

**Brazilian Government  
Executive Committee of Electronic Government**



**e-PING  
Electronic Government  
Interoperability Standards**

**Reference Document**

**Version 3.0**

**December 14, 2007**

**SUMMARY**

**ACKNOWLEDGMENTS.....4**

**PART I – OVERVIEW OF E-PING.....5**

**1. INTRODUCTION.....6**

**2. SCOPE.....7**

    2.1. JOINING E-PING.....7

    2.2. FOCUS ON INTEROPERABILITY.....8

    2.3. SUBJECTS NOT ADDRESSED.....8

**3. GENERAL POLICIES .....9**

**4. SEGMENTATION.....10**

    4.1. INTERCONNECTION .....10

    4.2. SECURITY.....10

    4.3. MEANS OF ACCESS .....10

    4.4. ORGANIZATION AND EXCHANGE OF INFORMATION .....11

    4.5. AREAS OF INTEGRATION FOR ELECTRONIC GOVERNMENT .....11

**5. MANAGEMENT OF E-PING .....12**

    5.1. HISTORY .....12

    5.2. IMPLEMENTATION STRATEGY .....12

    5.3. MANAGEMENT MODEL.....13

        5.3.1. *Assignments* .....13

        5.3.2. *Responsibilities* .....14

    5.4. ADDITIONAL ACTIVITIES .....15

        5.4.1. *Selection and Certification of Technology Standards*.....15

        5.4.2. *Audit of Compliance* .....16

        5.4.3. *Creation and Maintenance of the Website* .....16

        5.4.4. *Legal and Institutional Monitoring*.....16

        5.4.5. *Dissemination* .....17

        5.4.6. *Training* .....17

    5.5. RELATIONSHIP WITH GOVERNMENT AND SOCIETY .....17

        5.5.1. *Organizations of the Federal Government - Executive Power* .....17

        5.5.2. *Other Instances of Government (other Federal Powers, State and Municipal Governments)* .....17

        5.5.3. *Organizations of the Private Sector and Third Sector*.....18

**PART II – TECHNICAL SPECIFICATION OF E-PING’S COMPONENTS.....19**

**6. INTERCONNECTION.....20**

6.1. INTERCONNECTION: TECHNICAL POLICIES..... 20

6.2. INTERCONNECTION: TECHNICAL SPECIFICATIONS..... 21

6.3. WEB SERVICES..... 22

6.4. ELECTRONIC MESSAGE (E-MAIL)..... 24

6.5. VPN..... 25

6.6. PEER-TO-PEER NETWORKS..... 25

**7. SECURITY.....26**

7.1. SECURITY: TECHNICAL POLICIES..... 26

7.2. SECURITY: TECHNICAL SPECIFICATIONS..... 27

**8. MEANS OF ACCESS .....33**

8.1. MEANS OF ACCESS: TECHNICAL POLICIES..... 33

8.2. MEANS OF ACCESS: TECHNICAL SPECIFICATIONS FOR WORK STATIONS..... 34

8.3. MEANS OF ACCESS: TECHNICAL SPECIFICATIONS FOR TOKENS, SMART CARDS AND CARDS IN GENERAL..... 38

**9. ORGANIZATION AND EXCHANGE OF INFORMATION.....47**

9.1. ORGANIZATION AND EXCHANGE OF INFORMATION: TECHNICAL POLICIES..... 47

9.2. ORGANIZATION AND EXCHANGE OF INFORMATION: TECHNICAL SPECIFICATIONS..... 47

9.3. NOTES ABOUT XML AND MIDDLEWARE..... 48

**10. INTEGRATION AREAS FOR ELECTRONIC GOVERNMENT.....49**

10.1. INTEGRATION AREAS FOR ELECTRONIC GOVERNMENT: TECHNICAL POLICIES..... 49

10.2. INTEGRATION AREAS FOR ELECTRONIC GOVERNMENT: NOTES ABOUT XML SCHEMAS CATALOG..... 49

    10.2.1. *Initial Considerations*..... 49

    10.2.2. *Objective*..... 49

    10.2.3. *Scope*..... 49

    10.2.4. *Property and Responsibility* ..... 50

    10.2.5. *Management Mechanisms of the XML Schemas Catalog*..... 50

    10.2.6. *XML Schemas Information set*..... 51

    10.2.7. *Classification of XML Schemas Catalog*..... 51

10.3. INTEGRATION AREAS FOR ELECTRONIC GOVERNMENT: TECHNICAL SPECIFICATIONS..... 52

**11. GLOSSARY OF ABBREVIATIONS AND TECHNICAL TERMS.....56**

**12. INTEGRANTS.....62**

### Acknowledgments

e-PING – Electronic Government Interoperability Standards – architecture defines a minimum group of premises, policies and technical specifications that regulate usage of Information and Communication Technology (ICT) in the interoperability of Electronic Government Services, establishing interaction conditions with the remaining Powers and spheres of government and with overall society.

The areas covered by e-PING are segmented in:

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

To each of these segments a series of components were applied, for which standards will be established.

All content of this reference document is consistent with guidelines from the Executive Committee of Electronic Government, created by Decree in October 18th 2000, and is published in an Internet website (<http://www.eping.e.gov.br>), ensuring public access to general interest information and transparency to the initiative. The Brazilian Government is compromised in assuring that these policies and specifications remain consistent with society's needs and with market and technology evolution.

e-PING reference document contains:

- Bases of e-PING's conception, implementation and administration, relating expected benefits with the work, defining limits of e-PING's architecture comprehension and highlighting considered premises and established policies;
- e-PING's management model, discriminating responsibilities, conformity assessing criteria, change management, spreading and orientation for capacity-building;
- Policies and technical specifications established for all components in each segment of e-PING;
- Glossary of referenced technical terminology;
- Relation of integrants and collaborators

Content of this document is of public domain, not standing any restrictions to its reproduction neither to use of information herein available. Reproduction may be done in any media, independently of specific authorization. Inappropriate use of material with depreciative ends will be considered subject to proper juridical treatment by the Brazilian Government, keeper of intellectual rights.

It is prohibited the use of whole or parts of this document for commercial purposes.

## Part I – Overview of e-PING

## 1. Introduction

The starting point for offering better services, adequate to citizens and business' necessities, with lower costs, is the existence of an Information and Communication Technology (ICT) infrastructure that stands as a pillar for the creation of these services. A modern, integrated and efficient government needs equally modern, integrated and efficient systems, working in a way that is integral, safe and consistent with the public sector.

In this context, interoperability of technology, processes, information and data is a vital condition for providing quality services, turning it into a premise for governments throughout the world, as a fundament for electronic government concepts, the *e-gov*. Interoperability allows rationalization of investments in ICT through sharing, re-use and exchange of technological resources.

Government such as the American, Canadian, British, Australian and Neo Zealand strongly invest in development of policies and processes and in establishing ICT standards, setting structures dedicated to obtaining interoperability, aiming to provide better quality and lower costs services.

The Brazilian Government has been consolidating its e-PING architecture – “Electronic Government Interoperability Standards”, which has the purpose to be a paradigm for establishing policies and technical specifications that allow delivering quality electronic services to society.

What is interoperability?

For establishing e-PING's goals, it is important to clearly define what is understood as *interoperability*. Below there are four concepts that fundament the Brazilian Government understanding on the subject:

“Consistent exchange of information and services among the systems. It must allow the substitution of any component or product used in the linking points by other of similar specification, not compromising the system's functionality.” (United Kingdom Government);

“Ability of transferring and using information in a uniform and efficient way among several organizations and information systems.” (Australian Government).

“Ability of two or more systems (computers, means of communication, networks, software and other components of information technology) to interact and exchange data according to a defined method, in order to obtain the expected results.” (ISO);

“Interoperability defines wetter two components of a system, developed with different tools, by different suppliers, may or may not act jointly.” (Lichun Wang, European Bioinformatics Institute – CORBA Workshops);

Interoperability is not just Systems Integration, nor is it just Networks Integration. It is not only about data exchange among systems. It does not simply contemplate a definition of technology.

It is, in fact, the sum of all these elements, also considering the existence of a legacy of systems, installed platforms of Hardware and Software. It parts from principles that are about diversity of components, using various products of distinct suppliers. It has the goal to consider all factors so that systems may act cooperatively, fixing norms, policies and patterns necessary to achieve these goals.

In order to achieve interoperability, people should be engaged in a continuous effort to ensure that systems, processes and culture of an organization are managed and directed to maximize opportunities of information exchange and re-use.

## 2. Scope

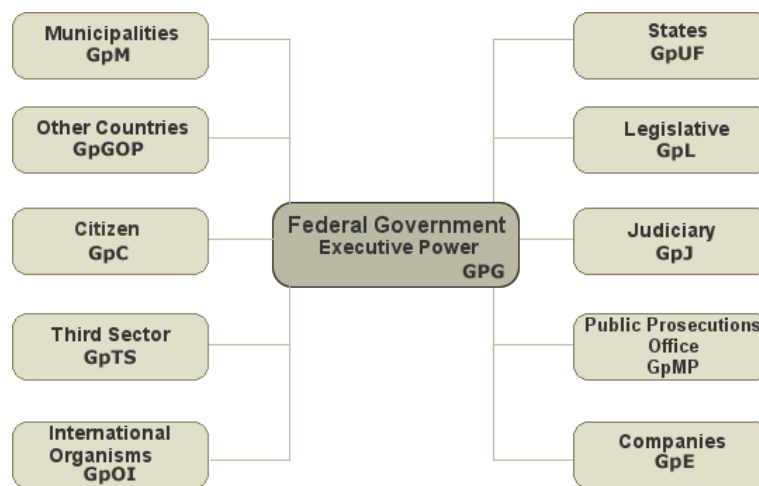
Policies and specifications clearly defined for interoperability and management of information are essential to propitiate government connection, both in domestic and society contact spheres and, on a bigger comprehension level, with the rest of the world – other governments and companies acting in the 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 participation, through voluntary enrollment, of other powers and government spheres.

Information resources of the government constitute valuable economic assets. When assuring that governmental information can be rapidly located and exchanged between the public sector and society, keeping the privacy and security obligations, government helps in the best use of this asset, propelling and stimulating the country’s economy.

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

- Citizens;
- Other levels of government (state and local);
- Other Powers (Legislative, Judiciary) and Public Prosecutions Office;
- International Organisms;
- Governments of other countries;
- Companies (in Brazil and abroad);
- Third Sector.

The following image represents this relationship.



**Image 1 – Relationships in the federal government**

### 2.1. Joining e-PING

Adoption of standards and policies contained in e-PING can not be imposed to citizens and to several government instances, inside and outside the country. The Brazilian government, however, establishes these specifications as the standard selected and accepted, that is, these are the standards in which it wishes to interoperate with entities outside the federal government – Brazilian Executive Power. Joining this activities takes place in a voluntary way, without any pressure from e-PING Coordination.

For the federal government – Brazilian Executive Power bodies, adoption of standards and policies contained in e-PING is compulsory.

“Brazilian federal government – Executive power” includes:

- Organs of Direct Administration: Ministries, Offices and other governmental entities of the same juridical nature, directly or indirectly linked to the Presidency of the Federative

Republic of Brazil;

- Autarchies and foundations.

In the scope of above mentioned entities, specifications contained in e-PING are compulsory to:

- All new information systems that may be developed and implemented in the federal government and that fits the interaction scope, inside the federal government and in society;
- Information systems that may be object of implementations that involve providing electronic government services or interaction among systems;
- Other systems that are part of the goals of making electronic government services available.

Joining will take place in a gradual way, according to an implementation plan that will consider specific situations of each of these institutions in relation to the possibility of fitting it to e-PING's specifications and recommendations.

All federal government – Executive Power's purchases and hiring directed to development of electronic government services and to upgrading of systems must be consistent with specifications and policies contained in this document.

e-PING supports participation of all interested parts in the continuous development and upgrading of specifications and recommendations that are part of the framework. e-PING's management foresees this participation, via internet (<http://www.eping.e.gov.br>) as a preferential means for contact between e-PING's managers and society.

### **2.2. Focus on interoperability**

e-PING will not have as focus of its work all matters of Information and Communication Technology (ICT). It will be considered only specifications that are relevant to ensure interconnectivity of systems, integration of data, access to electronic government service and content management. e-PING involves matters comprehended in segmentation, described on item 4 of this document.

### **2.3. Subjects not addressed**

e-PING does not have the goal to standardize the presentation of information of electronic government services, being restricted to definition of data exchange requests and conditions of availability of these data to access devices.

### 3. General Policies

Each of the segments of e-PING contains a set of technical policies that guides the establishment of its components specifications. These specific sets of each segment are based on the following policies:

**Alignment with the INTERNET:** all information systems of public administration should be aligned with the main specifications used over the Internet and the World Wide Web.

**Adoption of XML** as a primary data exchange standard for all systems in the public sector.

**Adoption of browsers** as the main means of access: all systems of government information should be accessible, preferably through technology based a browser; other interfaces are allowed in specific situations, as in routines of upgrade and collection of data where there is no alternative technology available based on browsers.

**Adoption of metadata** for the information resources of the government.

**Development and adoption of a standard of Metadata of the Electronic Government- e-PMG,** based on internationally accepted standards (<http://www.eping.e.gov.br>).

**Development and maintenance of the List of Government Affairs:** Taxonomy of Browsing (LAG), envisaging, in a directory structure, issues related to the performance of government (<http://www.eping.e.gov.br>).

**Market support:** all the specifications of e-PING have solutions widely supported by the market. The objective is the reduction of costs and risks in the design and production of services in systems of government information.

**Scalability:** the selected specifications should meet changes of demand in the system, such as changes in volumes of data, number of transactions or number of users. The standards will not be a restrictive factor and should be able to support the development of services that meet more specific needs, from small volumes of transactions and users, to demands for national scope, with large amounts of information and involvement of a high number of users.

**Transparency:** the documents of e-PING will be available to society, through the Internet, and there will be mechanisms for distribution, reception and evaluation of suggestions. In that sense, deadlines and commitments will be defined - and disseminated for broad knowledge – for implementation and management of the website ([http:// www.eping.e.gov.br](http://www.eping.e.gov.br)).

**Preferential Adoption of Open Standards:** e-PING defines that, wherever possible, open standards in technical specifications will be adopted. Private standards are accepted, temporarily, keeping up the prospects for replacement as soon as there are conditions for migration. Notwithstanding, situations where there is a need for consideration of requirements of security and integrity of information will be taken into account. When available, Free Software solutions are preferential, as defined by the Executive Committee of Electronic Government (CEGE).

e-PING has full compatibility with the initiatives of government in the area of ICT. An example is the Guide to Free Software Migration of the Brazilian Government (<http://www.governoeletronico.gov.br>).

**Ensuring privacy of information:** all agencies responsible for offering e-gov must guarantee the conditions for preserving the privacy of information of citizens, businesses and government agencies, respecting and abiding the law that defines restrictions on access and divulgation.

## 4. Segmentation

e-PING's architecture was segmented in five parts, aiming at organizing definitions of standards. For each segment a working group was set up, composed of professionals that work in federal, state and municipal agencies, experts in each subject. These groups were responsible for drafting this version of the architecture, a base for the establishment of standards for interoperability of the Brazilian government.

The five segments - "Interconnection", "Security", "Means of Access", "Organization and Exchange of Information" and "Integration Areas for Electronic Government" - were subdivided in **components**, for which it was established policies and technical specifications to be adopted by the federal government. Following are the components that are related to each of the five segments.

### 4.1. Interconnection

The "Interconnection" segment establishes the conditions under which the government bodies interconnect themselves, besides setting the conditions for interoperation between the government and society.

In this segment, the specifications are for:

- Hypertext Transfer Protocol;
- Transport of Electronic Messages;
- Security Content of Electronic Messages;
- Access to Mailbox;
- Secure Access to Mailbox;
- Directory;
- Domain Name Services;
- Electronic Addresses;
- File Transfer Protocol;
- Intercommunication LAN / WAN;
- Transportation;
- Web Services: SOAP, UDDI and WSDL.

### 4.2. Security

This segment deals with the security aspects of ICT that the federal government should consider. The standards are for:

- IP Security;
- E-mail Security;
- Encryption;
- System Development;
- Network Services;
- Collection and filing of evidence.

### 4.3. Means of Access

In the segment "Means of access", issues relating to the standards of devices for accessing e-government services are explained. In this version, only the policies and specifications for workstations, smart cards, tokens and other cards are addressed. In future versions, other devices will be addressed, such as mobile phones, hand-helds and digital television. It consists of two subgroups, with the following components:

Standards for access through work stations:

- Browsers;
- Character Sets and Alphabets;
- Hypertext Exchange Format;

- Document Type Files;
- Schedule Type Files;
- Presentation Type Files;
- Database for Work Stations Type Files;
- Specification of Exchange of Graphic Information and Static Images;
- Vector Graphics;
- Specification of Standards of Animation;
- Audio and Video Files;
- Compaction of General Use Files;
- Files for geo-referencing.

### Smart Card / Tokens / Other:

- Definition of data;
- Applications (including multi-application);
- Electrical Components;
- Communication Protocols;
- Standards for Physical Interface;
- Security;
- Infrastructure of the Terminal.

#### **4.4. Organization and exchange of information**

It addresses aspects related to the processing and transfer of information in electronic government services. It includes the standard structure of government affairs and metadata, comprising the following components:

- Language for data exchange;
- Language for processing data;
- Definition of data for exchange;
- Catalogue of Database Standards (CPD);
- List of Government Affairs: Taxonomy for Navigation (LAG);
- Standard of Government Metadata (e-PMG).

#### **4.5. Areas of Integration for Electronic Government**

The goals of analysis and proposal of this segment are:

- XML *Schemas* for applications geared to Practice Areas of Government, which will be organized in the form of a Catalog, available on the website of e-PING, and presented with the current content on topics below;
- Components related to themes of Practice Areas of Government, whose standardization is relevant to the interoperability of services of Electronic Government, such as Procedures and Geographic Information.

## 5. Management of e-PING

In this item aspects of management of e-PING's architecture are discussed, specifying the way in which the Brazilian government intends to consolidate the implementation of policies and technical specifications as effective standards adopted both internally, by the agencies that make up the Federal Public Administration, and in the interoperation with external entities, represented by other bodies of government, the private sector, institutions working in the third sector and the citizen.

### 5.1. History

E-PING architecture aims to be the paradigm of interoperability for federal government, initially under the Executive Power. The initiative for setting up the architecture was of three agencies of the federal sphere:

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

These three agencies held a seminar, with participation of the federal government, under the Executive Power, aiming at forming an interagency committee -called Constituent Committee - to conduct the initial work of the architecture.

After their institutionalization, through Normative Decision No. 5, July 14, 2005, it was called Coordination of e-PING. In addition to the three organizers, the following agencies also participate: Presidency of the Republic, Ministry of Foreign Affairs, Ministry of Health, Banco do Brasil, Caixa Economica Federal, DATAPREV and ABEP – Brazilian Association of Data Processing State Companies.

The Committee established the following work program:

- Definition of an initial development and management of e-PING architecture;
- Definition of segmentation of the subjects to be covered by e-PING;
- Creation of five working groups responsible for the initial definitions of policies and technical specifications for each of the segments;
- Establishment of a work schedule for assembling and promoting the initial version of the architecture, known as version 0;
- Carrying out public consultation and public hearings in the states of RS, SP, DF, RJ, MG and PE, to collect contributions of the society on the content proposed in version 0;
- Publication of version 1, along with the resolution of institutionalization of e-PING under the APF – Executive Power;
- Publication of version 1.5, containing the updates and revision of technical specifications and the overview of e-PING. The versions 1.1 to 1.4 were being discussed internally between working groups and the coordination of e-PING;
- Carrying out public consultation and public hearings to collect contributions of the society on each new version of the reference document;
- Publication of an annual version, containing the updates and revisions to the technical specifications and overview of e-PING.

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

### 5.2. Implementation Strategy

The dissemination of standards and specifications set by the Brazilian government follows a precise outline. The establishment of an annual version is envisaged, with intermediate publication of updates, whenever there are significant changes.

This version has consolidated the work of the groups assembled for the five defined segments. All its content was made available for Public Consultation, with the purpose of obtaining contributions to the proposed standards published in version 2.9.

### 5.3. Management Model

In this item the ways of managing e-PING architecture are specified and related to the main tasks and how to implement these activities in the organizational structure of government.

#### 5.3.1. Assignments

The management of e-PING includes the performance of administrative and technical assignments.

Among the administrative assignments are:

- To define the strategic and management objectives of government for the establishment of standards;
- To administer the architecture of interoperability of the Brazilian government, providing the necessary management for its correct use and ensuring its update, taking into account: the priorities and goals of government, the needs of society and availability of new mature technologies, supported by the ICT market;
- To act as a center of coordination of e-PING architecture, seeking alignment of efforts for interoperability, ensuring coherence of the initiatives undertaken by government agencies;
- Specifically for the segments of interoperability, to manage the relationship of federal government - Executive power - with the other agencies set out in item 2 - Scope;
- To manage and operate the dissemination of the standards of e-PING, considering the:
  - Establishment and administration of a website for e-PING (<http://www.eping.e.gov.br>);
  - Coordination of the process of public consultation;
  - Coordination of the process of receiving and evaluation of proposals for amendment and complementation;
  - Coordination of the process of applying for suggestions for e-PING;
  - Publication of updated versions of e-PING and intermediary updates;
- To manage the interaction with the similar initiatives, conducted by other governments, in the country or abroad;
- To encourage training of teams of federal government, acting together with the agencies, both in consideration of e-PING in specific training plans for each of them, and also in carrying out corporate events targeted to spread e-PING standards;
- To establish, implement and disseminate indicators for monitoring the performance of e-PING;
- To manage the interaction with specification agencies (W3C, IEEE, BSI, OMG, OGC, OASIS, IETF, Normative Institutes of specific segments, such as ABNT, INMETRO, ISO, NIST, etc.). These agencies will be chosen by the coordination of e-PING, taking into account their remarkable international recognition, in its area of competence and performance and the establishment of open standards.
- To manage the interaction with national and international promotion agencies, to channel resources, aiming to meet the needs of infrastructure of e-PING and promote research and development;
- To facilitate the implementation and manage the process of approval of the standards to be established for the government;
- To facilitate the implementation and managing of inspections conducted for the purpose of ascertain the level of adherence to the recommendations and specifications of e-PING;
- To act cooperatively, as support for the organs of government, in conducting the proceedings needed to match the patterns and-PING; assess the possibility of sponsoring extensive programmes that promote the intensive use of the proposed standards.

Among the technical assignments are:

- To establish ways of preparing and maintaining the policies and technical specifications that make up e-PING, taking into account the:
  - Identification, development and management of specific work groups;
  - Establishment of agreements and definition of government institutions as responsible

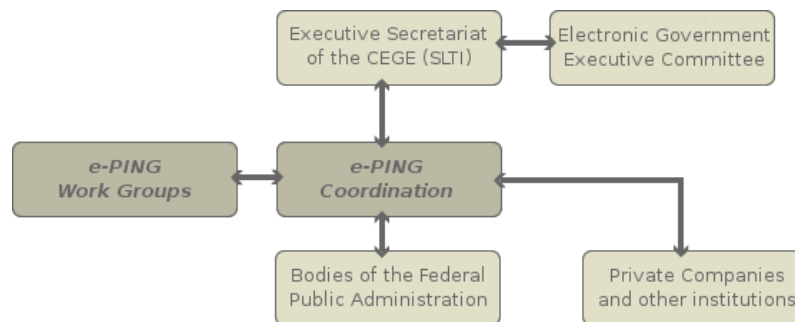
for policies and technical specifications for specific components of the segments of interoperability;

- Identification and implementation of alternative forms of technical management of the topics covered in the scope of activity of e-PING;

- To coordinate the development and maintenance within the federal government - Executive Power of the:
  - Standard of Government Metadata (e-PMG);
  - List of Government Affairs: Taxonomy of Navigation (LAG);
  - Catalogue of Database Standards (CPD);
  - Catalogue of Reference of XML Schemas;
  - Other patterns of Organization and Information Exchange;
  - Standards of Interconnection;
  - Standards of Security;
  - Standards of Means of Access to electronic government services;
  - Patterns of use of Smart Cards, Tokens and other types of cards;
- To ensure the unity of design, concepts, definitions and establishment of standards by the persons responsible for the technical segments defined for e-PING.

### 5.3.2. Responsibilities

The government structure created for managing e-PING is presented in the Simplified Scheme below.



**Image 2 – Administration of e-PING.**

The Secretariat of Logistics and Information Technology of the Ministry of Planning, Budget and Management, through the System of Administration of Resources and Information Technology (SISP), established by Decree 1048 of January 21, 1994, is responsible for institutionalization and definition of the legal format of the Coordination of e-PING.

- The activities of the Coordination of e-PING will be guided by the following points:
- Implementation of e-PING architecture, providing the necessary activities to consolidate the current version and the dynamics of its evolution;
  - Management of e-PING architecture;
  - Establishment and management of standards and institutional and legal instruments that ensure the effectiveness of recommendations and specifications of e-PING;
  - Administration of the standards considered in e-PING;
  - Ensuring maintenance of update of several e-PING catalogs;
  - Management of the processes of communication and dissemination of standards, decisions and activities of e-PING, including the publication of new versions and intermediate upgrades;
  - Creation of an e-PING stamp and administration of the process that certifies the link between a specific product or service and e-PING;
  - Provision of criteria and subsidies for the development of Law of Annual Budget of the Federal Government;
  - Management of procedures for hiring services and establishment of agreements to carry out the necessary assignments for consolidation of standards, such as evaluating proposals for e-gov projects aimed at the Federal Public Administration, approval of standards and verification

of compliance;

- Establishment of points of contact with the various agencies of the Federal Public Administration;
- Administration of Workgroups, defining its composition and determining the guidelines for work, based on technical, general and specific policies, in the needs of government and monitoring of the technological scenario.

e-PING Workgroups, consisted of representatives nominated by various agencies of APF and representatives of institutions in other spheres of government, are responsible for:

- Discussing the issues that make up the segments of e-PING;
- Monitoring systematically the market, specifically for the segments under its responsibility, in order to detect the need for technological upgrading of policies and technical specifications;
- Subsidizing performance of the Coordination of e-PING, in the performance of their administrative and technical assignments.

The coordinators of the Work Groups will have seats on the coordination of e-PING.

### 5.4. Additional Activities

In addition to administrative and technical assignments for implementation and evolutionary maintenance of e-PING architecture, other activities are under responsibility of the Coordination of e-PING.

#### 5.4.1. Selection and Certification of Technology Standards

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

e-PING foresees a process of analysis of standards that may join the architecture. This process involves selection, certification and classification of the selected specifications in five levels of situations, which characterize the degree of adherence to general, technical and specific policies of each segment.

These five levels are:

- **Adopted (A)**: adopted item by the government as the standard e-PING architecture, and was subjected to a formal certification process conducted by an institution of government or by another institution with formal delegation to complete the process. It is considered approved if based on a proposition required by the coordination of the segment, published on the website and approved by the Coordination of e-PING;
- **Recommended (R)**: item that meets the technical policies of e-PING, and is recognized as an item that must be used within the institutions of government, but not yet submitted to formal approval;
- **In Transition (T)**: item that the government does not recommend, because it did not meet one or more requirements established by the general and technical policies of the architecture; is included in e-PING because of its significant use in institutions of government, tends to be shut down as soon as some other component in one of the two previous situations will have condition to replace it. It may be considered a component "Recommended" if it would be suitable for all established technical policies. It should be noted that the development of new services or the reconstruction of significant parts of the existing ones should avoid the use of components classified as in transition;
- **In Study (S)**: component that is being evaluated and will be framed in one of the situations above, as soon as the evaluation process is completed;
- **Future Study (F)**: component not yet assessed and subject of further study.

The selection process of the components used by e-PING and its consequent classification in the situations above is responsibility of the Workgroups, which are composed of government specialists from institutions with which some kind of agreement or contract is to be established.

The selection is based on formal suggestions, internal demand from agencies of the federal government, Executive Power, and researches made by the workgroups.

The certification should be subject to closer scrutiny by the managers of e-PING. Given the variety of components addressed by the architecture, it will be necessary to develop a process of certification that covers from the assessment of physical characteristics of certain components (Smart Cards, for example) to others where there is a need to study aspects that involve the use of the component in the development of services (organization, information exchange and security, for example).

In this case, the government should establish agreements or accredit institutions to develop compliance tests, defining which components should be subject to procedures for approval, the criteria for evaluating the results and what are the conditions for completion of the procedures.

The full definition of the selection and certification process, taking into account the specificities of the segments, will be under responsibility of the Coordination of e-PING.

### 5.4.2. Audit of Compliance

Compliance with the specifications and recommendations by the agencies of the federal government - Executive Power, is a critical factor for success in the implementation and consolidation of e-PING. The managers of e-PING will recommend audit processes to verify the compliance with specifications of the architecture.

There may be delegation of responsibility for teams assembled especially for this purpose, composed of experts in government with experience in such procedures.

The preferred way of achieving this type of procedure, however, will be the use of auditing systems of the agencies. The Coordination of e-PING will act suggesting the basic criteria to be followed by the agencies.

Another issue to be considered will be the cooperation of government agencies acting in the sector, for it is expected contacts with institutions from other powers and spheres of government.

### 5.4.3. Creation and Maintenance of the Website

The whole process of exchanging information on e-PING with users, developers and interested parties is carried out, preferably, through the Internet, at <http://www.eping.e.gov.br>

In its most advanced stage of operation, the website will have as main features:

- Complete dissemination of documentation on the architecture: official versions and their updates, versions for public consultation, technical documentation for support, legal documentation and institutional connection;
- Availability of recommendations, determinations, technical specifications and policies for validation, approval, commentaries and suggestions;
- Publication of request for comments on the specification of components of the architecture;
- Availability of electronic means for receiving suggestions;
- Availability of links to documents, standards, rules or any other type of constant reference in e-PING.

### 5.4.4. Legal and Institutional Monitoring

e-PING will have constant support of Legal Advisory of the Ministry of Planning, Budget and Management to ensure adherence of the contents of the architecture documents to legal standards of the country.

Additionally, the Advisory will also have the responsibility to prepare all the necessary institutional part to ensure adequacy and that recommendations of e-PING will comply with the framework of legal instruments of ICT in the country.

The Coordination of e-PING can act to establish a form of collaboration with any other government agency able to provide legal support for conducting this activity.

### 5.4.5. Dissemination

The entire content of e-PING will be strongly advertised. The main forms of dissemination, in addition to the web site, are:

- Specific events, such as seminars, workshops and presentations in general;
- Participation in government events in the area of ICT and related areas;
- Participation in events targeted to specific audiences;
- Publication of all versions of e-PING and intermediary updates;
- Exchange with other spheres of government and other powers, with public, private and third sector institutions and foreign governments.

### 5.4.6. Training

Training events will be part of the agenda of implementation and management of e-PING. It is also envisaged the use of the Distance Learning (ODL).

The Coordination of e-PING will prepare and publish a minimum grade of training, so that each agency of the APF has subsidies for planning and estimating the investment on training of professionals involved in the process of adaptation to e-PING's recommendations.

Each agency will follow the standard definitions of e-PING in the assembly of its training plans, ensuring the provision of appropriate training for members of their technical teams.

## 5.5. Relationship with Government and Society

In this item the relationship between e-PING and the entities that make up the government and the society is discussed.

### 5.5.1. Organizations of the Federal Government - Executive Power

Under the scope of the Executive Power, participation of all levels of Public Federal Administration, its agencies, regulatory bodies, enterprises and public institutions is essential for the promotion and consolidation of interoperability in the public sector.

While general guidelines are managed by the Coordination of e-PING, each institution in it will have its responsibility in managing and ensuring usage of e-PING standards. The main assignments are to:

- Contribute to the development and continuous improvement of e-PING;
- Ensure that their organizational strategies consider that ICT systems members of e-government services under their responsibility are appropriate to recommendations of e-PING;
- Have a plan of implementation and adequacy of ICT infrastructure of the organization to e-PING architecture;
- Ensure that the domain of teams of the institution, the ability to define and use the specifications required for interoperability, providing support training when necessary;
- Establish point of contact in the institutions, to exchange information and Coordination with the needs of e-PING;
- Allocate and supply resources to support their processes of adaptation to e-PING;
- Use the opportunity to rationalize processes (as a result of increased interoperability) in order to improve the quality and reduce costs of delivering e-gov services).

### 5.5.2. Other Instances of Government (other Federal Powers, State and Municipal Governments)

In its initial phase, e-PING aims, basically, at the federal government, Executive Power. Other Powers (Judicial, Legislative and Federal Public Ministry) and other spheres of government (state and local) are considered as external institutions.

In this case, it is worth the guidance that the federal government - Executive Power does not determine the way how other entities of society should act. It only specifies the preferential way it interoperates with them.

The access of other instances of government is encouraged and recognized as a good strategy to improve the establishment of standards and consolidate e-PING as an architecture of standards for interoperability of the Brazilian government.

In the management plan of e-PING, other federal powers and state and local governments are priorities. The extension of the discussions to the bodies and institutions that make up those areas of government is a target to be reached as soon as the standards under the Federal Executive Power are signed and prepared.

### 5.5.3. Organizations of the Private Sector and Third Sector

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

All entities that participate in bidding processes to supply products and services for the Federal Executive Power shall meet the specifications and recommendations of e-PING.

Other forms of participation of these institutions in e-PING can be considered, setting up criteria to ensure transparency and equity of opportunities.

### 5.5.4. Citizen

Electronic government means, essentially, that the government is better serving the needs of the citizen, using resources of Technology, Information and Communication. e-PING architecture allows integration and makes available services in a full, safe and consistent way, to higher levels of efficiency in government.

The government should encourage the society to think, comment, and contribute with suggestions for innovations that can help it improve access to information and provision of its services. All procedures for dissemination and the inter-relationship of e-PING foresee participation of citizens and society in general, in the process of construction and management of the architecture.

## **Part II – Technical Specification of e-PING's Components**

## 6. Interconnection

### 6.1. Interconnection: Technical Policies

Technical policies for interconnection are:

**6.1.1.** APF organs should be interconnected using an IPv4 and plan its future change to IPv6. New hiring and network updating should foresee support to coexistence of protocols IPv4 and IPv6 and to products that support both protocols.

**6.1.2.** E-mail systems should use SMTP/MIME to deliver messages. For access to messages, protocols POP3 and/or IMAP shall be used, being encouraged the use of *web* interfaces for electronic mailing, observing when security aspects are necessary.

**6.1.3.** APF organs should use a scheme of Directory that is compatible with the Directory Service of the federal government, available on the electronic page [http://www.e.gov.br/correios/dir\\_redegoverno.htm](http://www.e.gov.br/correios/dir_redegoverno.htm).

**6.1.4.** APF organs should obey to the domain naming policy of the federal government, established on Resolution no. 7 which may be visualized on the electronic page [https://www.planalto.gov.br/ccivil\\_03/Resolucao/2002/RES07-02web.htm](https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm).

**6.1.5.** FTP and/or HTTP protocols should be used for files transference, observing its functionalities for recovering interruptions and for security, when necessary. HTTP should be prioritized for transference of files from Internet websites.

**6.1.7.** Whenever possible<sup>1</sup>, web-based technology must be used in applications that have utilized Terminal Emulation before.

**6.1.8.** Web Services technology is recommended as an e-PING's interoperability standard.

**6.1.9.** Web Services should be registered and located in directory structures compatible with the UDDI standard. The access protocol to this structure should be HTTP.

**6.1.10.** SOAP protocol is recommended for communication between clients and Web Services and the service specification should use WSDL language. See note about Web Services, item 6.3.

---

<sup>1</sup> There are products that may offer Access through browser to legacy systems, not needing to change these systems; normally these products may offer direct access to legacy screens or be substituted by graphic interfaces (GUIs). Attention should be paid to any security implication related to its use.

6.2. Interconnection: Technical Specifications

Table 1 – Specifications for Interconnectivity<sup>2</sup>

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Protocol of hypertext transference	Use HTTP/1.1 (RFC 2616) and/or HTTPS (RFC 2660).	<b>A</b>	
Delivering of electronic message	Use electronic message products that support interfaces in conformity with SMTP/MIME for delivering messages. Correlated RFCs: RFC 2821; RFC 2822; RFC 2045; RFC 2046; RFC 2646; RFC 2047; RFC 2231; RFC 2183; RFC 2048; RFC 3023 and RFC 2049.	<b>R</b>	
Content security of electronic message	S/MIME v3.1 should be used when appropriate for content security of general government messages, unless security requirements determine differently. Correlated RFCs: RFC 3852; RFC 2631; RFC 3850 and RFC 3851.	<b>R</b>	
Access to mail box	Unless security requirements determine differently, mail programs that provide access to mails should, at least, be according to POP3 for remote access to mail box. Correlated RFCs: RFC 1939; RFC 1957 and RFC 2449.  When additional facilities are needed, unless security requirements determine differently, mail programs that provide advanced facilities for access to mails should be according to IMAP3 for remote access to mail box. Correlated RFCs: RFC 3501; RFC 2342; RFC 2971; RFC 3502; RFC 3503; RFC 3510 and RFC 2910.	<b>R</b>	
Safe access to mail box	Access to mail box through unsafe networks should use HTTPS, according to delivering security standards. When necessary, use IMAP or POP, through TLS, in conformity with RFC 2595.	<b>R</b>	
Directory	Use central directory scheme, as defined in the following webpage: <a href="http://www.e.gov.br/correios/dir_redegoverno.htm">http://www.e.gov.br/correios/dir_redegoverno.htm</a>  LDAP v3 should be used for general Access to directory.	<b>R</b>	
Domain Naming Services	DNS should be used for solving Internet domain naming, according to RFC 1035. By its turn, the Brazilian government domain naming directives are found in Resolution no. 7 of the Electronic Government Executive Committee, on the webpage <a href="https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm">https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm</a>  Besides these directives, by decision of the Brazilian Internet Managing Committee, domain naming obeys to orientations from the Ministry of Planning, Budget	<b>A</b>	

<sup>2</sup> RFCs may accessed in <http://www.ietf.org/rfc.html>

Component	Specification	SIT	Observations
	and Management, to whom concerns managing domains .GOV.BR  The particularities of other government levels, for instance, government domains of the Federation Units, which include the abbreviation UF in their addresses, are referred on the webpage <a href="http://registro.br/faq/faq1.html#1">http://registro.br/faq/faq1.html#1</a>		
Electronic mail box addresses	Rules for defining names of electronic mail boxes should follow dispositions of the document “Individual-Functional Mail box of the Federal Government”, available on the webpage <a href="http://www.e.gov.br/correios/cp_individ.htm">http://www.e.gov.br/correios/cp_individ.htm</a>	<b>A</b>	
Protocols of file transferences	FTP (RFC 959 and RFC 2228) (with re-initialization and recovery) and HTTP (RFC 2616) for file transferences.	<b>R</b>	
Signalization protocols	Use of Session Initialization Protocol (SIP), defined by RFC 3261 as a protocol for controlling the application (signalization) layer to create, modify and terminate sessions with one or more participants.	<b>R</b>	
Instant Messaging	Model and requisites for Instant Messaging and Presence Protocol (XMPP) are defined by RFC 3920 e RFC 3921.	<b>T</b>	
	Model and requisites for Extensible Messaging and Presence Protocol (XMPP) are defined by RFC 3920 e RFC 3921.	<b>R</b>	
Short Messages Service	The Short Messages Service (SMS) should use protocol SMPP, as defined by SMS Forum <a href="http://www.smsforum.net">http://www.smsforum.net</a>	<b>R</b>	
LAN/WAN Intercommunication	IPv4 (RFC 791)	<b>A</b>	
	IPv6 (RFC 2460)	<b>S</b>	
Transport	TCP (RFC 793); UDP (RFC 768) whenever necessary, subject to security limitations.	<b>R</b>	
Advanced traffic	Whenever necessary, network traffic may be optimized by using MPLS (RFC 3031), given that it has, at least, four classes of service.	<b>R</b>	
Local Wireless Network	IEEE 802.11 b/g, in accordance with determinations of <i>Wi-Fi Alliance</i> ( <a href="http://www.wi-fi.org">http://www.wi-fi.org</a> ) and rules by Anatel ( <a href="http://www.anatel.gov.br">http://www.anatel.gov.br</a> ).	<b>R</b>	
Wireless metropolitan network	IEEE 802.16, in accordance with determinations of <i>WiMax Forum</i> ( <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> ) and rules by Anatel ( <a href="http://www.anatel.gov.br">http://www.anatel.gov.br</a> ).	<b>S</b>	

### 6.3. Web Services

The term *Web Service*<sup>3</sup> may be defined as a service available on the net (Internet or Intranet) that uses a standard system – XML – for exchanging messages, independently of operational system or programming language, with two basic properties:

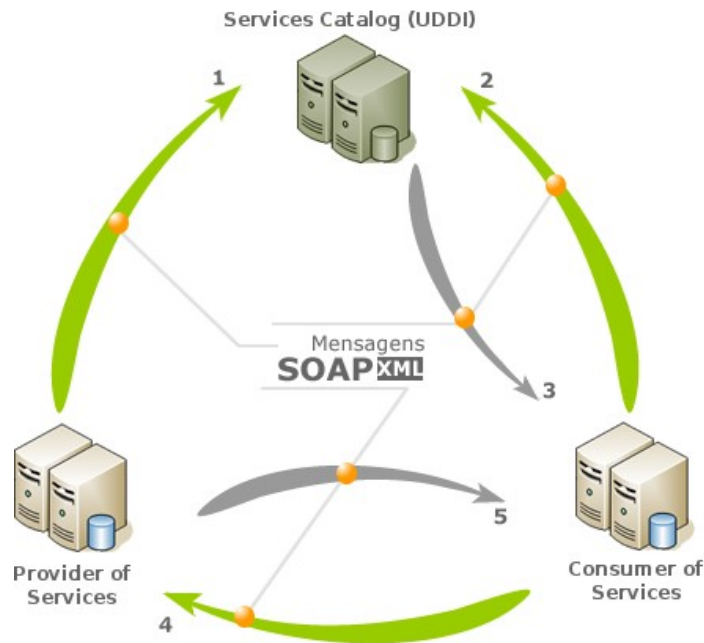
(a) making possible its finding: when creating a Web Service, it should be published, registered in a services catalog so that potential users may find it. The catalog may use UDDI.

<sup>3</sup> This definition of Web Service was adapted from a book by Ethan Cerami - *Web Services Essentials - Distributed Applications with XML-RPC, SOAP, UDDI & WSDL, 2002. O’Reilly & Associates Inc., Sebastol, CA.*

Other forms of repositories may be used, among them ebXML – currently under research by e-PING;

(b) self-description: Web Services provide a complete description of its services and of how users (developers) may create applications to interact with them. This description is made through WSDL.

Image 3 presents the generic steps to provide and consume a service through Web Services:



**Image 3 – General vision of Web Services working<sup>4</sup>.**

(1) product is registered when the service provider describes his service using WSDL. This definition is published in a services catalog;

(2) the consumer of services makes one or more consultations to the services directory to locate a service and to verify which is the communication with the service;

(3) information about the service located is sent to the service’s consumer. Such information is part of the WSDL provided by the services provider, such as the address where the requested service is located;

(4) and (5) refer to consume of the service. Provider and consumer exchange messages (XML) among them. When receiving a message, Web Service will validate the agreement with information contained in the WSDL. From this moment on, Web Service knows how to deal with the message, how to process it (perhaps sending it to another program) and it knows how to assemble the consumer’s response.

The need of integration among the different government information systems, implemented in different technologies implies in adopting an interoperability standard to ensure scalability, easiness of use, besides allowing instant and real time updating.

Due to this context, it is understood that using Web Services is adequate to these necessities. Web Services offer a dynamic approach to integration, in which services are automatically located, determined and used. Web Services technology provides a standard way of interoperation between different applications of software. Besides, a Web Service may have different levels of granularity. Both an application of a web page and a software component, which encompass a complex trading rule, may be transformed in Web Services, what makes its use very flexible.

<sup>4</sup> Image 3 is an adaptation of the image made available by W3C Working Group - <http://www.w3.org/TR/wsarch/#whatis>.

Web Services support for direct integration with other software applications uses messages written in XML as an interoperability standard. These messages are encompassed in standard online application protocols – SOAP. It is important to stress that XML documents structures are described through XML *Schemas*, as a way of validating the types of data belonging to business lines.

**Table 2 – Specifications for Web Services<sup>5</sup>**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Information exchange protocol	SOAP v1.2, as defined by W3C <a href="http://www.w3.org/TR/soap12-part1/">http://www.w3.org/TR/soap12-part1/</a> <a href="http://www.w3.org/TR/soap12-part2/">http://www.w3.org/TR/soap12-part2/</a> SOAP protocol specifications can be found at <a href="http://www.w3.org/TR/soap12-part0/">http://www.w3.org/TR/soap12-part0/</a>	R	
Registering infrastructure	UDDI v3.0.2 (Universal Description, Discovery and integration) specification defined by OASIS <a href="http://uddi.org/pubs/uddi_v3.htm">http://uddi.org/pubs/uddi_v3.htm</a>	R	
	ebXML ( <i>Electronic Business using eXtensible Markup Language</i> ). Specification can be found at <a href="http://www.ebxml.org/specs/index.htm">http://www.ebxml.org/specs/index.htm</a>	S	
Service definition language	WSDL 1.1 ( <i>Web Service Description Language</i> ) as defined by W3C. Specification can be found at <a href="http://www.w3.org/TR/wsdl">http://www.w3.org/TR/wsdl</a>	R	
	WSDL 2.0 ( <i>Web Service Description Language</i> ) as defined by W3C. Specification can be found at <a href="http://www.w3.org/TR/wsdl20/">http://www.w3.org/TR/wsdl20/</a>	S	
Basic interoperability profile	<i>Basic Profile 1.1 Second Edition</i> , as defined by WS-I <a href="http://www.ws-i.org/Profiles/BasicProfile-1.1.html">http://www.ws-i.org/Profiles/BasicProfile-1.1.html</a>	S	Version 1.2 of Basic Profile is found as a working draft at <a href="http://www.wsi.org/Profiles/BasicProfile-1.2.html">http://www.wsi.org/Profiles/BasicProfile-1.2.html</a>
Remote <i>portlets</i>	WSRP 1.0 (Web Services for Remote Portlets) as defined by OASIS <a href="http://www.oasis-open.org/committees/wsrp">http://www.oasis-open.org/committees/wsrp</a>	S	

**6.4. Electronic Message (E-mail)**

In order to solve out possible doubts, e-PING will use the following concepts:

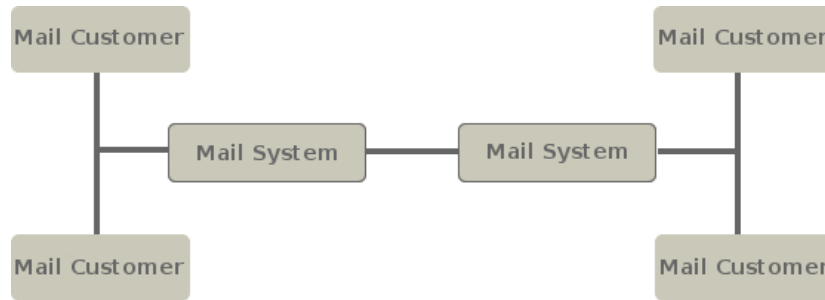
**Electronic Message Delivering**

Electronic Message Delivering is defined as the interface between two mailing systems.

<sup>5</sup> Security matters related to Web Services will be addressed on chapter 7.

**Access to mail box**

Access to mail box is defined as the interface between a mailing client and a mailing service



**Image 4 – Interfaces between Mail systems and clients**

**6.5. VPN**

Virtual Private Network (VPN) is a private virtual tunnel built over a public or private network infrastructure. Instead of using dedicated circuits or parcel networks to connect remote networks, it usually uses internet infrastructure.

Such usage, as a connection infrastructure between private network hosts, is a good solution in terms of costs, but not in terms of privacy, as moving data may be read by any equipment, being necessary the use of VPN.

Virtual tunnels move around cryptographic data over public or private networks, forming a safe virtual channel through these networks. In order to do so, tunneling protocols are used.

Devices responsible for managing VPN must be capable of ensuring data privacy, integrity and authenticity.

VPN specifications are presented in the security segment.

**6.6. Peer-to-peer networks**

Peer-to-Peer (P2P) are distributed systems that consist of interconnected nodes, capable of self-organization in network topologies, aiming to share resources such as processing, storing and band wide, capable of adapting to malfunctions and to accommodate transient node populations, while they keep acceptable connectivity and performance, not depending on intermediation or support of an central authority (server).

Although P2P systems may contribute to resource sharing and large scale cooperation, with a decentralized control and low coupling, they are still susceptible to several security problems, turning impossible the systematic use of P2P networks. This subject will be addressed later.

## 7. Security

### 7.1. Security: Technical Policies

**7.1.1.** Data, information and government information systems may be protected against threats in a way to reduce risks and ensuring integrity, confidentiality and availability.

**7.1.2.** Data and information must be kept with the same level of protection, independently of the means in which they are processed, stored or moved.

**7.1.3.** Information that is transported in unsafe networks, including wireless, must adopt security controls available in the transport layer (IPv4). In case of wireless LAN the security protocols specific of this technology must be used whenever necessary. Government information systems must be protected against security risks in connection with these networks.

**7.1.4.** Information, services and infrastructure security requirements must be identified and treated according to classification of information, defined service levels and result of risk analysis.

**7.1.5.** Security should be addressed in a preemptive way. For systems that support critical processes continuity plans must be elaborated, and they should address residual risks aiming to reach minimum levels of production.

**7.1.6.** Security is a process that must be inserted in all steps of the development cycle of a system.

**7.1.7.** Systems must possess history logs in order to allow inspections and forensic proofs, being necessary adoption of a centralized synchronism system, as well as the use of mechanisms that ensure authenticity of stored registers, if possible with a digital signature.

**7.1.8.** XML security services must be in accordance with W3C specifications.

**7.1.9.** In metropolitan wireless networks, it is recommended adopting random figures in security associations, different identifiers for each service and limitation of authorization keys lifetime.

**7.1.10.** Use of cryptography and digital certification for protection of data traffic and storing, access control, digital signature and code signature must be according to ICP-Brazil rules.

**7.1.11.** Documentation of systems, security controls and environments' topologies must be kept updated and protected.

**7.1.12.** Users must know their responsibilities in regard to security and should be able to perform their tasks and correctly use the means of access.

**7.1.13.** APF bodies, envisaging improvement in security, must have as a reference rule NBR ISO/IEC 27002:2005, a code of practice for management of information security, and NBR ISO/IEC 27001:2006 for systems of management of information security, edited by ABNT.

7.2. Security: Technical Specifications

Table 3 – Technical Specifications for IP Security

Component	Specification	SIT	Observations
	<p>A = Adopted                      R = Recommended                      T = In Transition                      S = In Study                      F = Future Study</p>		
Data transference in unsafe networks thorough protocols HTTP, LDAP, IMAP, POP3, Telnet whenever possible. – Security of IPv4 networks in transport layer	<p>TLS – <i>Transport Layer Security</i>, RFC2246 (<a href="http://www.ietf.org/rfc/rfc2246.txt">http://www.ietf.org/rfc/rfc2246.txt</a>). In case it is necessary, protocol TLS v1 may emulate SSL v3.</p> <p>HTTP about TLS, RFC 2818 (<a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a>)</p> <p>The following cryptographic algorithms may be implemented:</p> <ul style="list-style-type: none"> <li>- Algorithms for exchange of session Keys, during <i>handshake</i>:                          RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;</li> <li>- Algorithms for definition of encryption key: RC4, IDEA, 3DES, AES;</li> <li>- Algorithms that implement <i>hash</i> function for definition in MAC:                          SHA-256 or SHA-512.</li> <li>- Type of Digital Certificate - X.509 v3 - ICP-Brazil, <a href="http://www.iti.gov.br">http://www.iti.gov.br</a></li> </ul> <p>SASL - <i>Simple Authentication and Security Layer</i>, RFC 4422 (<a href="http://www.ietf.org/rfc/rfc4422.txt">http://www.ietf.org/rfc/rfc4422.txt</a>).</p>	R	
Security of IPv4 networks	<p><i>IPSec Authentication Header</i> RFC 2402 e RFC 2404 (<a href="http://www.ietf.org/rfc/rfc2402.txt">http://www.ietf.org/rfc/rfc2402.txt</a> <a href="http://www.ietf.org/rfc/rfc2404.txt">http://www.ietf.org/rfc/rfc2404.txt</a>)</p> <p>IKE – <i>Internet Key Exchange</i>, RFC 2409 (<a href="http://www.ietf.org/rfc/rfc2409.txt">http://www.ietf.org/rfc/rfc2409.txt</a>), must be used whenever necessary to negotiation of security association between two entities for exchange of key materials.</p> <p>ESP – <i>Encapsulating Security Payload</i>, RFC 2406 (<a href="http://www.ietf.org/rfc/rfc2406.txt">http://www.ietf.org/rfc/rfc2406.txt</a>) Requisite for VPN – Virtual Private Network.</p>	R	
Security of IPv4 networks for application protocols	<p>S/MIME v3 ,RFC2633 (<a href="http://www.ietf.org/rfc/rfc2633.txt">http://www.ietf.org/rfc/rfc2633.txt</a>) must be used when appropriate for security of general government messages.</p>	R	
Security of IPv6 networks in network layers	<p>IPv6 defined in RFC2460 (<a href="http://www.ietf.org/rfc/rfc2460.txt">http://www.ietf.org/rfc/rfc2460.txt</a>) presents implementation of native security in the protocol.</p> <p>IPv6 specifications defined two security mechanisms:                      AH (<i>Authentication Header</i>) RFC2402</p>	R	

Component	Specification	SIT	Observations
	( <a href="http://www.ietf.org/rfc/rfc2402.txt">http://www.ietf.org/rfc/rfc2402.txt</a> ) or IP authentication, and ESP ( <i>Encrypted Security Payload</i> ) RFC2406 ( <a href="http://www.ietf.org/rfc/rfc2406.txt">http://www.ietf.org/rfc/rfc2406.txt</a> ).		

**Table 4 – Technical Specifications for Electronic Mailing Security**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Access to mail box	Access to mail box should take place through client of the used electronic mail software, considering native security elements of the client. When it is not possible to use the specific client or when it is necessary to access the mail box through unsafe networks (for example: Internet) HTTPS should be used in accordance with delivering security standards described in RFC 2595 ( <a href="http://www.ietf.org/rfc/rfc2595.txt">http://www.ietf.org/rfc/rfc2595.txt</a> ), about usage of TLS with IMAP, POP3 e ACAP.	<b>R</b>	
E-mail content	S/MIME V3 must be used when appropriate to security of general government messages. This includes RFC 3369 ( <a href="http://www.ietf.org/rfc/rfc3369.txt">http://www.ietf.org/rfc/rfc3369.txt</a> ), RFC 3370 ( <a href="http://www.ietf.org/rfc/rfc3370.txt">http://www.ietf.org/rfc/rfc3370.txt</a> ), RFC 2631 ( <a href="http://www.ietf.org/rfc/rfc2631.txt">http://www.ietf.org/rfc/rfc2631.txt</a> ), RFC 3850 ( <a href="http://www.ietf.org/rfc/rfc3850.txt">http://www.ietf.org/rfc/rfc3850.txt</a> ) and RFC 3851 ( <a href="http://www.ietf.org/rfc/rfc3851.txt">http://www.ietf.org/rfc/rfc3851.txt</a> ).	<b>R</b>	
E-mail deliver	Verify if reverse is according to name in HELO, for ensuring message origin and to control SPAM.	<b>F<sup>6</sup></b>	
Signature	Use ICP-Brazil standard for e-mail signature, when necessary. According to disposition of Decree 3,996 of October 31, 2001.	<b>R</b>	

<sup>6</sup> Possible implication on performance; possible discarding of valid messages; impossibility of treating multiple domains.

**Table 5 – Technical Specifications for Electronic Mailing Security**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Encrypting algorithm	3DES or AES	<b>R</b>	
Signature/hasing algorithm	SHA-256 or SHA-512	<b>R</b>	Systems must have support to hash algorithm MD5 with RSA, for ensuring compatibility with previous implementations.
Signature/hasing algorithm	SHA-224 or SHA-238	<b>S</b>	Considering that they were included in the Final Report of the Work Group on Cryptography I, instituted by Institutional Security Office of the Presidency of the Republic, however, they have not yet been transformed into norm of the Federal Public Administration
Algorithm for moving content/ session cryptographic key	RSA	<b>R</b>	
Cryptographic algorithms based on elliptical curves	ECMQV and ECDH, both for key settlement, ECDSA for digital signature, and ECIES for encryption and safe transport of cryptographic keys. Use of these algorithms is subject to regulation and normalization by ICP-Brazil concerning security requisites.	<b>S</b>	
Requisites of security for cryptographic modules	FIPS 140-2 – minimum requirements for storing solutions of private keys and digital certificates issued in the sphere of ICP-Brazil, which use devices both of software and hardware of the type token or smart card. Joining the standard: a. Follow, at least, rules established for levels 1 and 2 of standard security; b. Follow, at least, rules established for level 2 of security of standard FIPS 140-1 or 2, for verification of hardware violation ( <i>Tamper Evidence</i> )	<b>R</b>	

**Table 6 – Technical Specifications for Security – Systems Development**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
XML Signatures	Syntax and Processing of XML signature (XMLsig) as defined by W3C <a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a>	<b>R</b>	
XML Encrypting	Syntax and Processing of XML Encrypting (XMLenc) as defined by W3C <a href="http://www.w3.org/TR/xmlenc-core/">http://www.w3.org/TR/xmlenc-core/</a>	<b>R</b>	
XML Signature and encrypting	Transformation of encrypting for XML signature as defined by W3C <a href="http://www.w3.org/TR/xmlenc-decrypt">http://www.w3.org/TR/xmlenc-decrypt</a>	<b>R</b>	
Main XML management when a PKI environment is used	XML – Key Management Specification (XKMS 2.0) as defined by W3C <a href="http://www.w3.org/TR/xkms2/">http://www.w3.org/TR/xkms2/</a>	<b>R</b>	
Authentication and authorization of XML access	SAML – as defined by OASIS when a ICP environment is used <a href="http://www.oasisopen.org/committees/security/index.shtml">http://www.oasisopen.org/committees/security/index.shtml</a>	<b>R</b>	
Intermediation or Federation of Identities	WS-Security 1.1 – Standards framework to ensure integrity and confidentiality of SOAP messages. ( <a href="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0.pdf">http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0.pdf</a> ).  WS-Trust 1.3 – extensions for WSSecurity standard, defining the use of credentials of security and distributed trusting management. ( <a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512</a> ).	<b>S</b>	The previous component (SAML) may be used together with this component after proper studies
Browsers	Only use connection witnesses of permanent character (cookies) with user agreement. Resolution no 7 of the Electronic Government Executive Committee (chapter II, article 7)	<b>A</b>	

**Table 7 – Technical Specifications for Security – Network Services**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Directory	Normative Decision No. 2, October 3 2002 – Published in the D.O. (Official Gazette) of October 4 2002. Section 1, page 85. LDAPv3 RFC 2251 <a href="http://www.ietf.org/rfc/rfc2251.txt">http://www.ietf.org/rfc/rfc2251.txt</a> . LDAP v3 extension for TLS RFC2830 <a href="http://www.ietf.org/rfc/rfc2830.txt">http://www.ietf.org/rfc/rfc2830.txt</a> .	<b>R</b>	
DNS	Resolution no. 7 of July 29 2002 – Electronic Government Executive Committee Security Practices for Network Administrators NIC BR Security Office <a href="http://www.nbso.nic.br/docs/seg-adm-redes/seg-admchklist.pdf">http://www.nbso.nic.br/docs/seg-adm-redes/seg-admchklist.pdf</a> Version 1.2 May 16 2003 Securing an internet name server, CERT – August 2002.	<b>R</b>	
Safe transference of files	HTTPS RFC 2818 <a href="http://www.ietf.org/rfc/rfc2818.txt">http://www.ietf.org/rfc/rfc2818.txt</a> .	<b>R</b>	
Safe transference of files	SSH FTP	<b>F</b>	Documents are still in draft form
Safe transference of files	Securing FTP with TLS, RFC 4217 <a href="http://www.faqs.org/rfcs/rfc4217.html">http://www.faqs.org/rfcs/rfc4217.html</a> and RFC 2246 <a href="http://www.faqs.org/rfcs/rfc2246.html">http://www.faqs.org/rfcs/rfc2246.html</a>	<b>S</b>	
Newsgroup		<b>F</b>	
Instant Message	RFC 2778 ( <a href="http://www.ietf.org/rfc/rfc2778.txt">http://www.ietf.org/rfc/rfc2778.txt</a> ), RFC 3261 ( <a href="http://www.ietf.org/rfc/rfc3261.txt">http://www.ietf.org/rfc/rfc3261.txt</a> ), RFC 3262 ( <a href="http://www.ietf.org/rfc/rfc3262.txt">http://www.ietf.org/rfc/rfc3262.txt</a> ), RFC 3263 ( <a href="http://www.ietf.org/rfc/rfc3263.txt">http://www.ietf.org/rfc/rfc3263.txt</a> ), RFC 3264 ( <a href="http://www.ietf.org/rfc/rfc3264.txt">http://www.ietf.org/rfc/rfc3264.txt</a> ) and RFC 3265. <a href="http://www.ietf.org/rfc/rfc3265.txt">http://www.ietf.org/rfc/rfc3265.txt</a> .	<b>S</b>	
Time synchrony	RFC 1305 IETF- <i>Network Time Protocol – NTP version 3.0</i> ( <a href="http://www.ietf.org/rfc/rfc1305.txt">http://www.ietf.org/rfc/rfc1305.txt</a> ). RFC 2030 IETF- <i>Simple Network Time Protocol - SNTP version 4.0</i> <a href="http://www.ietf.org/rfc/rfc2030.txt">http://www.ietf.org/rfc/rfc2030.txt</a> .	<b>R</b>	
Time stamping	RFC 3628 TSAs - <i>Policy Requirements for Time-Stamping Authorities</i> <a href="http://www.ietf.org/rfc/rfc3628.txt">http://www.ietf.org/rfc/rfc3628.txt</a> , <i>Time-Stamp Protocol</i> , RFC 3161 ETSI TS101861 ( <i>Time-Stamping Profile</i> ) <a href="http://www.ietf.org/rfc/rfc3161.txt">http://www.ietf.org/rfc/rfc3161.txt</a> .		

**Table 8 – Technical Specifications for Security of Wireless Networks**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Wireless MAN <sup>7</sup> 802.16-2004 <sup>8</sup> 802.16.2-2004 <sup>9</sup> 802.16e <sup>10</sup> e 802.16f <sup>11</sup>	Use PKM-EAP ( <i>Privacy Key Management - Extensible Authentication Protocol</i> ) with: <ul style="list-style-type: none"> <li>• EAP – TLS or TTLS;</li> <li>• AES<sup>12</sup> (Advanced Encryption Standard).</li> </ul>	<b>S</b>	
Wireless LAN 802.11	Use specification WPA2 ( <i>Wi-Fi Protect Access</i> ).	<b>R</b>	

**Table 9 – Technical Specifications for Security – Evidence Collection, Treatment and Archiving**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Registers preservation	<i>Guidelines for Evidence Collection and Archiving</i> , RFC 3227 ( <a href="http://www.ietf.org/rfc/rfc3227.txt">http://www.ietf.org/rfc/rfc3227.txt</a> ).	<b>R</b>	
Incident response	<i>Expectations for Computer Security Incident Response</i> , RFC 2350 ( <a href="http://www.ietf.org/rfc/rfc2350.txt">http://www.ietf.org/rfc/rfc2350.txt</a> ).	<b>R</b>	
Forensic Informatics	<i>Guide to Integrating Forensic Techniques into Incident Response – NIST - Special Publication 800-86 (Draft) –</i> ( <a href="http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf">http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf</a> ).	<b>R</b>	

<sup>7</sup> 802.16 is defined by IEEE as a technologic interface for wireless metropolitan access network - WMAN.

<sup>8</sup> <http://standards.ieee.org/getieee802/download/802.16-2004.pdf>.

<sup>9</sup> <http://standards.ieee.org/getieee802/download/802.16.2-2004.pdf>.

<sup>10</sup> <http://standards.ieee.org/getieee802/download/802.16e-2005.pdf>.

<sup>11</sup> <http://standards.ieee.org/getieee802/download/802.16f-2005.pdf>.

<sup>12</sup> <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf>.

## 8. Means of Access

### 8.1. Means of Access: Technical Policies

Technical policies to allow access to federal government electronic services for overall society – citizens, other government spheres, other Powers, civil servants, private companies and other institutions – are:

**8.1.1.** Information systems of the government should be planned in a way to respect Brazilian legislation, providing accessibility resources to citizens with special necessities, ethnic minorities and those under risk of social or digital exclusion. Counter service should be considered in all its scope, in a way to make possible that benefits from use of electronic government services come to be extended to population who does not have direct access to these services through provisioned devices.

**8.1.2.** Government information systems that offer electronic government services:

- When using internet as a means of communication and work stations as access devices, they will be specially projected to offer access to information using web communication technologies and protocols based on browsers;
- When using other access devices, such as mobile phones, digital television and smart cards, they may use other interfaces besides web browsers;
- Should be projected to make available to users electronic government services through several means of access;
- Should foresee gradual substitution of “login/password” systematic for user authentication by use of digital certificates, preferentially contained in smart cards or tokens, according to standards put forward by ICP-Brazil (reference: <http://www.icpbrasil.gov.br/>);
- New services should be created with support to user authentication through ICP-Brazil digital certificates;
- In this version, e-PING deals with the following means of access:
  - Work stations, considering users direct or indirect access, through counter services;
  - Smart cards, tokens and other cards;
  - Other means of access, such as mobile phones, hand-held phones and digital television will be subject to future studies for determining standards accepted by the federal government.

**8.1.3.** Government information systems, built to support a specific access device should follow, obligatorily, specifications published on e-PING for that device.

**8.1.4.** All government information systems that provide electronic services should be capable of using internet as a means of communication, be it direct or through third party services.

**8.1.5.** Development of electronic government services should be directed as to deliver to users that do not have access to up-to-date technologies available in the market. On the other hand, it should also be taken into account the necessity of delivering to users with special necessities, requisite that involves use of more sophisticated and specific use resources. In a way to conciliate these necessities, recommendations of the Electronic Government Accessibility Model (e-MAG) should be observed.<sup>13</sup>

**8.1.6.** When Internet is used as a means of communication, government information systems should be projected in a way that a maximum of information may be worked from browsers that respect the minimum standard given by support to technical specifications foreseen in section 8.2. Completely, e-PING recommends that every electronic government service clearly specify (preferentially in the home page) the minimum browser versions that support the functionalities required by the service associated.

**8.1.7.** When the internet is used as a means of communication, additional middleware or plug-ins may be used, if there is no technically viable alternative to optimize the browser functionality in work stations. In this case, this additional software should be offered without payment of license fees and should be in accordance with all correspondent technical specifications described in e-PING. Besides, it should be made available in a safe repository kept by the government body responsible for the application.

<sup>13</sup> BRAZIL. Ministry of Planning, Budget and Management. Accessibility Recommendations for construction and adaptation of contents of the Brazilian Government over the internet: accessibility models. Version 2.0. Brasília, 2005. Available at: (<http://www.governoeletronico.gov.br/emag/>). Accessed in July 13, 2006.

**8.1.8.** Electronic government services should be projected in a way to ensure users of content authenticity through issuing of a digital certificate, according to standards foreseen by ICP-Brazil. Reference: <http://www.icpbrasil.gov.br/>. In this sense, all websites should obligatorily use HTTPS instead of HTTP.

**8.1.9.** Society’s necessity allied to government possibility of developing and implementing electronic services will give ground to definition of technical specifications demanded through available means of access. Techniques of management of content and technologies that make possible the adaptation of devices to support electronic government services may be used to make access easier through the minimum web browser standard (according to item 3. General Policies) and to make viable the use of public kiosks, service counters and Central Citizen Services (such as “Telecentros”).

**8.1.10.** Information systems of the federal government should set out, when necessary and when technically and economically viable, the construction of adaptors that allow access to information about web electronic services for a diversity of environments, presenting acceptable responsiveness and reduced costs.

These adaptors may also be used as an alternative way of allowing access to ethnic minorities, bearers of visual disabilities (for instance: through use of text translators, bigger fonts and graphics, audio, etc.). Such aspects are addressed by Resolution no 7 of the Electronic Government Executive Committee. Reference:

[https://www.planalto.gov.br/ccivil\\_03/Resolucao/2002/RES07-02web.htm](https://www.planalto.gov.br/ccivil_03/Resolucao/2002/RES07-02web.htm)

**8.1.11.** It will be considered preferential those types of archives that have as packing standard the “xml”, in order to facilitate interoperability among electronic government systems.

**8.1.12.** Electronic government systems that make documents available to their users should do it by employing, in the access link to the document, clear information related to its provenience, version, publishing date and format. Publishing date refers to that in which the document was published on the official gazette, for the cases in which this measure is required, or date of availability on the website, for the remaining cases. Other information about the document, such as author, writer, issuer, date or others relevant to its precise characterization should be in the field “properties” of the document.

**8.2. Means of Access: Technical Specifications for Work Stations**

For development of minutes of documents or works that need to be cooperatively created by more than one person and/or body, the formats presented in Table 9 may be used.

Concerning the writing of final versions of documents, which should be sent to other organs or even digitally archived, it is recommended use of pdf/a format. Documents that need integrity and/or property warranty should be digitally signed by its author, using ICP-Brazil certificate.

Mention to products that generate the file formats cited on Table 9 has the objective of identifying a **minimum reference** from which e-gov services should exchange information, being able to receive and send files through **equal or subsequent** versions.

**Table 10 – Technical Specifications – Work Stations**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Browsers	See item 3. General Policies	<b>S</b>	
Group of characters and alphabets	UNICODE standard versão 4.0, latin-1, UTF8, ISBN 0-321-18578-1.	<b>R</b>	

Component	Specification	SIT	Observations
Format of hypertext exchange	HTML version 4.01 (.html or .htm), generated according to specifications of W3C <sup>14</sup> .	A	
	XHTML version 1.0 or 1.1 (.xhtml), generated according to specifications of W3C <sup>15</sup> .	A	
	XML version 1.0 or 1.1 (.xml), generated according to specifications of W3C <sup>16</sup> .	A	
	SHTML (.shtml).	R	
	MHTML (.mhtml or .mht) <sup>17</sup>	T	
Document-type files	XML version 1.0 or 1.1 (.xml), or with (optional) XSL (.xsl) format, generated according to specifications of W3C <sup>18</sup> .	R	
	Open Document (.odt), generated according to specifications of ISO/IEC 26300 standard <sup>19</sup> .	R	
	OpenOffice.org XML (.sxw), generated in the format of OpenOffice version 1.0.	T	
	Rich Text Format (.rtf)	T	
	PDF (.pdf) generated in format up to version 1.3.	T	
	PDF open version PDF/A <sup>20</sup> .	R	
	Pure text (.txt)	A	
	HTML version 4.01 (.html or .htm), generated according to specifications of W3C.	R	
	Microsoft Word document (.doc), generated in MS Office format of version up to 2000.	T	
Spreadsheet Files	Open Document (.ods), generated according to specifications of ISO/IEC 26300.	R	
	OpenOffice.org XML (.sxc). generated in Open Office format version 1.0.	T	
	MS Excel Spreadsheet (.xls), generated in MS Office format of version up to 2000.	T	
Presentation files	Open Document (.ods), generated according to specifications of ISO/IEC 26300.	R	
	OpenOffice.org XML (.sxi). generated in Open Office format version 1.0.	T	
	HTML (.html or .htm), generated according to specifications of W3C.	R	
	MS Power Point Presentation (.ppt), generated in MS Office format of version up to 2000.	T	

<sup>14</sup> HTML 4.01 Specification - W3C Recommendation 24 December 1999. Available at: <http://www.w3.org/TR/html4/>.

<sup>15</sup> XHTML 1.0 The Extensible HyperText Markup Language (Second Edition): A Reformulation of HTML 4 in XML 1.0 - W3C Recommendation 26 January 2000, revised 1 August 2002. Available at: <http://www.w3.org/TR/xhtml1/>.

<sup>16</sup> Extensible Markup Language (XML) 1.0 (Third Edition) - W3C Recommendation 04 February 2004. Available at: <http://www.w3.org/TR/2004/REC-xml-20040204/>.

Extensible Markup Language (XML) 1.1 - W3C Recommendation 04 February 2004, edited in place 15 April 2004. Available at: <http://www.w3.org/TR/2004/REC-xml11-20040204/>.

<sup>17</sup> Microsoft web files packing format (Mime Encapsulation of Aggregate HTML Documents).

<sup>18</sup> Extensible Stylesheet Language (XSL) Version 1.0 - W3C Recommendation 15 October 2001. Available at: <http://www.w3.org/TR/xsl/>.

<sup>19</sup> Open Document Format for Office Applications (OpenDocument) v1.0 -ISO/IEC 26300 standard. Available at: <http://www.iso.org/>.

<sup>20</sup> 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. Available at: <http://www.iso.org/>.

Component	Specification	SIT	Observations
Data bank-type files for work stations	XML versions 1.0 or 1.1 (.xml)	R	
	MySQL Database (.myd, .myi), generated in the format of MySQL, version 4.0 or superior.	R	
	Pure text (.txt)	A	
	Pure text (.csv) – comma-separated values	A	
	Object Database File (.odb), generated in the format of BrOffice.org (or OpenOffice.org) version 2.0 or subsequent.	R	
	MS Access file (.mdb), generated in the format of MS Office, up to version 2000.	T	
Exchange of graphic information and static images	PNG (.png), generated according to specifications of W3C <sup>21</sup> – ISO/IEC 15948:2003 (E).	A	
	TIFF (.tif) <sup>22</sup>	R	
	SVG (.svg), generated according to specifications of W3C <sup>23</sup>	R	
	JPEG File Exchange Format (.jpeg, .jpg ou .jif) <sup>24</sup>	R	
	Open Document (.odg), generated according to specifications of ISO/IEC 26300 standard.	R	
	OpenOffice.org XML (.sxd). generated in Open Office format version 1.0.	T	
	XCF (.xcf), generated in format of GIMP version 1.0 or superior.	R	
	BMP (.bmp).	T	
	GIF (.gif), generated according to specifications of GIF87a e GIF89a <sup>25</sup> .	T	
	Corel Photo-Paint Image (.cpt), generated in Corel Draw suit up to version 7.	T	
	Photoshop Image (.psd), generated in Adobe Photoshop format up to version 4.	T	
Vector graphics	SVG (.svg), generated according to specifications of W3C.	R	
	Open Document (.odg), generated according to specifications of ISO/IEC 26300 standard.	R	
	OpenOffice.org XML (.sxd). generated in Open Office format version 1.0.	T	
	Corel Draw Graphic (.cdr), generated in format up to version 7.	T	
	MSX (.msx), generated in the format of Corel Draw suite up to version 7.	T	
	MS Visio graphic (.vss or .vsd), generated in format of version up to 2000.	T	
	Windows Metafile (.wmf).	T	
Specification of Animation standards	SVG (.svg), generated according to specifications of W3C.	R	

<sup>21</sup> Portable Network Graphics (PNG) Specification (Second Edition). W3C Recommendation 10 November 2003. ISO/IEC 15948:2003 (E) - Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification. Available at: <http://www.w3.org/TR/2003/RECPNG-20031110/>. Access in: Dec 7, 2005.

<sup>22</sup> Tagged Image File Format (Adobe Systems).

<sup>23</sup> Scalable Vector Graphics (SVG) 1.1 Specification. W3C Recommendation 14 January 2003. Available at: <http://www.w3.org/TR/2003/REC-SVG11-20030114/>. Access in: Dec 7, 2005.

<sup>24</sup> JPEG File Exchange Format (version 1.02) 1 September 1992. Available at: <http://www.jpeg.org/public/jfif.pdf>. Access in: Dec 7, 2005.

<sup>25</sup> Graphics Exchange Format (CompuServe/America Online, Inc.).

Component	Specification	SIT	Observations
	GIF (.gif), generated according to specifications of GIF89a.	T	
	Shockwave Flash (.swf), generated in format of Macromedia Flash up to version 4, of Macromedia Shockwave version 1.	T	
Audio and video files	.mpg	R	
	MPEG-4 audio and video, Part 14 (.mp4) <sup>26</sup>	R	
	MIDI (.mid) <sup>27</sup>	R	
	Audio Ogg Vorbis I (.ogg) <sup>28</sup>	R	
	<i>Audio-Video Interleaved</i> (.avi), with Xvid codification.	T	
	<i>Audio-Video Interleaved</i> (.avi), with divX codification.	T	
	Audio MPEG-1, Audio Layer 3 (.mp3) <sup>29</sup>	T	
	<i>Real Media</i> (.rm ou .rmm), generated in format of Real Audio Media Player, up to version 8.	T	
	<i>Real Audio</i> (.ra ou .ram), generated in format of Real Audio Media Player, up to version 8.	T	
	WAVE (.wav)	T	
	<i>Shockwave Flash</i> (.swf), generated in format of Macromedia Flash, up to version 4 or Macromedia Shockwave, version 1.	T	
	<i>Windows Media Video</i> (.wmv), generated in format of Windows Media Player, up to version 6.4.	T	
	<i>Windows Media Audio</i> (.wma), generated in format of Windows Media Player, up to version 6.4.	T	
	<i>QuickTime</i> (.mov) generated in format of Apple Quicktime, up to version 6.	T	
<i>QuickTime</i> (.qt), generated in format of Apple Quicktime, up to version 6.	T		
Compression of general use files	ZIP (.zip).	R	
	GNU ZIP (.gz).	R	
	TAR Pack (.tar).	R	
	Compacted TAR Pack (.tgz ou .tar.gz).	R	
	BZIP2 (.bz2).	R	
	TAR Pack compressed with BZIP2 (.tar.bz2).	R	
	MS Cabinet (.cab).	T	

<sup>26</sup> ISO/IEC 14496-14:2003 - Information Technology - Coding of audio-visual objects - Part 14: MP4 file Format.

<sup>27</sup> Musical Instrument Digital Interface, according to specification in *The Complete MIDI 1.0 Detailed Specification*. Version 96.1, 2.ed., Nov. 2001. Available at: <http://www.midi.org/aboutmidi/specinfo.shtml>. Access in May 30, 2007.

<sup>28</sup> Xiph.Org Foundation. Specification available at [http://xiph.org/vorbis/doc/Vorbis\\_I\\_spec.html](http://xiph.org/vorbis/doc/Vorbis_I_spec.html).

<sup>29</sup> 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.

Component	Specification	SIT	Observations
Geo-referenced information – standards for exchange of files between work stations	GML version 1.0 or superior <sup>30</sup> .	<b>A</b>	Indicated for complex vector structures, involving primitive geographic shapes such as polygons, dots, lines, surfaces, collections and numeric or textual attributes with no limit of number of characters.
	ShapeFile <sup>31</sup> .	<b>A</b>	Indicated for vector structures limited to lines, dots and polygons, whose textual attributes is not over 256 characters. It may also store M and Z dimensions.
	GeoTIFF <sup>32</sup>	<b>A</b>	Indicated for matrix structures limited to pixel matrices.
	SFS	<b>S</b>	
Extended programming (Plug-ins)	Subject to future consideration	<b>F</b>	

**8.3. Means of Access: Technical Specifications for tokens, Smart Cards and Cards in general**

Initial specifications about smart cards and tokens were added by conclusions of the ICP-Brazil Work Group (Decision no. 33, of April 8, 2003) which used as basic guidelines ISO/IEC family (7816 parts 1 to 6).

Conclusions of that group were also used for creating Handbooks of Technical Conducts of ITI, documents that establish technical requirements to be observed in the processes of homologation of smart cards and encrypted tokens in the scope of ICP-Brazil. Specifications pursuant in these handbooks were also used for confection of this reference document, especially for the cryptographic devices.

Homologation of systems and equipment of digital certification in the scope of ICP-Brazil was instituted by Resolution 36 of the ICP-Brazil Managing Committee, of Oct. 21, 2004, being the National Institute of Information Technology (ITI) responsible for conducting the process, while the Laboratories of Studies and Inspection (LEA), created by Resolution 36, were responsible for conformity reports.

According to that Resolution, media that store digital certificates and respective readers, besides systems and equipment necessary to digital certification, should obey to standards and minimum technical specifications, as to ensure its interoperability and reliability of security information resources used by them.

<sup>30</sup> *Geography Markup Language*. Specifications available at: <http://www.opengeospatial.org/standards>.

<sup>31</sup> *ESRI Shapefile Technical Description*. Available at: <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>.

<sup>32</sup> *GeoTIFF Format Especification*. Available at: <http://remotesensing.org/geotiff/geotiff.html> .

The regulation predicts homologation of medias as cryptographic tokens and smart cards, systems such as electronic signature, signature authentication, certifying and registering authorities, and equipment such as HSM, synchronism and time stamp, among others. Products homologated by this process will have a conformity report issued and will use the homologation stamp and its correspondent identification number.

It is important to note that the stored data in a specific smart card or token may not be protected by any kind of licensing that forbids its reading by any other software than that of the supplier of the smart card or token.

Normalization of these devices will facilitate Brazil's insertion in international agreements relating to digital certification, besides maintaining allegiance to Electronic Government Interoperability Standards – e-PING and helping to spread the use of certification, for among other aspects it may contribute for reducing costs of this technological solution.

In the context of e-PING, it was also considered: ISO/IEC 7810 which defines physical properties such as flexibility, resistance to temperature and dimensions to three different types of card format (ID-1, ID-2 and ID-3), the PC/SC Workgroup standard and standardization security of FIPS-140 devices, of the *National Institute of Standards and Technology* (<http://www.nist.gov>). These basic standards were used in ICP-Brazil Workgroup with the goal of obtaining better interoperability in the universe of access devices of smart cards and tokens type, devices that manage digital certificates. It was also incorporated to ISO rules for magnetic cards and optic cards, the former traditional and low-cost, the latter bolder and high-cost.

For future versions of e-PING, it will be established a minimum agenda that should review the whole set of specifications to map, in the scope of the federal government, and action and government plans that use some kind of smart cards and that, consequently, should be contemplated. An exhaustive consultation should be carried out in order to provide subsidies for inclusion or not in e-PING of the standards of cards effectively used by government bodies. As an example of this situation, it may be created the so-called *embossed smart cards* (ISO/IEC 7811), cards that are not contemplated in this version. In case it is found in this research the intensive use of such device, the viability of its inclusion in the set of e-PING's specifications will be assessed.

Still for future versions, it will be analyzed the standards typically aimed at the European community. It is the case of eEurope, the *Open Smart Card Infrastructure for Europe* – version 2, which assimilate contactless cards technology, constant in ISO/IEC 14443. The same is applied to CALYPSO standard (*Fourth European Research and Technological Development Framework Program*) for card (or tickets) systems, aimed at public transportation systems. It should be assessed standardizations, patent and licensing systems that might come to exist.

**Table 11 – Specifications for Means of Access – Smart cards, tokens and Cards in general**

Component	Specification	SIT	Applicable to	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study			
Data Definition	ITI Technical Consultations Handbooks – Volume 1 ( <a href="http://www.iea.gov.br/">http://www.iea.gov.br/</a> )	<b>A</b>	All token cards that handle with digital certificates.	
	ISO/IEC 7816-6 identification cards. Integrated Circuit Cards with contacts Part 6: Interindustry data elements for exchange	<b>A</b>	All.	According to ICP-Brazil WG choice
	ISO/IEC 7812-1 identification cards. Identification of emitters Part 1: Numbering System	<b>R</b>	All.	
	ISO 9992-2 Financial transaction cards Messages between the integrated circuit card and the card accepting Device Part 2: Functions, messages (commands and responses), data elements and structures	<b>F</b>	All.	
	Identification card systems BS EN 1546-3 – Inter-sector electronic purse. Part 3: Data elements and exchanges  Identification card systems BS EN 1546-4 - Inter-sector electronic purse. Part 4: Data objects	<b>F</b>	All.	Current edition was published on July 1999.  Current edition was published on August 1999.

Component	Specification	SIT	Applicable to	Observations
Applications including multi-applications	<p><b>ISO/IEC 7816-4</b> Identification cards. Integrated circuit(s) cards with contacts Part 4: Interindustry commands for exchange</p>	<b>A</b>	Integrated Circuit Cards with contacts	<p>Establishes files structures, ensure messages to access files, initialization of cards application, and logic channels for using when card can not have more than one active virtual communication channel. Specific application commands are not described, so that the standard treats command codes as specific applications when not defined in this part.</p> <p>According to ICP-Brazil WG choice. Current edition was published on June 1994. There is a ISO/IEC 7816-5/AM1 modification <i>Registered Application Provider Identifiers (RDIs)</i>, published on Dec. 1996.</p>
	<p><b>ISO/IEC 7816-5</b> Identification cards - Integrated circuit(s) cards with contacts Part 5: Numbering system and registration procedure for application.</p>	<b>R</b>		
	<p><b>ISO/IEC 7816-7</b> Part 7: Interindustry commands for Structured Card Query Language (SCQL);</p>	<b>R</b>		
	<p><b>ISO/IEC 7816-11</b> Part 11: structure of interindustry commands and data objects related to personal verification through biometric methods in integrated circuits</p>	<b>R</b>		
	<p><b>ISO/IEC 7813</b> Identification cards Financial transaction cards.</p>	<b>R</b>	Financial cards.	
	<p>Identification cards <b>ISO/IEC 7812-2</b> Identification of issuers Part 2: Application and registration procedures</p>	<b>R</b>	All.	
	<p><b>ISO/IEC 15693-4</b> Identification cards - Contactless integrated circuit( s) cards - Vicinity cards Part 4: Registration of Applications/ issuers</p>	<b>R</b>	Contactless Integrated Circuit Cards	
	<p><b>EN 1332-1:1999</b> Identification card systems - Man-machine interface – Part 1: Design principles for the user interface <b>EN 1332-4:1999</b> Identification card systems - Man-machine interface – Part 4: Coding of user requirements for people with special needs</p>	<b>R</b>	All.	
Electric	<p><b>ISO/IEC 7816-10</b> Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to</p>	<b>R</b>	Integrated Circuit Cards with contacts	

Component	Specification	SIT	Applicable to	Observations
	<p>reset for synchronous cards.</p> <p><b>ISO/IEC 7816-12</b> Part 12: Cards with Contacts - USB Electrical Interface</p>			
	<p><b>ISO/IEC 7813</b> Identification cards – Contactless integrated circuit(s) cards - Proximity cards</p> <p>Part 2: Radio frequency power and signal interface</p>	<b>R</b>	Proximity Integrated Circuit Cards	This part defines radio frequency interface and contains two very distinct modulation techniques (Types A and B) for data communication between card and terminal. Type A is based on Philips Mifare technology (widely licensed to other fabricants). Type B is a new concept. These two types are paralleled processes in this part of the standard and part 3. Besides, some specific items of Type A appear on part 4.
	<p><b>ISO/IEC 10536-3</b> Identification cards - Contactless integrated circuit(s) cards (Close Coupling Integrated Circuits Cards) CICC</p> <p>Part 3: Electronic signals and reset procedures</p>	<b>F</b>	Close coupling integrated circuit(s) cards	
	<p><b>ISO/IEC 15693-2.</b> Identification cards - Contactless integrated circuit(s) cards.</p> <p>Vicinity Integrated Circuits Cards (VICC).</p> <p>Part 2: Air interface and initialization;</p>	<b>R</b>	Vicinity integrated circuit(s) cards	
Communication protocols	<p><b>ISO/IEC 7816-3</b> Identification cards</p> <p>Part 3: Electronic signals and transmissions</p>	<b>R</b>	Integrated Circuit Cards with contacts	According to ICP-Brazil WG choice
	<p><b>ISO/IEC 14443-3</b> Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision</p> <p><b>ISO/IEC 14443-4</b> Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol.</p>	<b>R</b>	Contactless Integrated Circuit Cards	<p>This part continues duopoly of Types A and B, defining initialization and anticollision procedures of cards and basic communications protocols. Anticollision procedures are methods used for identifying and selecting a card when several cards are active in the terminal RF camp.</p> <p>This contains high level information (protocol message level of data transference, equivalent</p>

Component	Specification	SIT	Applicable to	Observations
				to protocol T=1 of ISO/IEC 7816, and is a bridge over ISO 7816-4. Only for Type A cards ISO/IEC 14443-4 includes a protocol initialization procedure.
	<b>ISO/IEC 15693-3</b> Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 3: Anticollision and transmission protocol	<b>R</b>	Contactless integrated circuit(s) cards.	
	<b>ISO 8583</b> Financial Transaction Card Originated Messages - Exchange message specification.	<b>F</b>	All.	
	<b>ISO 9992-1</b> Financial transaction cards - Messages between the integrated circuit card and the card accepting device - Part 1: Concepts and structures; ISO 9992-2  Part 2: Data functions, messages (commands and responses), elements and structures	<b>F</b>	All.	
	<b>ISO 10202-2</b> Financial transaction cards - Security architecture of financial transaction. systems using integrated circuit cards - Part 2: Transaction process; ISO 10202-6  Part 6: Cardholder verification.	<b>R</b>	All.	
	<b>ISO/ IEC 10536- 4</b> Identification cards - Contactless integrated circuit(s) cards (Close Coupling Integrated Circuit(s) Cards) CCIC Part 4: Answer to reset and transmission protocols	<b>F</b>	Close coupling integrated circuit(s) cards	

Component	Specification	SIT	Applicable to	Observations
Physic/physic and interface Standards cover card dimensions;  contact location and layout.	<b>Physical features</b> <b>ISO/IEC 7810</b> Identification Cards	R	All contact and combination cards	To ensure that they may be read in standard readers, all cards should follow ID-1 format as defined in this standard.
	<b>ISO/IEC 7811 Magnetic Card</b> , parts 2, 4 and 5: define properties, positioning and coding of card's magnetic band.	R	All magnetic band cards	
	<b>ISO/IEC 11693 and 11694 Optic memory card</b>	F	Optic cards	Cards that support storing lots of megabytes
	<b>ISO/IEC 7816-1</b> Identification cards Part 1: Physical characteristics <b>ISO/IEC 15693-1</b> Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -Part 1: Physical characteristics <b>ISO/IEC 7816-2</b> Identification cards - Integrated circuit cards. Part 2: Dimensions and location of the contacts	A	Integrated circuit(s) cards with contacts	This part supplements ISO/IEC 7810, establishing particular physical characteristics of IC cards with contacts. According GT choice of ICP-Brazil and ITI Technical Conducts Handbook – Volume 1
	<b>ISO/IEC 14443-1</b> Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics	R	Contactless integrated circuit(s) cards	This part supplements physical characteristics defined in ISO/IEC 7810.
	<b>ISO/IEC 15693-1</b> Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -Part 1: Physical characteristics. This part of <b>ISO/IEC 15693</b> was published in July 7, 2000.	R	Contactless integrated circuit(s) cards	This part was of <b>ISO/IEC 15693</b> was published on July 15, 2000.
	<b>ISO/IEC 10536-1</b> Identification cards - Contactless integrated circuit(s) cards - Close-coupled cards - Part 1: Physical characteristics; <b>ISO/IEC 10536-2</b> Part 2: Dimensions and location of coupling areas	F	Close coupling integrated circuit(s) cards	
	Tactile identifiers. <b>BS EN 1332-2</b> Identification Cards Systems Part 2: Dimensions and Location of a Tactile Identifier for ID-1 Cards	F	When embossing is not used and the user is asked to introduce his card in a specific way, a tactile identifier should be provided as support to visual disabilities.	Some card personalization equipment, unless modified, may have difficulty in processing cards with notch tactile identifiers. An agreement, therefore, should be made with the supplier of the personalization service for use of such cards.

Component	Specification	SIT	Applicable to	Observations
Security	<p><b>ISO/IEC 7816-8</b> Identification cards -- Integrated circuit(s) cards with contacts Part 8: Security related interindustry commands.</p> <p><b>ISO/IEC 7816-9</b> Part 9: Additional interindustry commands and security attributes.</p> <p><b>ISO/IEC 7816-11</b> Identification cards -- Integrated circuit cards - Part 11: Personal verification through biometric methods.</p> <p><b>ISO/IEC 7816-15</b> Identification Cards - Integrated Circuit Cards with Contacts - Part 15: Cryptographic Information Application in IC cards</p>	<b>A</b>	Integrated circuit(s) cards with contacts.	
	<p><b>ISO 10202</b> Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards: Part 1: Card life cycle; Part 2: Transaction process Part 3: Cryptographic key relationships Part 4: Security application module Part 5: Use of algorithms Part 6: Cardholder verification Part 7: Key management</p>	<b>F</b>	All.	
Terminal infrastructure	EN 1332-3:1999 Identification card systems - Man-machine interface - Part 3: Key pads	<b>R</b>	All.	
	<p>PC/SC Standards.</p> <p>Standards of the PC/SC Workgroup Systems Specification of Interoperability for ICCs and Personal Computer Part 1: Introduction and architecture overview. Part 2: Interface requirements for Compatible IC Cards and Readers. Part 3: Requirements for PC-Connected Interface Devices Part 4: IFD Design Considerations and Reference</p>	<b>A</b>	All.	For general use in PCs.

Component	Specification	SIT	Applicable to	Observations
	Design Information. Part 5 ICC Resource Manager, definition. Part 6: Service Provider Interface Definition. Part 7: Application Domain/Developer Design Considerations Part 8: Recommendations for ICC Security and Privacy Devices			
	ITI Handbook of Technical Conduct – Volume I.	A	Cards with capacity of managing digital certificates.	
	FIPS-140-2 Standard.	A	All.	According to item 1 of IGP-Brazil WG: follow at least the rules established for level 1 security of FIPS-140-2. Follow at least rules established for level 2 security for hardware violation assessment.
<b>Java Card®</b>	API ( <i>Application Programming Interface</i> ) for Java Card card platform.	A	This API defines a set of level from which Java Card technology based on applets may be built.	General version for Java Card technology is 2.2.1 (October 2003). <a href="http://java.sun.com/products/javacard/">http://java.sun.com/products/javacard/</a>
	Specification for a run time environment for Java Card platform.	A	This specification describes the required environment for running Java Card-based applets.	
	Specification for virtual machine for Java Card platform.	A	This specification defines the minimum requirement requested for the card virtual machine.	

## 9. Organization and Exchange of Information

### 9.1. Organization and Exchange of Information: Technical Policies

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 for definition of exchangeable data.
- 9.1.3. Use of XML for transformation of data.
- 9.1.4. Use of a metadata standard for management of electronic content.

### 9.2. Organization and Exchange of Information: Technical Specifications

**Table 12 – Specifications for Organization and Exchange of Information**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
Language for data exchange	XML (Extensible Markup Language) as defined by W3C <a href="http://www.w3.org/XML">http://www.w3.org/XML</a>	<b>R</b>	
Data transformation	XSL ( <i>Extensible Stylesheet Language</i> ) as defined by W3C <a href="http://www.w3.org/TR/xsl">http://www.w3.org/TR/xsl</a> XSL <i>Transformation</i> (XSLT) as defined by W3C <a href="http://www.w3.org/TR/xslt">http://www.w3.org/TR/xslt</a>	<b>R</b>	
Definition of exchangeable data	XML <i>Schema</i> as defined by W3C: - XML <i>Schema Part 0: Primer</i> <a href="http://www.w3.org/TR/2004/RECxmlschema-0-20041028/">http://www.w3.org/TR/2004/RECxmlschema-0-20041028/</a> - XML <i>Schema Part 1: Structures</i> <a href="http://www.w3.org/TR/xmlschema-1/structures">http://www.w3.org/TR/xmlschema-1/structures</a> - XML <i>Schema Part 2: Datatypes</i> <a href="http://www.w3.org/TR/xmlschema-2/datatypes">http://www.w3.org/TR/xmlschema-2/datatypes</a> UML ( <i>Unified Modeling Language</i> ) as defined by OMG <a href="http://www.omg.org/gettingstarted/specsandpr ods.html/">http://www.omg.org/gettingstarted/specsandpr ods.html/</a>	<b>R</b>	
Data description	RDF ( <i>Resource Description Framework</i> ) as defined by W3C.	<b>F</b>	
Elements of metadata for content management	e-PMG – Electronic Government Metadata Standard	<b>S</b>	
Browser taxonomy	LAG – Government Matters List. Version 1.0. As defined by <a href="http://www.eping.e.gov.br">http://www.eping.e.gov.br</a>	<b>A</b>	
Data definition	CPD – Data Standards Catalog, Version 1.0. According to definition in <a href="http://www.eping.e.gov.br">http://www.eping.e.gov.br</a>	<b>A</b>	

9.3. Notes about XML and Middleware

Not every system need to be able to communicate directly in XML, as represented in Image 5. When appropriate it is acceptable the use of middleware according to illustration of Image 6.

Although the following configurations present potential solutions, the direct XML model (Figure 5) is preferential, being possible the use of indirect models, presented in Image 6, in cases where there are reasons that justify its use.



Image 5 – Direct XML Model – Direct Exchange

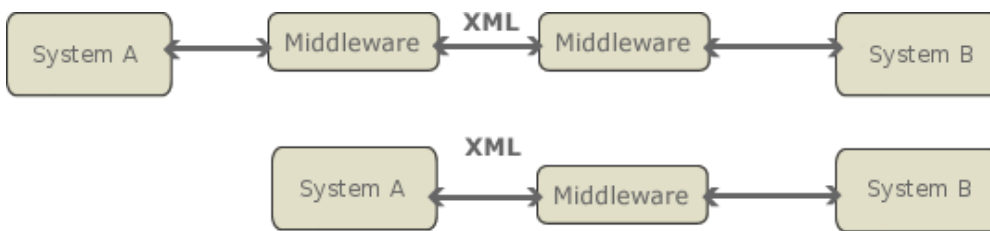


Image 6 – Exchange via middleware

## 10. Integration Areas for Electronic Government

### 10.1. Integration Areas for Electronic Government: Technical Policies

The segment guidelines are:

- Technical specifications under responsibility of the segment include:
  - XML Schemas related to applications aimed at Government Acting Areas, organized in a Catalog, available on e-PING's website and presented with updated contents in the following topic;
  - Components related to matters transversal to Government Acting Areas, whose standardization is relevant for interoperability of Electronic Government services, such as Geographical Processes and Information.
- Concerning XML *Schemas* referent to applications aimed at Government Acting Areas, the segment will act seeking identification, following of production and analysis of interest contents of the Public Administration, in articulation with groups that are representative of government and society, reporting to competent instances in what concerns prioritization;
- Technical specifications referent to XML *Schemas* constant in the Organization and Exchange of Information Segment should be respected by the proponents;
- From the understanding that materialization of the use of XML *Schemas* is given through interoperable services:
  - It is recommended that the Services Oriented Architecture (SOA) and technical policies related to the Interconnection Segment be observed in the project and implementation of applications based on referred XML *Schemas*;
  - The segment refers to the initiative "Referential Interoperation Architecture of Government Electronic Systems" which is a model of Architecture Oriented to Services, adapted to reality of Government Electronic Systems and can be accessed at <http://i3gov.cos.ufrj.br/igov/>;
  - There is strong interconnection between the Catalog of Data Standards and the Catalog of XML *Schemas* and, considering content specifications, it is aimed to keep general principles and compatible management mechanisms.

### 10.2. Integration Areas for Electronic Government: Notes about XML Schemas Catalog

#### 10.2.1. Initial Considerations

e-PING's architecture – Electronic Government Interoperability Standards – forecasts adoption of XML and the development of XML *Schemas* as bases for integration and electronic interoperability of the government. Thus, constitution of a repository that allow managers and planners of Electronic Government applications to consult consolidated XML *Schemas*, as well as propose cataloguing of schemes under its responsibility, has undeniable contribution to consolidate good interoperability practices in the governmental sphere.

#### 10.2.2. Objective

The Catalog has the goal of establishing XML *Schemas* standards that are applicable to interfaces of systems that support delivering of Electronic Government.

#### 10.2.3. Scope

The Catalog contains accepted standards in the form of XML *Schemas* for data exchange involving the public sector. Such patterns can be both a single scheme and a group of XML *Schemas*, if only the group refers to a same thematic inside the associated Integration Area.

Publication of XML *Schemas* does not automatically imply in warranty of access to correspondent contents or associated services, for which specific rules may be defined by the respective manager.

### 10.2.4. Property and Responsibility

e-PING's coordination is responsible for this Catalog, especially for the management of changing processes and for encouraging patterns to be used in future developments.

In this sense, it is recommended that the development or maintenance of systems that support delivering of Electronic Government services correlated to areas/sub-areas of government acting contemplated in the Catalog consider published XML *Schemas*.

Development and maintenance of this Catalog are responsibility of the Group Areas of Electronic Government Integration which has the participation of different government segments in federal and state spheres.

### 10.2.5. Management Mechanisms of the XML *Schemas* Catalog

Entries in the XML Catalog may take place through the following situations:

- a) Proposition followed by proposal acceptance for Data Standards Catalog (CPD);
- b) Submission followed by content proposal acceptance to Referential Interoperation Architecture of Government Electronic Systems (AR);
- c) Submission by professional linked to the public sector of content directly to the XML *Schemas* Catalog, through electronic formulary available on e-PING's website.

In the situations described on items (b) and (c) the contents will be sent to analysis by integrants of the Group Organization and Exchange of Information, thus evaluating pertinence of publishing associated Data Standard(s).

Proposition of XML *Schemas* logging will be submitted to analysis by integrants of the Group Integration Areas for Electronic Government through specific electronic formulary, available at e-PING's website ([www.e-ping.e.gov.br](http://www.e-ping.e.gov.br)). It will be kept in the Catalog only the accepted propositions, with the ones under study or already rejected, as well as previous versions of accepted XML *Schemas* being kept in a "work" environment to be opportunely conceived and implemented.

The evaluation criteria employed will include:

- Recognition by user community;
- Agreement with area/sub-area manager (in case he is not the proponent); and
- Adhesion to e-PING's standards.

That is, occurrence of submissions in which the proponent of a specific XML *Schemas* is not the foreseen area manager, but will have as additional acceptance condition the manager agreement, from talking carried out by the proponent and/or the Group Integration Areas for Electronic Government.

Solicitations of XML *Schemas* alteration already published will be preliminarily analyzed by integrants of the Group Integration Areas for Electronic Government. Acceptance will be up to the e-PING's Central Coordination, which may adopt the proposed changes according to its comprehension and impact or submit them to public consultation through the website <http://www.governoeletronico.gov.br>.

The initial Catalog infoset, presented below, was constituted by XML *Schemas* groups related to initiatives already mapped by integrants of the Group Integration Areas for Electronic Government. The goal of publishing these contents is to give visibility to cases of effective use of XML *Schemas* by the Federal Public Administration and partner bodies.

Consolidated contents in the initial infoset and the updates may be checked at e-PING's page ([www.e-ping.e.gov.br](http://www.e-ping.e.gov.br))

#### 10.2.6. XML Schemas Information set

Each XML *Schema*, or grouping of correlated XML *Schemas*, should be documented according to the following information set:

**PROPONENT ORGAN:** Name of superior Organ proponent of XML *Schema*. Ex.: Ministry of Agriculture, Ministry of Education, Ministry of Environment etc;

**RESPONSIBLE:** Name of professional responsible for XML *Schema* proposition;

**CPF:** CPF (Tax Payer Number) of the professional responsible for XML *Schema* proposition;

**LOTATION UNIT:** Lotation Unit of the responsible for logging. Proposal. Indicate the sequence of units up to the superior Organ, for example, GIS/DSI/SLTI/MP;

**E-MAIL:** Electronic address of the professional responsible for XML *Schema* proposition;

**TELEPHONE 1:** Telephone contact number of the professional responsible for XML *Schema* proposition;

**TELEPHONE 2:** Alternative Telephone contact number of the professional responsible for XML *Schema* proposition. Optional filling;

**MANAGEMENT INDICATOR:** Indication of proponent situation in regard to management of area/sub-area to which XML *Schema* refers to. It must be filled through signaling one of two options (“yes” or “no”).

**MANAGEMENT ORGAN:** The organ with attributions to manage the area/sub-area to which XML *Schema* refers to. It must be filled only when management indicator is “no” and the management organ is known to the proponent;

**NAME OF XML SCHEMA:** Usual denomination of grouping or of the only XML *Schema* that is supposed to be cataloged;

**VERSION:** XML *Schema* version that will be used.

**XML SCHEMA URL:** URL in which XSD file will be found (Definition of XML *Schema*) and detailed information about the (group of) XML *Schema*;

**DESCRIPTION:** Brief description about the (group of) XML *Schema*. And considerations that the proponent may find pertinent;

**SUB-AREA:** Usual denomination inside the government acting area to which the group of XML *Schema* refers to, should be informed only when the area is not enough to qualify the thematic contemplated by XML *Schema*;

**XML SCHEMAS COMPONENTS:** Name of XML *Schemas* that are part of the one being logged.

#### 10.2.7. Classification of XML Schemas Catalog

The XML *Schema* Catalog will be organized by Thematic Areas of Government Action, in which it XML *Schema* will be related according to first level classification given by the List of Government Acting Areas, which has as reference the Pluriannual Plan (PPA), and is presented below:

List of Government Acting Areas, based on Pluriannual Plan – PPA:

1. Social Assistance;
2. Health care;
3. Public Safety;
4. Education;
5. Administration;
6. Tributary Administration;
7. Habitation;
8. Science and Technology;
9. Trade and Services;
10. Foreign Affairs;
11. National Defense;
12. Special Charges;

- 13. Culture;
- 14. Environment Management;
- 15. Social Security;
- 16. Work;
- 17. Transport;
- 18. Energy;
- 19. Agriculture;
- 20. Agrarian Organization;
- 21. Communications;
- 22. Judiciary;
- 23. Legislative;
- 24. Essential to Justice;
- 25. Citizenship Rights;
- 26. Sport and Leisure;
- 27. Industry;
- 28. Sanitation;
- 29. Urbanism.

The electronic version of XML *Schemas* catalog will provide, as an option of alternative search to classification by List of Government Acting Areas, an alphabetic list of XML *Schemas* catalogued.

**10.3. Integration Areas for Electronic Government: Technical Specifications**

Specifications for the Integration Areas for Electronic Government are:

**Table 13 – Specifications for Integration Areas for Electronic Government – Transversal Topics to Government Acting Areas**

Component	Specification	SIT	Observations
	A = Adopted R = Recommended T = In Transition S = In Study F = Future Study		
PROCESSES – Language for Running Processes	BPEL4WS V1.1, as defined by OASIS <a href="http://www.oasisopen.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf">http://www.oasisopen.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf</a>	R	
PROCESSES – Process Modeling Noting	BPMN 1.0, as defined by OMG <a href="http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf">http://www.bpmn.org/Documents/OMG%20Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf</a>	R	
GEOREFERENCED INFORMATION – Interoperability between geographic information system	WMS version 1.0 or latter <a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>	A	
	WFS version 1.0 or latter <a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>	A	
	WCS version 1.0 or latter <a href="http://www.opengeospatial.org/standards">http://www.opengeospatial.org/standards</a>	A	
	CAT	S	
	WFS-T	S	

**Table 14 – Specifications for Integration Areas for Electronic Government – Catalog of XML Schemas referent to Government Acting Areas**

Component	Specification	Observations
ADMINISTRATI ON – Governmental Purchases	<a href="https://www.comprasnet.gov.br/xml/aviso.xsd">https://www.comprasnet.gov.br/xml/aviso.xsd</a> <a href="https://www.comprasnet.gov.br/xml/consultamatserv.xsd">https://www.comprasnet.gov.br/xml/consultamatserv.xsd</a> <a href="https://www.comprasnet.gov.br/xml/dispinex.xsd">https://www.comprasnet.gov.br/xml/dispinex.xsd</a> <a href="https://www.comprasnet.gov.br/xml/contratoent.xsd">https://www.comprasnet.gov.br/xml/contratoent.xsd</a> <a href="https://www.comprasnet.gov.br/xml/empenho.xsd">https://www.comprasnet.gov.br/xml/empenho.xsd</a> <a href="https://www.comprasnet.gov.br/xml/resultado.xsd">https://www.comprasnet.gov.br/xml/resultado.xsd</a>	ComprasNet system XML Schemas referent to Ending of Biding, Performance, Exemption/ Non-obligation of Public Biding, Material Consultation via CATMAT, Contract of non-SISG entities and Biding Notice.
ADMINISTRATI ON – Government Structures	<a href="http://guialivre.governoeletronico.gov.br/igov/">http://guialivre.governoeletronico.gov.br/igov/</a>	Group of XML Schemas related to administrative management systems of the Federal Public Administration.
ADMINISTRATI ON – Management of Local Networks/ CACIC	<a href="http://guialivre.governoeletronico.gov.br/cacic/isp2/invent/Invent.html">http://guialivre.governoeletronico.gov.br/cacic/isp2/invent/Invent.html</a>	These Schemas are part of CACIC solution, developed by Dataprev, and are used for transmission of data of hardware inventory and its connected components in a network environment. Implementation of these Schemas occurred in partnership with the Ministry of Environment (MMA).
TRIBUTARY ADMINISTRATI ON – Electronic Invoice	<a href="http://200.198.224.29/portal/info/Schemas.htm">http://200.198.224.29/portal/info/Schemas.htm</a>	Schema XML used for issuing of electronic invoice, substituting paper and judicially legal. This project is coordinated by the National Meeting of State Fiscal Managers and Coordinators (ENCAT) and developed jointly with the Federal Tax Office.
CITIZENSHIP RIGHTS – Registry Offices	<a href="http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd">http://www.mj.gov.br/Schemas/Cartorio/ConsultaCartorio.xsd</a>	It is up to the Ministry of Justice to keep the National Registry Offices Log. This scheme, counting on a filter generated by the state and/or municipality and/or neighborhood and/or office's attribution, consults the Brazilian registry offices log, developing a list of offices that are part of the filter. The scheme allows, still, to deliver details of each listed registry office.
CITIZENSHIP RIGHTS – Customer Defense	<a href="http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd">http://www.mj.gov.br/Schemas/DireitoConsumidor/SINDEC.xsd</a>	This scheme allows consultation to consolidated statistics about delivering in "Procons" registered in the National System of Information and Customer

Component	Specification	Observations
		<p>Defense (SINDEC) by state or name of supplier or CNPJ, giving service statistics of the researched criteria.</p>
<p>CITIZENSHIP RIGHTS – Customer Defense</p>	<p><a href="http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd">http://www.mj.gov.br/Schemas/Recall/ConsultaRecall.xsd</a></p>	<p>It is up to the Ministry of Justice to formulate, promote, supervise and coordinate the economical order protection policy, in the areas of competition and consumer defense. The procedure by which the supplier informs the public about defects detected on products and services that he had delivered is called recall. Essential goals of this kind of procedure are protecting and preserving customers, as well as avoiding or minimizing any kind of damage, be it material, be it moral. This scheme allows consultation to the recall databank of the Department of Customer Defense and Protection as to check if a given product is being subject to recall. For that, the scheme returns to the suppliers/models list that made recall, allowing to verify recall details from the choice of product or series number, chassi, lot, among others.</p>
<p>CITIZENSHIP RIGHTS</p>	<p><a href="http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd">http://www.mj.gov.br/Schemas/ClassificacaoIndicativa/ConsultaClassindFilmes.xsd</a></p>	<p>It is up to the Ministry of Justice to exert classification, with indicative purpose, of public leisure activities and radio and television programs. From the name of the movie or program, this scheme consults the Indicative Classification databank and returns a list of coincident names for which details and justification of the indicative classification will be exhibited.</p>
<p>ENVIRONMENTAL MANAGEMENT – Environmental Licensing/PNLA</p>	<p><a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_completo.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_completo.xsd</a></p> <p><a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_simples.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_simples.xsd</a></p> <p><a href="http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_totalizadores.xsd">http://integradorpnla.mma.gov.br/integrador/schemas/licenciamento_ambiental_totalizadores.xsd</a></p>	<p>The <i>Schemas</i> are applied to environmental licensing and are adopted by the platform of the National Environment Licensing Gate (PNLA) of MMA which consolidate information about environmental licenses of several states through Web Services.</p> <p>Bellow is a description of the purpose of each scheme:</p>

Component	Specification	Observations
		<ul style="list-style-type: none"> <li>• Licenciamento_ambiental_simples.xsd – offers the scheme for development of a report containing a group of licenses with minimum data of its identification. It is useful for preliminary browsing about licenses for a subsequent detailing that is done through the first scheme;</li> <li>• Licenciamento_ambiental_totalizadores.xsd – consolidates the quantitative of licenses based on an arbitrary topic.</li> </ul>
<p>JUDICIARY – Services of Extrajudicial Registry Offices</p>	<p><a href="http://www.anoregsp.org.br/arquivos">www.anoregsp.org.br/arquivos</a></p>	<p>The XML <i>Schemas</i> refer to standardization of consultations to extrajudicial registry offices services.</p>

## 11. Glossary of Abbreviations and Technical Terms<sup>33</sup>

On this item will be presented the meaning of the main technical terms used on e-PING.

**ABNT – Brazilian Technical Standards Association:** publishes rules that pose as guidelines to preparation and compilation of references of material used for making documents and for inclusion of bibliography, summaries, reviews and others.

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

**APF – Federal Public Administration:** unites bodies of the direct (integrated services in the administrative structure of the Presidency of the Republic and Ministries) and indirect (Autarchies, Public Enterprises, Mix Economy Societies and Public Foundations) administration of the Executive Power. [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del0200.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm).

**BPM – Business Process Management:** Vision of business processes of an organization such as service flows using standards of presentation of notation, execution and coordination in XML, whose semantic stiffness allows its interoperability among different platform systems, being thus a fundament for implementation of solutions based on service-oriented architecture. When coordination of services execution is done with subordination to a master process, normally intra-organization, such coordination is named Orchestration. When coordination occurs without subordination to a master process, usually inter-organization, it is name Choreography.

**Browser:** Web browser – A client application that allows users to visualize contents of the World Wide Web in other network or in the user's computer, following hypertext links and transfer files.

**XML Schemas Catalog:** information directory about XML *Schemas*.

**Cryptography:** Technique of Information protection that consists in encrypting a message's or signal's content, transforming it into an illegible text, through complex mathematical algorithms.

**CAT – Catalog Service Implementation Specification:** *OpenGIS* specification that defines interfaces to publish, access, navigate and consult metadata about geo-referenced information. Currently most used term for Catalog Service is CSW.

**CSW – Catalog Service Implementation Specification:** *OpenGIS* specification that defines interfaces to publish, access, navigate and consult metadata about geo-referenced information.

**Device:** physical component (work station, mobile phone, smart card, hand-held, digital television with access to the internet).

**DNS – Domain Name System:** form in which domain names are found and translated in the internet protocol address. A domain name is a easy resource to remember when referenced as an Internet address.

**FTP – File Transfer Protocol:** is an application protocol that uses TCP/IP Internet protocols, being the easiest way to exchange files between computers in the internet.

**GML – Geography Markup Language:** *OpenGIS* specification XML-based developed to allow transport and storing of geographical/spatial information.

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

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

**Hashing:** is the transformation of a character chain in a fixed-sized value usually lower or in a key that represents the original chain. It is used to index and recovery items in a databank, because it is

<sup>33</sup> Microsoft Press. Dicionário de informática. Translator and editorial advisor: Fernando Barcellos Ximenes - KPMG Peat Marwick. Editora Campos Ltda, 1993. ISBN 85-7001-748-0.

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

faster to find the item using the lower transformed key than the original value. It is also used in cryptography algorithms.

**HELO:** parameters that limit delivering of non-solicited commercial e-mail. <http://www.postfix.org/uce.html>.

**HTTP – Hyper Text Transfer Protocol:** set of rules for file exchange (texts, graphics, sound, videos and other multimedia files) on the World Wide Web.

**HTTPS – Secure Hyper Text Transfer Protocol:** web protocol developed by Netscape and coupled to the browser. Cryptographs and analyze solicitations and returns of returned pages through web server. HTTPS is simply the use of Netscape SSL (Secure Sockets Layer) as a sub-layer under normal organization of programs for HTTP applications.

**ICP-Brazil:** set of techniques, practices and procedures to be implemented by Brazilian governmental and private organizations aiming to establish the technical and methodological fundamentals of a digital certification system based on a public key. <http://www.icpbrasil.gov.br>.

**IEEE – Institute of Electrical and Electronic Engineers:** foments development of standards and rules that usually become national and international accepted.

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

**IMAP – Internet Message Access Protocol:** standard protocol for accessing e-mail from a local server. IMAP is a client-server protocol in which the e-mail is delivered and stored by the internet server.

**IP – Internet Protocol:** method or protocol through which data are sent from a computer to another on the internet. Each computer, on the internet, has at least one IP address that identifies it uniquely in relation to all other internet computers.

**IPSec – Internet Protocol Security:** development standard relative to security in the network layer or in network communication parcels processing. A great advantage of IPSec is that security topics may be manipulated with no need of changes in the individual users' computers. IPSec offers two options of security services: Authentication Header (AH), which essentially allows identification of the data sender, and Encapsulating Security Payload (ESP), which supports both identification of sender and encrypting of data.

**IPv4 – Internet Protocol Version 4:** see “IPv6”.

**IPv6 – Internet Protocol Version 6:** Last level of IP, currently already included as part of support IP in many products, including main computer operational systems. Formally, IPv6 is a set of IETF specifications. IPv6 was projected as an evolving set of improvements done to IPv4. The most significant improvement of IPv6 in regard to IPv4 is that IP addresses are raised from 32 bits to 128 bits.

**LAN – Local Area Network:** group of associated computers and devices that share one same line of communication and normally the resources of a single processor or server in a small geographical area. Normally, the server has applications and data storing shared by several users in different computers.

**LDAP – Lightweight Directory Access Protocol:** software protocol for allowing localization of organizations, people and other resources such as files and devices in a network, be it the public internet or a corporative intranet.

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

**Instant Message:** Is a type of communication that allows a user to change messages in real time with another user also connected to the web.

**Metadata:** additional information necessary to make data useful. It is the essential information for use of data. In summary, metadata are a group of characteristics about data that are not normally included in data properly said. <http://www.isa.utl.pt/dm/sig/sig20002001/TemaMetadados/trabalho.htm>.

**Middleware:** is a general term that is used to mediate two separate and usually already existing programs.

**Newsgroup:** discussion about a specific subject, consisting of messages sent to a central internet

website and redistributed by Usenet, a global network of groups of news discussion. Users can send messages to existing news groups, answer to previous messages and create more news groups.

**OGC – Open Geospatial Consortium:** it has the mission to “develop specifications for spatial interfaces that will be made available for general use”.

**OWS – OGC Web Services:** refers to all OpenGIS specifications that apply geoprocessing through the Web.

**Open standard:** the whole technological standard established by international bodies or companies clusters that develop specifications which are found public available. The PC (personal computer) was launched and is developed as an open standard. Internet specifications and its development, too.

**Metadata standard:** a group of metadata is a standard, defined by a community of users which includes a vocabulary of descriptive elements and a scheme or rules of codification of these elements in a way that is computer readable. <http://www.uff.br/gdo/htm/tsld013.htm>.

**Plug-in:** Supporting program that adds capacities to the main program. Usually, in web applications, they are programs that may 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 shown.

**POP3 – Post Office Protocol 3:** latest version of the standard protocol to recovery e-mails. POP3 is a client/server protocol in which the e-mail is received and stored by the internet server.

**Portal:** Website that aggregates services, news and great volume of informative content and/or entertainment.

**Government Network:** is the entrance portal for every page of the federal government over the internet. [http://www.federativo.bndes.gov.br/destaques/egov/egov\\_redegoverno.htm](http://www.federativo.bndes.gov.br/destaques/egov/egov_redegoverno.htm).

**Resolution no. 7 of the Electronic Government:** establishes rules and guidelines for internet websites of the Federal Public Administration (gov.br and mil.br). Divided in 7 chapters, the resolution is about the information structure, control and monitoring, management of interactive elements, organizational model, visual identity and security of governmental sites over the computers world network. <http://www.governoeletronico.e.gov.br>.

**RFC – Request for Comments:** formal document of IETF, resulting of models and reviews from stakeholders. The final RFC version is a standard in which neither commentaries nor alterations are allowed. Alterations may occur, however, through subsequent RFCs that substitute or elaborate over all parts of previous RFCs. RFC is also an abbreviation for Remote Function Call.

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

Electronic Government Services (related topics Services of Electronic Government, Electronic Services):

Electronic government may be defined by the use of technology to increase access and improve supplying of government services to citizens, suppliers and servers. In general lines, the characteristic functions of the electronic government are:

1. Electronic delivering of information and services.
2. Regulation of information networks, mainly involving governance, certification and taxing.
3. Accountability of public expenditure, transparency and monitoring of budget execution.
4. Long-distance education, digital alphabetization and maintenance of virtual libraries.
5. Cultural diffusion with emphasis on local identities, fostering and preservation of local cultures.
6. e-procurement, that is, acquisition of goods and services through the internet, like electronic public biddings, electronic auctions, markets of virtual public purchases and other types of digital markets for goods purchased by the government.
7. Encouragement to e-business, through creation of safe transactions environment, especially for small and medium-sized companies. <http://www.governoeletronico.gov.br/r1>.

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

- Government management: Planning, Budget, Budget Execution, Finance Administration, Human Resources Administration, General Services Administration, Management of Documentation and Information, Administrative Organization and Modernization, Information and Informatics Resources and Internal Control;
- Final government acting: activities of the various bodies of governmental framework, like infrastructure (transport, communications, energy, natural resources administration). Agriculture, Health, Education, etc.

Reference: [http://www.redegoverno.gov.br/projetos/reg\\_gestao.asp](http://www.redegoverno.gov.br/projetos/reg_gestao.asp).

**SFS – Simple Features Specifications for SQL:** OpenGIS specification that defines standardization of the SQL scheme that supports storing, recovering, consultation and updating about geo-referenced information.

**Smart Cards:** plastic cards, with approximately the size of a credit card, with an imbedded microchip that may be filled with data, may be used for phone calls, electronic payment in cash or other applications. It is periodically updated to receive additional functions.

**S/MIME – Secure Multi-Purpose Internet Mail Extensions:** safe method for sending e-mail that uses RSA (Rivest-Shamir-Adleman) encrypting system. S/MIME describes how 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 e-mails. MIME is an extension of internet e-mail protocol that allows exchanging different kinds of data files through internet.

**SOA – Service Oriented Architecture:** Architecture proposed for interoperability of systems through a set of services interfaces loosely coupled, where services do not need technical details of platform of other services for performing information exchange.

**SOAP – Simple Object Access Protocol:** describes a model for packing of XML inquiries and answers. Sending of SOAP messages is used to allow exchange of a variety of XML information. SOAP norm assumes the task of transmitting inquiries and answers about services between service users and suppliers.

**Free Software:** computer program available through its font-code and with permission for anyone to use it, copy it or distribute it, be it in its original form or with modifications, be it freely or with costs. Free software is necessarily non-appropriated, but it is important to not confuse free software with freeware.

**SPAM:** non-solicited internet e-mail. From the sender's view, this is a form of mass message, generally to a separate list of people signed in a discussion group Usenet or obtained by companies specialist in creating e-mail distribution lists. For the recipient, spam is usually considered trash.

**SSL – Secure Sockets Layer:** is a protocol commonly used to manage security of an internet message sending.

**Browser Taxonomy:** is a controlled vocabulary of terms and phrases, hierarchically organized and structures, according to natural or presumed relations, aiming to facilitate to users of websites and internet portals the finding of information through browsing.

**TCP – Transmission Control Protocol:** set of rules used with IP to send data in form of message units between internet computers. While IP deals with the real delivery of data, TCP controls individual data units in which a message is divided for efficient internet routing.

**Telnet:** way for accessing someone else's computer, assuming that permission was given. More technically, Telnet is a user command and a concealed TCP/IP protocol for accessing remote computers.

**TLS – Transport Layer Security:** protocol that guarantees privacy for communication applications and internet users. When server and user communicate, TLS guarantees that no other part may assess or intercept the message.

**Token:** structured data object or a message that continuously circulates among the knots of a token ring network and describes the current state of the network.

**UDDI – Universal Description Discovery and Integration:** is a repository in which developers register available Web Services that allow clients to find and use services allocated on Extranets

and Intranets.

**UDP – User Datagram Protocol:** communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to TCP and, with IP, is referred as UDP/IP. Just as TCP, UDP uses IP to take a data unit from a computer to another. Differently from TCP, UDP does not offer the service of splitting a message in packs and ensemble it in the other extremity. UDP does not offer the sequence of packs in which the data arrive. This means that the application program that uses UDP should ensure that the whole message arrived and is ok. Network applications that want to spare processing time because they have very small data units for exchanging may prefer UDP instead of TCP.

**UML – Unified Modeling Language:** UML is much more than standardization of a notation, that is, it is a standard-language for elaboration of software projects structure, including conceptual aspects such as business processes and system functions, besides concrete items such as written classes in a given programming language, schemes of databanks and components of reusable software. UML may be employed for visualization, specification, construction and documentation of artifacts of software systems, and also for modeling of business and other types of systems that not just software.

**URI – Uniform Resource Identifier:** codification standard of internet names and addresses. A URI is composed of a name (ex.: file, http, ftp, news, mailto, gopher), followed by a column and a path, standardized by a list of schemes that follow RFC 1630. URI encompass URNs and URLs concepts.

**Usenet:** collection of notes and messages submitted by users about several subjects that are sent to servers in a world network. Each collection of notes sent is known as a newsgroup.

**VPN – Virtual Private Networks:** Private Networks that uses infrastructure of a public telecommunications network, such as the internet, for example, for transmission of confidential information. Data sent are encrypted. Its implementation occurs through virtual tunnels, through which information goes, protecting them from access of unauthorized users.

**W3C – World Wide Web Consortium:** association of industries that aims to promote standards for evolution of web and interoperability among products for WWW, producing specification and reference software.

**WAN – Wide Area Network:** Network of computers that encompass extensive geographical area such as a state, a country or a continent.

**WCS – Web Coverage Service Implementation Specification:** OpenGIS specification that defines interfaces for accessing and manipulating operations (GetCapabilities, DescribeCoverage and GetCoverage) about geo-referenced information in the Coverage format.

**Web Services:** Logical and programmable application that create compatibilities among very different applications, independently of operational service, allowing communication and data exchange between different networks.

**WFS – Web Feature Service Implementation Specification:** OpenGIS specification that defines interfaces for accessing and manipulating operations (GetCapabilities, DescribeFeatureType, GetFeature, Transaction and LockFeature) over geo-referenced information, through HTTP protocol. Based on these operations, two classes of service may be defined:

- Basic WFS (WFS): is capable of implementing only operations: GetCapabilities, DescribeFeatureType and GetFeature. Because of that, it is considered a reading WMS service
- Transactional WFS (WFS-T): is capable of implementing all operations of a basic WFS and transactional operations. Optionally, it could also implement LockFeature operation.

**WMS – Web Map Service Implementation Specification:** OpenGIS specification that defines interfaces for accessing and manipulating operations (GetCapabilities, GetMap and GetFeatureInfo) about multiple layers and geo-referenced information, containing vectors and/or images.

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

**XML – eXtensible Markup Language:** flexible way of creating formats of common information and

sharing both formats and data over the World Wide Web, intranets and anywhere else. XML is extensible because, differently from HTML, markup symbols are limited and self-defined.

**XML Schemas:** XML documents, also found on an internet site, which specify the structure, number of occurrences of each element, allowed values, units, etc., that is, document's syntax. Schemas of a XML set of documents are public available on an internet site, so that programs may have access to them in order to validate 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 messages.

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

**XSLT – eXtensible Stylesheet Language transformations:** standard way of describing how to change the structure of a XML document into another XML document with other structure. XSLT may be thought as a XSL extension. XSLT shows how the XSL documents should be re-organized in another structure of data (that may be presented following a XSL spread sheet).

## 12. Integrants

### e-PING's coordination

Brazilian Association of Data Processing State Enterprises (Associação Brasileira de Empresas Estaduais de Processamento de Dados - ABEP)

Dayse Vianna  
Paulo Cezar Coelho

Bank of Brazil (Banco do Brasil - BB)

Ulisses de Sousa Penna

Data Processing Federal Service (Serviço Federal de Processamento de Dados - SERPRO)

Antônio Sérgio Borba Cangiano  
Elói Juniti Yamaoka  
Geancarlo Noronha Vinhal  
Paulo Cezar Czarnewski  
Wagner Junqueira Araújo

Federal Savings Bank (Caixa Econômica Federal - CAIXA)

Ângela B. Baylo

Ministry of External Relation (Ministério das Relações Exteriores - MRE)

Celso Ricardo Hottum Meira

Ministry of Health (Ministério da Saúde - MS)

Eliane Pereira dos Santos  
Ernani Bento Bandarra  
Márcia Helena Gonçalves Rollemberg

Ministry of Planning, Budget and Management – Office of Logistics and Information Technology (Ministério do Planejamento, Orçamento e Gestão – Secretaria de Logística e Tecnologia da Informação - MP/SLTI)

Leandro Corte (Coordinator Geral)  
Ednylton Maria Franzosi  
Eduardo Favero  
José Ney de Oliveira Lima  
Leonardo Boselli da Motta  
Leonardo Lanna Guillén  
Nazaré Lopes Bretas  
Rogério Santanna dos Santos  
Sylmara Campos Pinho Garcia

Presidency of the Republic (Presidência da República - PR)

Marcelo André de Barros Oliveira

Presidency of the Republic – National Institute of Information Technology (Presidência da República – Instituto Nacional de Tecnologia da Informação - ITI)

Mauricio Augusto Coelho  
Renato da Silveira Martini  
Viviane Regina Lemos Bertol

Social Security Company of Technology and Information (Empresa de Tecnologia e Informações da Previdência Social - DATAPREV)

Humberto Degrazia Campedelli  
José Antônio Borba Soares  
Rodrigo Novais Coutinho  
Ministério da Justiça (MJ)  
Jorilson da Silva Rodrigues

## Workgroup Interconnection

Leonardo Lanna Guillén (MP/SLTI) - Coordinator  
Adriano Soriano (CAIXA)  
Areno Pires Filho (MC)  
Carlos Bellone Neto (RFB)  
Daniel Moreira Guilhon (CGU)  
Filipe Guimarães (MRE)  
José Rodrigues Gonçalves Júnior (ITI)  
Júlio César Japiassu Lyra (MJ)  
Leonardo Boselli da Motta (MP/SLTI)  
Luciene Pinheiro Capra (ANS)  
Odilon de Freitas Militão Neto (CAIXA)  
Paulo Guilherme Lanzillotti Jannuzzi (DATAPREV)  
Ruben César Macedo (CELEPAR-PR)  
Sérgio de Oliveira Barcellos (MCT)  
Sílvia Aparecida da Cunha (MP/CGTI)  
Ulisses de Sousa Penna (BB)

### Subgroup: *Web Services*

Ednylton Maria Franzosi (MP/SLTI) – Coordinator  
Bruno Pacheco (SERPRO)  
Carlos Falcão Maranhão (MS/ANS)  
Cláudio Muniz Machado (MS)  
Elaine Fabiano Tocantins (MJ)  
Louise Neves (SERPRO)  
Mauricio Dayrell (MMA)  
Paulo Azevedo (BB)

### Collaborators

Claudia do Socorro Ferreira Mesquita (MP/SLTI)  
Patrycia Barros de Lima Klaydianos (MP/SLTI)

## Workgroup Security

Jorilson da Silva Rodrigues (MJ) – Coordinator  
Alessandra Silva Moura(ANS)  
Dante de Matos Gomes(PRODEB)  
Edgar Luciano Moraes Martins (MP/SLTI)  
Érica Dantas (STJ)  
Filipe Carneiro Guimarães (MRE)  
Gleyner Martins Novais (SERPRO)  
Humberto Degrazia Campedelli (DATAPREV)  
Igor Guimarães (MC)  
José D'Aleluia Nascimento (MinC)  
José Maria Leocádio (SERPRO)  
Júlio César de Magalhães (FNDE)  
Luiz Augusto Barbosa Mozzer (CGU)  
Maisa Netto Ludemer (MC)  
Marcelo Henrique Rios dos Reis (MT)  
Marco Antônio Reis Henriques (RFB)  
Marcos José Cândido Euzébio (BACEN)  
Ricardo Luiz Chiacchio (MCidades)  
Roberto dos Santos Rodrigues (MCT)  
Rodrigo Costa dos Santos (ELETROBRÁS)  
Sérgio Carreira dos Santos (IPHAN)

### Workgroup Means of Access

Mauricio Augusto Coelho (ITI) – Coordinator  
Renato da Silveira Martini (ITI) – Coordinator  
Carlos Bellone Neto (RFB)  
Cleisson Rodrigues (MTur)  
Eduardo Viola (MCT)  
Eliane Aristóteles Moreira (DATAPREV)  
Eliane Pereira dos Santos (MS)  
Ellio Alves de O. Soares (CEF)  
Geancarlo Noronha Vinha (SERPRO)  
Hilton P. Mendes Sobrinho (MS)  
Jean Carlo Rodrigues (ITI)  
Paloma Nascimento (MT)  
Paulo Édison de Souza (MEC)  
Rosane dos Santos Lourenço (MT)  
Rubem César Macedo (CELEPAR-PR)  
Thimoteo Borges (CGU)  
Viviane Regina Lemos Bertol (ITI)

### Workgroup Organization and Exchange of Information

Eloi Juniti Yamaoka (SERPRO) – Coordinator  
Aline Ramalho Bezerra (MJ)  
Ana Lúcia de Medeiros (CORREIOS)  
Ângela B. Baylo (CAIXA)  
Aurélia Dolores Gonçalves Bruner (ELETROBRAS)  
Beatriz Barreto Brasileiro Lanza (CELEPAR)  
Brenda Couto de Brito Rocco (AN-CC)  
Cláudia Carvalho Masset Lacombe Rocha (AN-CC)  
Dalva Clementina Luca (MJ)  
Dayse Vianna (PRODERJ)  
Dilma de Fátima Avellar Cabral da Costa (AN-CC)  
Eliane Pereira dos Santos (MS)  
Elizabeth da Silva Maçulo (AN-CC)  
Fernanda Hoffmann Lobato (MP/SLTI)  
Geny Conte Pessoa (SERPRO)  
Hilda Pimentel (ANCINE)  
João Alberto Lima (Senado Federal)  
Ligia Leindorf Bartz Kraemer (UFPR)  
Luciana Ferreira Pinto da Silva (INEP)  
Luciano Seite Nishikawa (CAIXA)  
Marcia Helena Gonçalves Rollemberg (MS)  
Márcia Izabel Fugizawa Souza (EMBRAPA)  
Márcia Luzia Albertini (MS)  
Márcio Imamura (IBGE)  
Marcos Augusto Francisco Borges (CPqD)  
Margareth da Silva (AN-CC)  
Maria de Fátima Porcaro (IPT)  
Maria do Socorro Rodrigo de Medeiros (INEP)  
Maria Valéria Lins Tenório (ATI-PE)  
Neuza Arantes Silva (MAPA)  
Paulo César Pereira Soares (FUNARTE)  
Paulo Cezar Czarnewski (SERPRO)  
Ricardo Torres Lenzi (INEP)  
Rosiane Fonseca (ANCINE)  
Samuel Batista dos Santos (IPT)  
Sérgio Silva dos Santos (MAPA)  
Siomara Zgiet (MS)

Taciano Tres (BB)  
Vicente de Paula Teixeira (CGU)  
Virgilio Dantas Lins Filho (ME)  
Vivianne Muniz Veras Barrozo (SERPRO)  
Wilson Yociteru Yamaji (AGU)

### **Workgroup Integration Areas of Electronic Government**

Nazaré Lopes Bretas (MP/SLTI) – COORDINATOR  
Adelino Fernando Correia (DATASUS/MS)  
Adriano de Medeiros (INCRA)  
Ana Lúcia Viçoso da Cruz Almeida (DATAPREV)  
Antônio Albuquerque (PR)  
Carlos Bellone Neto (RFB)  
Ceres Albuquerque (ANS)  
Cláudio Manoel Cordeiro (SERPRO)  
Frederico Duarte Guerra de Macedo (ESPORTES)  
Maurício M. Martinez (MEC)  
Mônica Lucatelli (DATAPREV)  
Paulo Henrique Santana (MMA)  
Pedro Paulo Cirineo (BB)  
Ricardo de Lima (INCRA)  
Rogério Werneck (DIRTI/PR)  
Sylmara Campos Pinho Garcia (MP/SLTI)  
Wagner Gardusi Guarizo (PR)

#### **Collaborators**

Igor de Freitas (MDS)  
Felix de Sousa (MDS)

#### **Subgroup: Standards for Exchange of Special Information**

Roberto Penido Duque Estrada (DSG/CIGEX) – COORDINATOR  
Alex Araújo (CAIXA)  
Aramis Mota (GSI/PR)  
Christian André H. Govastki (MME/SEE)  
Dêner Lima F. Martins (ABIN/PR)  
Ellio Alves de O. Soares (CAIXA)  
Eneias Roberto Shüller (CAIXA)  
Fernando Gibotti (CAIXA)  
Gerson Barrey (MEC)  
Gilberto Ribeiro Queiroz  
Gustavo Araújo (MME)  
Hisao Fujimoto (MME)  
Jorge D. M. Cerqueira (PR/GSI)  
Linda Soraya Issmael (DSG/CIGEX)  
Lúbia Vinhas (INPE)  
Lúcia Helena Luz (CAIXA)  
Moema José de Carvalho Augusto (IBGE)  
Mosar Rabelo Júnior (MMA)  
Silmara Ramos (PR/GSI)  
Silvio Carlos Heitor Jorge (CAIXA)  
Tálsia Garcia Meira (DIRTI/CC/PR)  
Valdevino S. Campos Neto (ANA)  
Zandhor F. S. Cavalli Pradi (MS)

#### **Collaborators**

Carlos Brasileiro (MDS)  
Edmar Morett (MMA)  
Enos Josué Rose (MCIDADES)  
Rafael M. Sperb (Univali)  
Wilfredo Pacheco (ANA)

## e-PING Reference Document – Version 3.0



Werner Leyh (MS)

### **Illustrations**

Hezrai de Souza Cruz (MP/SLTI)