T):** implements the transactional operations used to handle data remotely

WMS – Web Map Service: OGC specification that defines the interface of a service making available maps (edited geographic data) or images in Internet (HTTP)

WSDL – Web Services Definition Language: is a XML format for description of the web services and their access information. It describes the functionalities of the services offered by the services provider, as well as their location and way of access.

XML – eXtensible Markup Language: flexible way to create formats of common information and share both formats and the data in the World Wide Web, in intranets, or in any location. XML is extensible because, differently of HTML, the markup symbols are unlimited and self-definers.

XML *Schemas*: are XML documents, also found in website, which specifies the structure, amount of occurrences of each element, allowed values, unities, etc, that is, the syntax of the document. The Schemas of a set of XML documents, of a same type, are publicly available in a website, so that programs can access them to validate the XML documents of this set. http://www.uff.br/gdo/htm/tsld106.htm

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

XSL – eXtensible Stylesheet Language: language for creation of worksheets that describes how a data is sent through the web, using XML, and is presented to the user. XSL is a language for formatting an XML document.

XSLT – eXtensible Stylesheet Language Transformations: standard way of describing how to change the structure of an XML document into another XML document with another structure. XSLT can be thought as an extension of the XSL. XSL shows how the XSL document should be reorganized into another structure of data (which may be made following the XSL worksheet)

12. Members

e-PING Coordination

Waters National Agency (ANA)
Sérgio Augusto Barbosa

Movie National Agency (ANCINE)
Sérgio Augusto S. de Morais

Brazilian Association of State Entities of Information and Communication Technology (ABEP)
Dayse Vianna

Bank of Brazil (BB)
Ulisses de Sousa Penna

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

Social Security Information Technology Company (DATAPREV)
Humberto Degrazia Campedelli

Ministry of Defense – Army Command (MD/CEX)
Emerson Magnus de A. Xavier
Jefferson Adelino Lemos Pita

Ministry of Justice (MJ)
Jorilson da Silva Rodrigues

Ministry of Health (MS)
Fábio Lima Cordeiro

Ministry of Foreign Affairs (MRE)
Filipe Carneiro Guimarães

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

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

Ministry of Planning, Budget and Management – Department of Logistics and Information Technology (MP/SLTI)
Nazaré Lopes Bretas (General Coordinator)
Cláudio Muniz Machado Cavalcanti
Cristiano Rocha Heckert
Jorge Arruda
José Ney de Oliveira Lima
Leonardo Boselli da Motta
Lilian Barbara Bender Portugal
Marcelo Martins Villar
Mário Henrique Paes Vieira
Rogério Santanna dos Santos
Yuri Fontes de Oliveira

Nuclebrás Heavy Equipments S/A (NUCLEP)
Adilson Custódio
Elizabeth Rodrigues Cunha

Presidency of the Republic (PR)
Macarino Bento Garcia de Freitas

Presidency of the Republic – National Institute of Information Technology (ITI)

Mauricio Augusto Coelho
Renato da Silveira Martini

Internal Revenue Service of Brazil (RFB)
Edna Pereira Pinto Fernandes

Department of Administration of the State of Bahia (SAEB)
Ernani Marques dos Santos

Federal Data Processing (SERPRO)
Bruno Pacheco de Paes
Elói Juniti Yamaoka

Interconnection Working Group

Cristiano Rocha Heckert (MP/SLTI) – Coordinator
Carlos Bellone Neto (RFB)
Dijasmo Martins Gomes Junior (ECT)
Filipe Carneiro Guimarães (MRE)
Helio de Araujo Castro (NUCLEP)
Juscelino Kilian (PR/GSI)
Leonardo Boselli da Motta (MP/SLTI)
Luiz Gustavo Lustosa Colombo (IPHAN)
Odilon de Freitas Militao Neto (CAIXA)
Paulo Guilherme Lanzillotti Jannuzzi (MPS)
Vanderlei de Jesus dos Santos Marques (ANVISA)
Wellington Luiz Barbosa (MP/SLTI)

Collaborators
Hermógenes Batista Correia (MP/SLTI)

Security Working Group

Jorilson da Silva Rodirgues (MJ) – Coordinator
Antônio Acras Filho (SERPRO)
Artur Nobre Mendes (FUNAI)
André Machado Caricatti (ITI)
Cláudio Muniz Machado Cavalcanti (MP/SLTI)
Cristiano Rocha Heckert (MP/SLTI)
Dante de Matos Gomes (PRODEB)
Filipe Carneiro Guimarães (MRE)
Gilberto de Oliveira Netto (SERPRO)
Humberto Degrazia Campedelli (DATAPREV)
Jean Carlo Rodrigues (ITI)
Joel Corrêa (DATAPREV)
José Eduardo Malta de Sá Brandão (IPEA)
José Luiz Povill de Souza (MJ/DPF)
Luiz Gustavo Lustosa Colombo (IPHAN)
Marcos Gomes Figueira (BB)
Marcos J.C. Euzébio (BACEN)
Mario Henrique Paes Vieira (MP/SLTI)
Nazaré Lopes Bretas (MP/SLTI)
Paulo Coelho Ventura Pinto (ANS)

Collaborators
Anderson Claiton Fernandes (MJ)
Cláudia do Socorro Ferreira Mesquita (MP/SLTI)
Ronaldo Íon Miranda do Nascimento (MJ)

Means of Access Working Group

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)

Collaborators
André Luís da Silva Gonçalves (MP/SLTI)

Information Organization and Exchange Working Group

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)
Cintia de Souza Cinquini (PR)
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 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)

Collaborators
Dalva Clementina Luca (MJ)

Integration Areas for the Electronic Government Working Group

Cláudio Muniz Machado Cavalcanti (MP/SLTI) – Coordinator
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)

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

Subgroup: ABEP
Dayse Vianna (Governo do Rio de Janeiro / PRODERJ) – Coordinator
Tarcísio Quirino Falcao (Government of Pernambuco / ATI)

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

Subgroup: Standards for Spatial Information Exchange
Emerson Magnus de A. Xavier (MD/CEX/CIGEx) – Coordinator
Cristiane Vaz Domingues (DATAPREV)
Jedson F. Passos (CAIXA)
Linda Soraya Issmael (MD/CEX/DSG)
Marcelo Martins Villar (MP/SLTI)
Moema Augusto (IBGE)
Yoshihisa Kawano (ABIN)
Yuri Fontes de Oliveira (MP/SLTI)

Reference Document of the e-PING – Version 2010

Illustrations
Hezrai de Souza Cruz (MP/SLTI)