



Risk factors in e-justice information systems



João Rosa, Cláudio Teixeira^{*}, Joaquim Sousa Pinto

Department of Electronics, Telecommunications and Informatics, University of Aveiro, Aveiro, Portugal

ARTICLE INFO

Available online 23 May 2013

Keywords:

E-justice
E-government
Risk factors
Information system
Developing countries
Cape Verde

ABSTRACT

With the increase of the communication systems' bandwidth and with the dissemination of the information systems, the fields of information and communication technology application expanded in almost all directions. E-government in general and e-justice in particular are no exception and these areas suffered strong changes in the last decades. There is no democracy without a system of swift and transparent justice. Therefore, the introduction of information systems in the courts allows a decrease both in time and number of pending processes, boosting the efficiency of the services provided to citizens and to the society in general.

This paper analyzes and discusses different worldwide e-justice experiences. Special emphasis is addressed on the risk factors on the design, development and implementation of such systems. Finally, we present our own experience in the development of an e-justice information system in Cape Verde, an African development country. The scope of our system ranges from the design team until the training of the justice agents.

© 2013 The Authors. Published by Elsevier Inc. Open access under [CC BY-NC-ND license](#).

1. Introduction

In the last decade e-government systems became a central concern in the countries' policies. E-government is defined by OECD as “the use of information and communication technologies, and particularly the Internet, as a tool to achieve better government” (OECD, 2003). These information systems provide a tool to organizations and people to computerize procedures and everyday tasks, combining technology, organization know-how and people experience.

E-government states that it can improve efficiency, decrease budget and increase trust between society and governments. With these major

behind Spain (ranked 25th). Over the last decades they have improved their democratic structures, developing democracy, and their efforts are recognized by the international community.

Cape Verde is an archipelago of 9 islands located in the Atlantic Ocean with a combined area of over 4000 km². According to the 2010 census, the country has 491,875 inhabitants, 50.5% female and 49.5% male (Instituto Nacional de Estatística de Cabo Verde, 2011). The population increased 11.6% compared to the 2000 census.

In terms of justice, in 2008, 8415 court cases were filed and in 2009 there was a decrease of 5.56% on filed cases, totaling 7972 new cases (Conselho Superior da Magistratura Judicial, 2010). In terms of cases

new metadata, citation and similar papers at core.ac.uk

brought to you by CORE

The separation amongst the executive, legislative and judicial powers is the keystone in democratic countries. Citizens hope to have a fair, efficient and transparent justice system. To help reaching for better justice, e-justice information systems are designed to handle lawsuit related information, mimicking and possibly improving traditional paper based workflows, thus providing a useful tool to involved agents.

According to the 2011 Economist Intelligence Unit report (Economist Intelligence Unit, 2011), Cape Verde is the first African country in the Democracy Index (ranked 26th), leading over countries like Portugal (ranked 27th), France (ranked 29th) or Brazil (ranked 45th) and just

decided cases (pendency), there is a drag of 60 cases in 2008 and 700 cases in 2009, totaling about 10% of dragged cases in just 2 years. At this rate, the courts will be more and more clogged and justice will be served more and more slowly. The informatics tools presented in the justice system were virtually nil with only productivity tools installed and used in the clerk's computers at the courthouses. This makes the procedure slow and time consuming, because there is no standard procedure through the justice system and the assignment of human resources is not efficient.

Therefore, in 2008 the Cape Verdean Ministry of Justice started the planning for the development of an information system, named SIPP (Sistema de Informação do Processo Penal/Criminal Proceedings Information System), to be used in the courts of law. SIPP is a joint initiative, sponsored by the Ministry of Justice of Cape Verde, the Superior Council of Magistracy and the Superior Council of Prosecutors and would be developed from scratch by the University of Aveiro and University of Cape Verde. The SIPP has been in testing phase since June 2010 and will be put in production during 2012. This paper

^{*} Corresponding author. Fax: +351 234 370 545.

E-mail addresses: joaorosa@ua.pt (J. Rosa), claudio@ua.pt (C. Teixeira), jsp@ua.pt (J. Sousa Pinto).

assesses the risk factors of developing such system, based on previous experiences and on our own experience.

This paper is organized as follows: this section introduces the problem addressed in this paper; [Section 2](#) details on previous experiences worldwide regarding the adoption of electronic systems to court cases; [Section 3](#) compares the cases studies presented and draws conclusions from these experiences; [Section 4](#) presents the information systems and tools used for modeling e-government systems; [Section 5](#) presents the Cape Verdean experience; [Section 6](#) presents the risk factors involved in e-justice systems; and finally, [Section 7](#) presents the conclusions and future work.

2. Case studies

In this section we present what we assessed as relevant case studies in e-justice systems. The process of analysis and comparison of the case studies is based on the methodology defined by Velicogna et al. (Velicogna, Errera, & Derlange, 2011; Velicogna, 2007). According with the authors, their methodology is the most effective to study the innovative character of ICT (Information and Communication Technology) in the broad area of Justice. In the aforementioned methodology, authors make a comparative analysis of the case studies within different categories (Technology, Organization, and Complexity). Similar to this approach, Fabri (2007) uses his own topic characterization to evaluate the case studies.

Despite being based on the Velicogna's approach, our analysis includes broader geographical, social, economic, and political information of the countries analyzed. This broader overview helps to contextualize the problems that each country tried to address at a given time. Within every case studied, we describe the Justice scenario from the first computerization attempts to the currently solutions (if any). As important as the system-per-system comparison, we bring a development perspective of each of the analyzed countries. Also, when information about the overall system infrastructure is available (from state of the art, local legislation and regulations, social communication, etc.), we include it on the evolution overview. Finally, considering that even the best computer systems require users to interact with, if available, we include the user's feedback, the development support groups' feedback and usage information about the analyzed systems.

This approach presents readers an overview in terms of evolution of each country's Justice ICT efforts, and offers an evolution comparison (Justice wide), rather than a comparison over specific systems. The evolution and outcome of each country's Justice System offer invaluable lessons in terms of what to do, what to expect, and what not to do when starting a new project or an evolution of a project within the Justice System.

The criteria to choose the relevant case studies were: (1) their innovative character; (2) the quality of available information (both technical and non-technical) about those systems; (3) the different social contexts and culture mindsets in which such systems were deployed; and (4) failed and successful examples.

2.1. Singapore

2.1.1. The Justice system prior to ICT attempts

Singapore was the first country to design and implement an information system for the justice system.

Back in 1991, Singapore's justice system faced the backlog problem, where a case took too long to produce a decision, and unsolved processes started to increase (Magnus, 1999). When the authorities diagnosed the justice system, they tried to find the causes for this problem and created a plan to decrease the time it took to produce a decision. This was accomplished by adopting solutions like night courts and cultural changes in methods and approaches when working in a case (Subordinate Courts). In 1993 the backlog problem was

solved and the justice authorities wanted to increase the courts' performance, continuing with the new reforms.

2.1.2. ICT evolution

To execute the new reforms, the justice authorities used the knowledge network created with their worldwide peers, facing the same problems, and adopted good practices, know-how and technology to create the first e-justice information system. This information system is based on multimedia kiosks, named ATOMS (Automated Traffic Offence Management System) (Magnus, 1999). With these multimedia kiosks they exposed some court services to citizens, like the payment of fines and the ability to plead guilty of offenses by the citizens, 24 h a day, 7 days a week, through this system.

This is a centralized system, where all multimedia kiosks are linked to ATOMS database, which manages the offender's information ([Fig. 1](#)). This system was the pioneer in the e-justice systems, enabling citizens to pay their fines, or consulting cases in other locations, without addressing to the court.

In 1996 Singapore authorities took a new approach in application development and infrastructure management. Until then, the application development and infrastructure management were ensured by IT (Information Technology) professionals linked to the public authorities. This approach led to a budget escalation. In 1996 however, the authorities decided to outsource both application development and infrastructure management, releasing resources to apply in other projects, other areas or new reforms. This approach was expected to reduce the overall budget, while boosting the country's economic growth. In 1999 web-based applications began replacing desktop applications. Not only had the application's interactivity changed, but also the standard web-based access to information enabled data and documents exchange between justice entities. This helped on improving efficiency, transparency and decreasing the time consumed, because it changed the way of addressing the Court. This second generation of information systems uses a typical 3-tier layer ([Fig. 2](#)) using Oracle databases, FileNet workflow systems and Powerbuilder or Oracle client software. To standardize electronic documents interchange, they have elected PDF (Portable Document Format).

After this shift, one of the new web-based information systems, designed and developed to replace the legacy systems, was the EFS

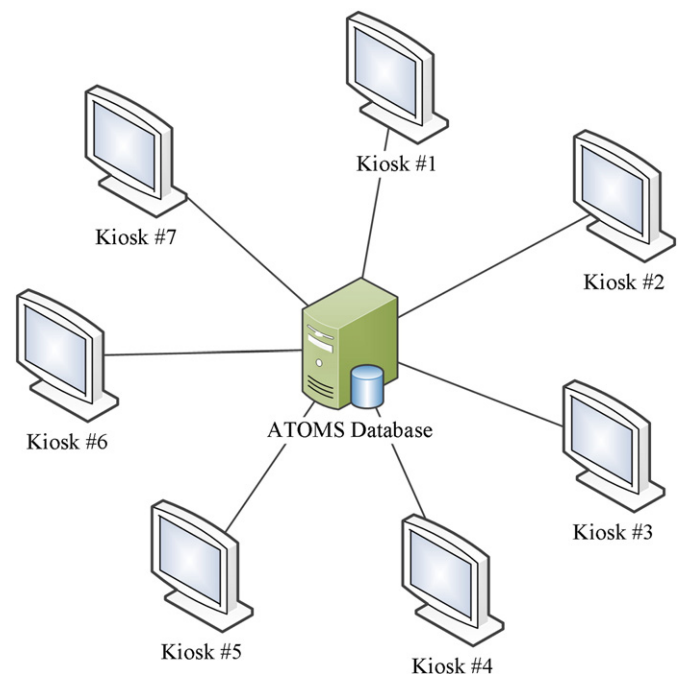


Fig. 1. ATOMS architecture.

(Electronic Filing System), implemented in the end of 1999. This information system was developed for civil matters, allowing lawyers to file electronic documents and providing real-time information to all involved entities.

In 2002 Singapore launched the ICJS (Integrated Criminal Justice System). This project intended to link all entities involved in the criminal justice process, using the country's justice network. With this approach, Singapore justice system gained an integrated system, and reached all the entities involved in court cases. At the same time they fitted the courtrooms with video-conferencing systems, thus enabling citizens to participate on trial sessions from any courthouse, protecting violent crime victims against their perpetrators.

But with all these systems, the flow of data grew exponentially and the communication network started to overflow. With this technological constrain, the authorities started a new project to upgrade the communication network infrastructure, creating the BENI (Broadband Enterprise Network Infrastructure) based on ATM (Asynchronous Transfer Mode) technology (Orzessek & Sommer, 1997; TelecomSpace, 2011). BENI was finished in 1999, and held a high speed backbone of 622 Mbps, scalable up to 2.1 Gbps, supported by WAN (Wide Area Network) segments of 45 Mbps each, connecting the different locations where justice entities operated. This upgrade led to the update of the retail communication network infrastructure, with download capacities ranging from 6 to 8 Mbps and a penetration rate of 98%. After a decade, a new project is running, to upgrade the country's network to broadband network at 1 Gbps, adding value to the economy and society (Wever, 2009).

In 2002 Singapore authorities estimated that 50% of the court services were already computerized. Nevertheless, it was still possible to address the courthouse using the traditional methods. Both methods (electronic and traditional) coexisted without impairing the efficiency in the courthouse or in the process.

To improve the security in these information systems, they implemented a PKI (Public Key Infrastructure) (Singapore Network Services Pte Ltd, 2007), represented in Fig. 3:

With this feature all documents can be ciphered/deciphered and digitally signed, increasing the security of the systems against threats. Electronic documents can be authenticated and their integrity and issuers verified. To manage the PKI, the Supreme Court or the Subordinate Courts nominate a publicly available, commercial entity as the Root CA (Certification Authority) authorized to issue the certificates to law firms, lawyers and court users.

2.1.3. Results and lessons learned

Currently, the described systems are in use, and subject to common software updates. Singapore's experience positively reinforced the general notion of gradual introduction of novel systems. They started by addressing a specific problem, with a tight goal oriented approach for handling traffic offenses. With the success of this first system, and considering that it required some core court services

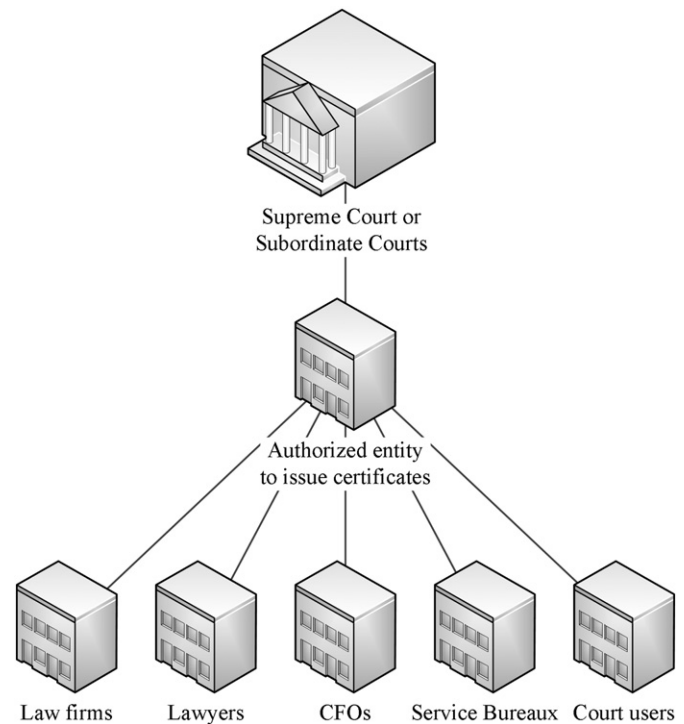


Fig. 3. Singapore justice PKI.

available for machine-to-machine communication, they embraced the new goal of managing court cases.

Considering that the first computerization approaches were made in the 90's there was the need to shift from a mainframe like approach to web technologies, making system maintenance and access simpler. The new web applications, with support for videoconferencing and other technological advances produced an unanticipated result: network overflow. To overcome this constrain, they upgraded the communication network infrastructure, with benefits for everyone (both public and private services).

In terms of the development and support models for the different applications in use, the first approach was based on an internal development team and later on outsourcing. To the best of our knowledge, there is no available information on problems regarding either solution, with budget constrains considered as the main reason for shifting from one approach to the other.

2.2. Brazil

2.2.1. The Justice system prior to ICT attempts

Brazil is a federation of states (despite having a national policy for financial and fiscal matters). Each state is responsible for its justice system, taking different interpretations of the law, different procedures and organics. This leads to a high level of fragmentation between states, not only at procedures level, but also at administrative level. At the court level, central courts exist in each state capital, and small claims courts spread around the state.

In terms of backlog and congestion rates, according to the Justice National Counsel (*Conselho Nacional de Justiça*), in 2003 there was a congestion rate of 81.4% in the first degree federal courts, 76.2% in the second degree federal courts and 77.2% in the specialized courts (*Conselho Nacional de Justiça*, 2013). From 2003 to 2007, the congestion rates kept on shortening (78%, 60.5% and 42.2%, respectively), mostly as a result of a bigger investment in manpower and new courthouses. From 2007 to 2011 (last known report), the congestion rates were kept relatively stable.

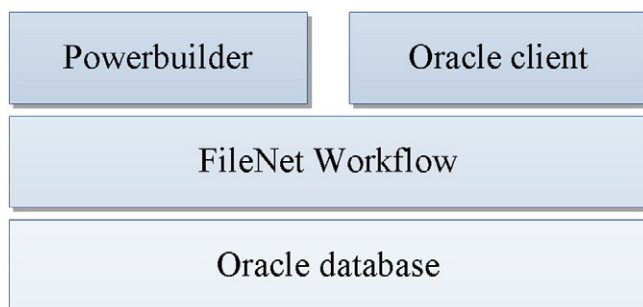


Fig. 2. General implementation of Singapore's 2nd generation of information systems.

2.2.2. ICT evolution

Brazil's justice information system passed through several stages of maturation (Andrade & Joia, 2010). Brazil's information system evolution is deeply connected with the Brazilian administrative system.

The ICT evolution in Brazilian courts can be divided into three phases: individual initiatives, computerization and virtualization. Individual initiatives are carried by each court member, and relate to the identification and usage of productivity tools (like text processors or spreadsheet editors) that each member best identifies to carry out its functions. With this approach, each court member created his own procedural criteria and taxonomy for each task, which resulted in a higher fragmentation level in work inside of the same court division.

To overcome the intrinsic fragmentation resulting from the individual initiatives, several information systems were created to coordinate the administrative work and justice process at state level. Some states bought their information systems, while others developed their own. This plethora of information systems raised data and documents interchange problems. The extreme example was that different versions of the same system, implemented in courts at the same state, were not able to communicate amongst each other.

When this problem became a liability, they advanced to a virtualization phase, with the creation of a national virtual system that would be implemented locally, with the rules of the state. This approach tried to create a unifying information system for all states. This system could be customized inside each state, at the court level. Despite of the different maturation levels in the computerization phase between courts (even in the same state), virtualization took the lead. However the results were a disaster, since the degree of customization in the information system led to a steep learning curve of the overall system. The studies made at the time revealed losses of over 50 million US dollars, leading to the abandonment of this model in 2010 (Andrade & Joia, 2010).

With this experience, a common strategy for the country was created, with a project until 2014 with the following requisites:

- Provide to all courts adequate computer equipment;
- Develop an information system that unifies the justice system.

This information system must:

- Be based in industry standards, preferably using open source technologies;
- Be web-based;
- Digitalize and automate the process distribution;
- Create mechanisms to monitor case related penalties, with special attention to temporary arrests;
- Make accessible process procedures, respecting the process privacy.

After identifying the major goals and defining the overall strategy, the communications infrastructure was singled out as an important piece to support the new information systems. To cope with the demands of communications, they devised a plan to upgrade the communications infrastructure. In this plan, the connection between the courthouses should be of at least 2 Gbps, and in each state capital the network should link central courts and small claims courts. The network over the state should connect at least 20% of small claims courts.

To secure data, Brazil took advantage of a preexisting national PKI (Barra, 2006; Coelho, 2010). This national PKI was created by federal law, in 2001, where the Civil House of the Presidency of the Brazilian Republic transformed the ITI (*Instituto Nacional de Tecnologia da Informação*/National Information Technology Institute) in the unique Root CA, creating the national PKI, with the infrastructure represented in Fig. 4. The Steering Committee was created for the regulation of the whole PKI and auditing the Root CA. Federal government and civil society representatives formed this committee. Along with this, the COTEC (*Comitê Técnico da Infraestrutura de Chaves Públicas Brasileira*/Steering Committee and Executive

Technical Commission) was created with representatives from federal government and consultants to this process. ITI was responsible for managing root certificates' life cycles and accreditation, auditing and issuance of subsequent CAs and their certificates.

Below the Root CA, each organic unit from the civil states in Brazil was entitled a first level CA with the RA (Registration Authority), with an optional ICA (Intermediate CA) and RA (depending on internal organization), as presented in Fig. 5. The ICAs and RAs can represent public or private sectors (ITI, 2011).

When the e-justice information system needed a PKI in 2004, they choose the national PKI, but the National Bar Association, on behalf of the lawyers, produced a strong opposition against this approach, using technical issues arguments (Martínez & Abat, 2009). The real argument however, was political, since lawyers did not want to use a system subordinated to the executive power. Moreover, the National Bar Association had its own PKI. If they joined the national PKI, that investment would be wasted. In 2006 a federal law modified the Civil Procedure Code, recognizing the national PKI as the single PKI in the justice system. With these changes, the National Bar Association accepted its use and shared the lawyers' information with this executive initiative, apart some lawyers' intent to the impugnation of these law changes.

2.2.3. Results and lessons learned

Brazilian Justice Information systems and applications are currently in a transition phase. Due to its intrinsic administrative organization, each Brazilian State was able to decide on how to implement its information system (internal development, copied from other state, or bought from software houses). However, since there were no directives to enforce the use of standards and systems communication, most

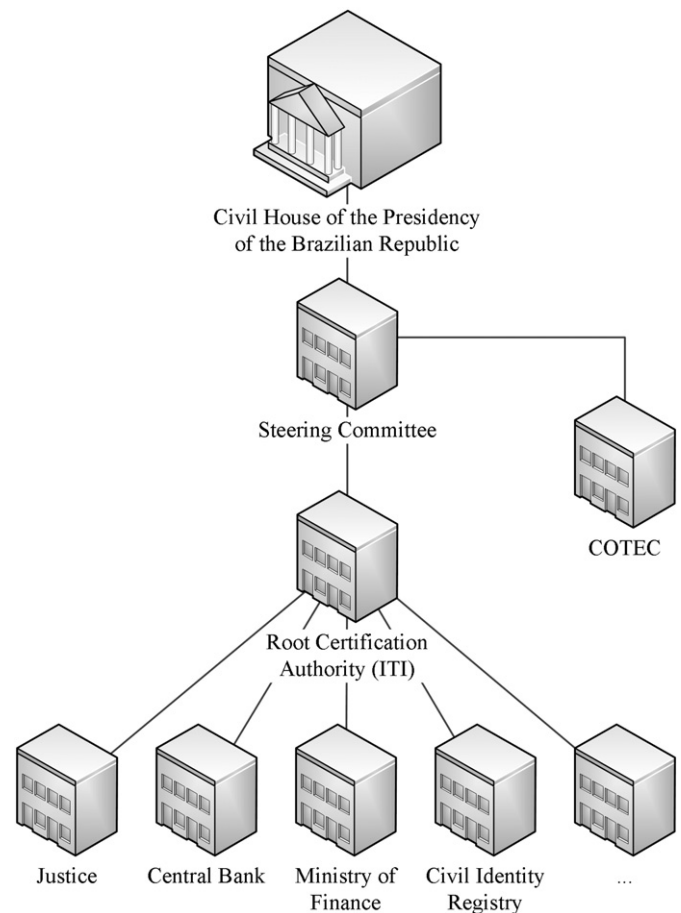


Fig. 4. Brazilian PKI.

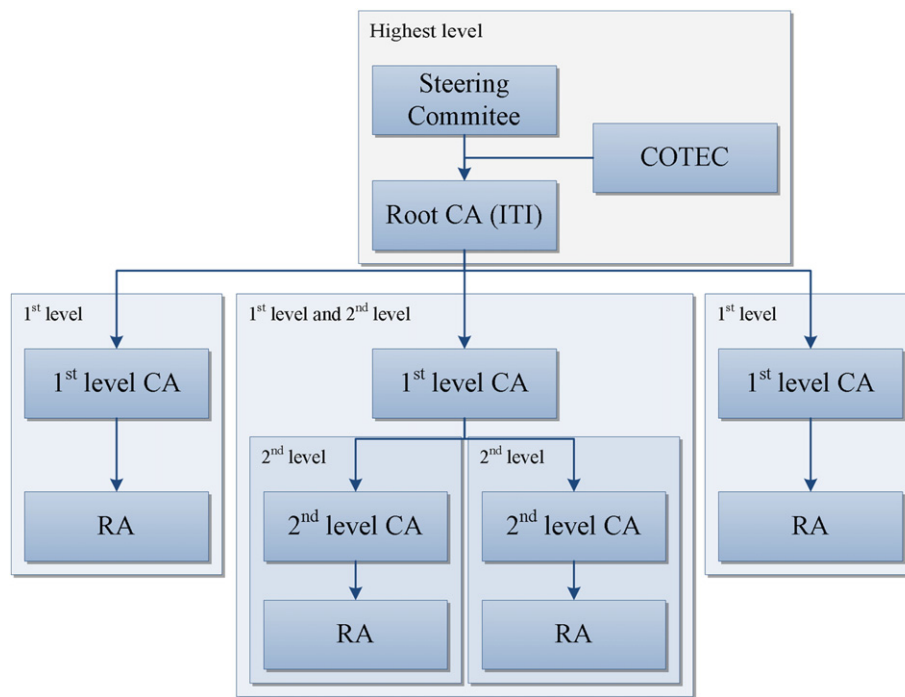


Fig. 5. Brazil's CA conceptual architecture.

adopted solutions failed to communicate with others (even on the same administrative State). To overcome this problem, Brazilian authorities started a new project for the development of a national information system.

Despite the theoretical benefits that arise with the introduction of information systems, only when this national information system is in place will it be possible to assess its factual benefits. Until now, the congestion rate drop was supported by the increase of judges and clerks.

The Brazilian experience reminded us that the correct planning of information interfaces and rules of communication is essential for projects of such magnitude to be successful. In the first attempts, Brazil failed to congregate its States' independence with the requirements of a national information system for the Justice. The new project tries to handle these specificities, by designing a communication standard to be used among all the systems.

Another interesting fact on the new project is the identification of the supporting system infrastructures upgrade as a major goal. The telecommunications network will be subject to an upgrade, providing higher bandwidth. The Brazilian authorities expect that this upgrade will provide the incentive needed for the use of information systems as a working tool.

As with Singapore, the Brazilian authorities decided to enforce document integrity and validation through the use of a PKI. Even if the PKI architectures in use may be debatable, the benefits of its use were clear for the authorities, given the assurance, by its use, in terms of security.

2.3. Belgium

2.3.1. The Justice system prior to ICT attempts

Back in the 90's, the Belgium Justice system was struggling with extreme slowness and sluggishness. Litigation over intellectual property, for example, would take many years to trial, and companies found themselves unable to sell their products until the court's decision. The same thing was happening in criminal matters, like in 1996, where the Dutroux case required 9 years to take a pedophile to trial.

2.3.2. ICT evolution

In the last decades, the Belgium authorities have tried to introduce some changes and reforms in the Justice, such as the purchase of computer equipment for the courts, and even given a laptop computer to each judge (Velicogna, 2007). Due to the more active role of the civil society, and in the light of the events of the 90's, authorities were forced to rethink their reforms thoroughly.

Until the year 2000, authorities made several attempts to computerize the justice process, all unsuccessful. These unsuccessful attempts were mainly due to lack of planning, like local attempts to develop information systems to support some court members, without the perspective of integration in a broader e-justice system. All these attempts resulted in many concurrent applications, resulting in a high level of fragmentation, information islands and rapidly obsolete information systems. An example of this problem was the existence, at a given time, of 13 different applications with more than 100 databases, despite the lack of data or document interexchange between them (Martínez & Abat, 2009). After authorities identified these problems and their causes, they started a restructuring project: the Phenix Project.

The Phenix Project was designed to increase the ICT in public administration, increasing the public service and the democratic process (Vuyst & Fairchild, 2006). This e-justice system was designed to cover criminal and civil matters, developing a unifying platform to the entire justice system. This project led to the creation of a flexible framework, created from the common practices of the various agents and re-engineering where IT technicians identified as more convenient.

During the developing phase of the information system, three major challenges were identified:

1. The information system had been designed to replace the traditional way to address to the courthouse, i.e., after the implementation, this would be the only way to address the courthouse;
2. The use of electronic documents was already enshrined in law, but the use of an information system to support the whole process was not. Due to the country government peculiarities, the changes are required in the national legislation, so that the information system could be used were identified as one of the main challenges;

3. The change in the justice agents' mindset, since the mode of interaction with the justice system would be changed.

Another key point of the system, according to their IT technicians, was its development using open source technologies. After the start of the development, a major issue was detected: in case of a catastrophe, the information recovery procedure was still to be designed and considered as a challenge (Vuyst & Fairchild, 2006).

The Phenix system was introduced in small instance courts, trying to standardize procedures, law interpretation, minimizing the occurrence of miscarriages of justice, thereby increasing the efficiency of the justice process and the efficient use of justice resources.

Although this system was web-based, the internet network penetration rate in the country was only 50%, thus constituting an obstacle to the implementation of an information system with this nature.

The authorities had high hopes in this project, and due to its simple and transparent procedures, they expected that it would make the justice system more accessible to society, leading to a greater understanding of justice decisions. They also expect to change the agents' mindset, moving from the physical paradigm, where everything was in paper—to the digital paradigm, where everything from the laws to consult and procedures to take was computer supported.

Despite the efforts between all stakeholders (IT technicians and court members) and the budget afforded to the information system, in 2007 the Ministry of Justice stopped the Phenix Project, leaving to the next government the final decision about its continuation (Martínez & Abat, 2009). The main argument was that the development team could not solve the complex technical problems inherent to such project.

2.3.3. Results and lessons learned

Currently, the Phenix project has come to a halt, by ministerial decision. This was indeed an ambitious project, since it was designed to support both criminal and civil matters.

From our perspective, and considering the Singapore case study, the complexity and scale of the problems may have been the main reason for its failure. In Singapore, authorities began to address small problems, before moving to the bigger scale issues concerning criminal and civil matters. This way, they managed to accumulate experience and user feedback.

A good project management and context adaptability could have avoided some of the encountered problems.

2.4. Portugal

2.4.1. The Justice system prior to ICT attempts

Portugal endeavored many efforts along the last three decades to jump in the digital era (Santos, 2005). In the 80's decade, several governmental agents tried to introduce information technology in courthouses, but these efforts had no success (Silva, 2006). In the following decade, this scenario did not change, despite the massive buying of computers and other electronic equipment to courthouses, just as presented in previous case studies.

With the increase of the internet penetration ratio, several public and private initiatives had created portals and legal databases, providing information to general public without any type of charges.

2.4.2. ICT evolution

The e-mail was the first electronic service used to exchange data amongst agents. Based on this, an internal network was created between the courthouses, linking secretaries and enabling documents to be sent by authenticated e-mail. This experience was essential to support the development of the Habilus information system. Habilus was created with the objective of simplifying the secretaries' administrative work. The main justice documents were standardized, and databases with the processes and their intervenient data were

designed to increase efficiency in the court. This information system was criticized by the stakeholders due to the wrong process taxonomy, the lack of elements and the mixing of legal terms.

Despite this information system, process backlog became a problem in the Portuguese Justice system. To speed up the procedures, streamline the resources and increase the courts' efficiency, a new integrated information system was developed (Ministério da Justiça, 2003), starting with the administrative and fiscal courts.

This information system, named SITAF (*Sistema de Informação para os Tribunais Administrativos e Fiscais*/Information System for the Administrative and Fiscal Courts), debuted on January 1, 2004. SITAF (Direcção-Geral da Política de Justiça, 2005; Instituto das Tecnologias de Informação na Justiça, 2004) was created to computerize the administrative and fiscal processes, with electronic filing and document delivering. It is a web-based application, with secure access and a distributed architecture as presented in Fig. 6, available in 19 courthouses. SITAF's main features include:

- A workflow engine to manage the process procedures;
- Daily automatic process distribution;
- Electronic document storage based on standard formats like RTF (Rich Text Format), TIFF (Tagged Image File Format) and PDF;
- Multi-access to the process and its documents between agents.

SITAF was the first major information system in Portugal developed specifically for the Justice. With this experience, the perspective about e-justice systems changed, and new projects were developed, in several phases (Ministério da Justiça, 2008a,b). Other actions were taken in parallel like renewing the desktop equipment and training the justice agents engaged in electronic proceedings. In 2008 a new application called CITIUS was developed to complement the Habilus. CITIUS was developed specifically to civil process acts but based on the SITAF's philosophy. It supports specifically declarative and executive acts and civil injunctions, and the main users are judges and, since 2009, also prosecutors.

CITIUS has electronic filing and electronic delivery of the digital documents used in the processes' acts, but for specific acts it is mandatory the use of the traditional/physical procedure – going to court secretary and deliver the pleading paper – instead of sending the

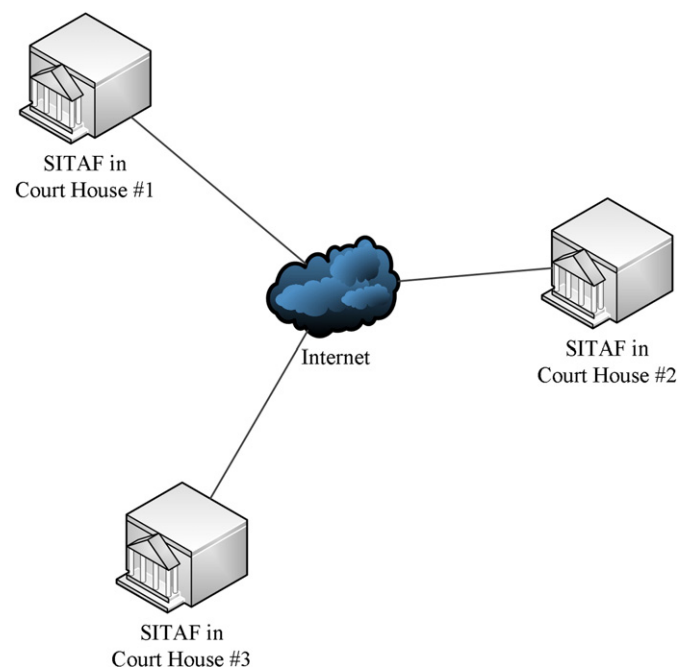


Fig. 6. SITAF distribution architecture.

digital document throughout the information system. This small change caused several system complaints. The system trials started first in a single courthouse for a period of half of a judicial year: after that period the system became universal. During the trials it was possible to send electronic documents by e-mail. After the universal introduction of the system no more documents could be sent by e-mail, because the digital platform handles and stores the documents more efficiently than the e-mail boxes. In 2009, prosecutors gained access to CITIUS and were obliged to use it (Ministério da Justiça, 2008a,b). Later in 2010, CITIUS information system was upgraded to CITIUS Plus, with some bug fixes and new features (Ministério da Justiça, 2010a,b). The major feature is the new ability to record the court's hearings offline when the system is down or unavailable.

In March 2011, the Portuguese government reinforced the strategic plan for the Justice, approving a new plan that involves the replacement of currently existing systems, upgrading users' equipment, improving the network equipment and increasing the available network bandwidth (Presidência do Conselho de Ministros, 2011).

SITAF was one of the selected systems to be upgraded (SITAF 2.0) due to the changes that occurred in the Administrative and Fiscal Laws.

The old Habilus – due to some of the known issues – will be replaced with a brand new application that is expected to improve the work in criminal cases by prosecutors and administrative staff. The AGIP (*Aplicação para a Gestão de Inquéritos-Crime*/Application for Criminal Investigations Management) is being implemented and is designed to digitally support all procedures in criminal investigations, decreasing costs, as pointed by Maria José Morgado, Deputy General Prosecutor. She claims that it will be possible to replace the piles of hundreds of papers that usually compose the volumes in criminal procedures, simply by using this information system. The total cost with AGIP is projected to be around 1.4 million euros, but a rapid return of the investment is expected (SIC, 2011).

The infrastructure changes were mainly focused on concentrating scattered resources and upgrading the communications network. With the new generation networks installed in Portugal, authorities created the RNCJ (*Rede Nacional de Comunicações da Justiça*/Justice National Communications Network). To improve process efficiency, a VPN (Virtual Private Network) is planned, ensuring secure communication in remote access to the judges and prosecutors. With the use of such VPN, users not physically in the courthouse can access the same features and functionalities as if they were working on the court, saving costs and time (in transports, at least), while maintaining the same level of integrity and security.

With RNCJ improvement, the ITIJ (*Instituto das Tecnologias de Informação na Justiça*/Justice Information Technology Institute) will change the overall system architecture, moving from a distributed environment – one server for each courthouse, or around 350 servers – to a centralized environment where all the processing activities will be concentrated on the ITIJ DPC (Data Processing Center). This change will improve the overall system security and maintenance.

With resource concentration it will be possible to use virtualization technologies and reduce the actual hardware infrastructure from nearly 900 servers in DPC to near 200, with the obvious decreasing of power consuming, space requirements, CO₂ emissions, and most importantly, with expected savings of nearly 500,000 euros per year.

All these information systems use the Portuguese PKI, created in 2006 by the Presidency of the Council of Ministers (Presidência do Conselho de Ministros, 2006). Fig. 7 outlines the Portuguese PKI. This national PKI has a SCEE (*Sistema de Certificação Eletrónica do Estado*/Steering Committee to the Electronic Certification System of the State), with representatives from the government, the GNS (*Gabinete Nacional de Segurança*/National Security Office), the National Homeland Security Network, the FCCN (*Fundação para a Computação Científica Nacional*/Foundation for National Scientific Computing), IT (*Instituto das Telecomunicações*/Telecommunications Institute), among others. The SCEE has a country level CA, which is available both as a

self-signed Root CA and as an ICA, certified by a publicly available, commercial Root CA, the ECEE (*Entidade Certificadora Eletrónica do Estado*/Electronic Certification Entity of the State) that is responsible for managing the PKI, and other ICA's in PKI.

The ANS (*Autoridade Nacional de Segurança*/National Security Authority) was empowered to audit and issue the certificates of accreditation to ICA entities present in the PKI. The SCEE works independently from other private and international PKIs, but guarantees that its certificates are recognized worldwide as valid, since the country level ICA is certified by an international certification authority. Portuguese PKI is conceptually similar to the Brazilian PKI previously presented: the country level CA can have several first level ICAs with the respective RA, and can support more than one CA level depth, as depicted in Fig. 8. The main difference is that the Brazilian PKI is isolated, with its main CA being in fact available only as a Root CA, meaning that no certificates can be recognized without a proper user administration action of installing a new Root CA public certificate (which may not be possible due to wide level computer domain policies, for example).

In the first year that CITIUS was operational (2009) more than 85% of the acts and proceedings were filed electronically, totaling more than 5 million acts and almost 2 million electronic notifications (Ministério da Justiça, 2010a,b). 51% of these processes were initiated using CITIUS (Neves, 2009). With these impressive numbers it should be safe to assume that this is a successful system. The reality shows that this fact is not so clear to all stakeholders. The system has suffered numerous critics and cheers. The strongest opposition came from the ASJP (*Associação Sindical dos Juizes Portugueses*/Association of Portuguese Judges) (*Gabinete de Acompanhamento da Informatização nos Tribunais* (GAIT/ASJP), 2009). ASJP issued a survey to which about 13% of its associates answered, and the main conclusions from the survey were as follows:

- CITIUS interface is not accessible, i.e., it does not follow the heuristics for accessibility and usability;
- The system is slow, and ASJP pointed out the main cause is the old equipment available;

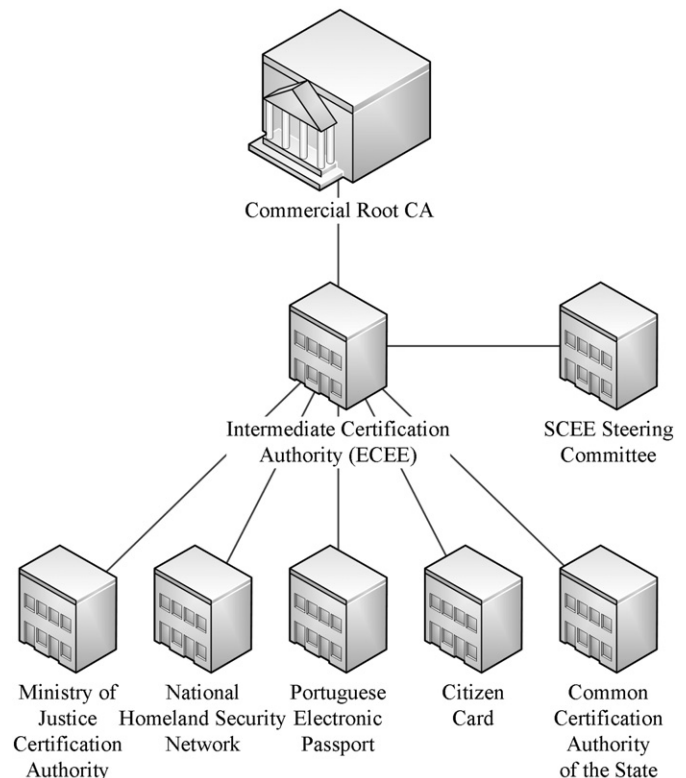


Fig. 7. Portuguese PKI.

- The judges' inability to understand the current digital paradigm used for handling processes in the system hamper their productivity.

In absolute contrast with the ASJP's critics, lawyers praised these reforms, pointing that CITIUS (Neves, 2009):

- May provide a better service to their constituents;
- Decreases costs of the proceedings;
- Decreases costs to their constituents, since lawyers do not need to go to court to file or deliver documents, due to the electronic submission;
- Increases transparency between all agents.

2.4.3. Results and lessons learned

Portuguese Justice Information System's panorama is changing. From the support of e-mail as an official vehicle for case files, to the creation of an information system to manage the law cases, Portuguese authorities are trying to keep up with the times. Currently, CITIUS and SITAF are being upgraded, and a new system is being designed to replace Habilus.

The supporting system's infrastructure is also being redesigned, moving from the scattered servers' solution to a centralized solution, accessible using a VPN. The VPN solution is expected to enable the Justice system's users more freedom and possibilities in terms of working location (office, home, traveling, ...).

As with Singapore, Portugal started with simpler experiences to solve smaller problems (e-mail integration and Habilus) and evolved to systems capable of handling entire cases (SITAF, CITIUS and AGIP). This evolution, accumulated experience and user's critics are seen as the breeding grounds for new features.

3. Comparative analysis between case studies

This section presents a comparison between the previously presented information systems.

Table 1 summarizes the relevant dates (when available) to the development time, the development team composition and whether the information system is still being in use today.

Singapore and Portugal implemented a phased coverage of the different areas of Justice. Both countries started with civil process and moved on to criminal process.

In terms of development and sustainability models, there was a mixture of in house, outsourcing and mixed (in-house and outsourcing) development.

In Portugal, the chosen approach was the in-house development for the information systems, because the Portuguese state created an institute with the staff having the technical skills required for various tasks (software and communications).

Belgium chose the opposite approach, outsourcing the Phenix e-justice information system.

In Brazil and Singapore we found a mixed approach but for different reasons. In Brazil, the first approach gave each State the freedom to choose between in-house development or outsource development of the information system. However, considering the results of such freedom (most of the systems cannot communicate and exchange data with each other), the new e-justice information system is being developed in-house. In Singapore until 1996 the e-justice information system was developed in-house, but in most recent developments, the national authorities choose to outsource as a way to promote the country's economic growth.

Most of the presented information systems are still being used. The exceptions worth mentioning are the Phenix project and Brazil's scattered systems (an approach that led to a wide variety of information systems), without data interexchange or communication between different information systems, decreasing the efficiency and increasing the costs. Table 2 summarizes the system's access type, architecture and its offline data processing ability. The developing technologies were not taken into consideration because that decision has no reflection on the architectural features.

Analyzing the data from Table 2 jointly with the developing time from Table 1, it is clear the paradigm shifts from desktop applications to web applications. This may have occurred both due to the evolution of the communication network, providing faster and more reliable communications, and due to the emergent web-based technologies. This paradigm shift is only observed in countries that started developing e-justice information systems in the earlier 90's, like Singapore or

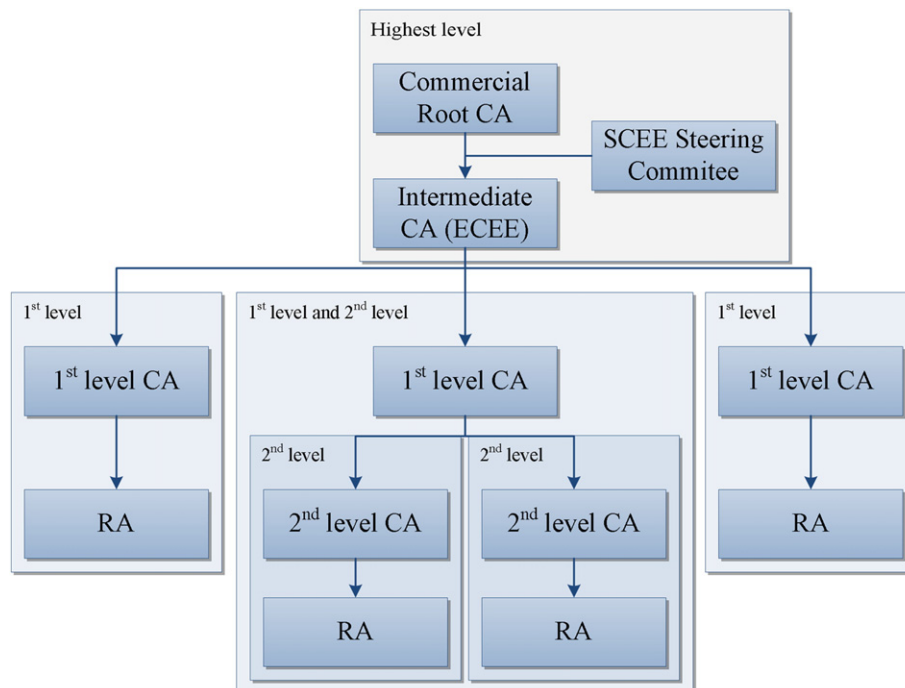


Fig. 8. Portugal's CA conceptual architecture.

Table 1
Developing comparative analysis.

Country	Information system	Developing time		Development	Still working?
		Start	End		
Singapore	ATOMS	1993	1999	In house and outsource	Yes
	Desktop app	1993	1999	In house and outsource	No
	EFS	1999	–	Outsource	Yes
	ICJS	2002	–	Outsource	Yes
Brazil	State IS	–	2010	In house and outsource	No
	Country IS	2010	–	In house	Yes
Belgium	Phenix	2001	2007	Outsource	No
Portugal	Habilus	–	–	In house	Yes
	SITAF	–	2004	In house	Yes
	CITIUS	2005	2008	In house	Yes
	CITIUS Plus	2010	–	In house	No
	SITAF 2.0	2011	–	In house	No
	AGIC	2011	–	In house	No

Portugal. In countries that started later, like Belgium or Brazil, the initial decision was immediately the web-based approach. This tendency is aligned with Fabri's findings. In [Fabri \(2007\)](#), the author describes this tendency within the case studies that he analyzed.

Focusing in [Table 2](#) on the systems' architecture column it is possible to verify that Portugal's information systems were designed based on different architectures. SITAF, for instance, is a distributed system, deployed with an installation in each administrative and fiscal court. This approach leads to smaller data repositories, but higher data interexchange between repositories. CITIUS information system follows the same approach: a distributed architecture with an installation for each court.

This type of architecture leads to a huge amount of scattered servers, since every court will require several servers (at least two, for redundancy) and a huge workload to update all the servers each time a system update is required. On the other hand, this architecture relies on a small need for interconnection among the courts. That means that a court can work normally even if the interconnection fails. The overall computational load on each server is very low.

All the recent information systems are centralized. This paradigm shift is once again associated with the factors mentioned in the previous analysis: both due to the evolution of the communication network, providing faster and more reliable communications and due to the hardware virtualization.

CITIUS Plus is a centralized system but with the possibility to work offline, providing leverage when the communication network fails. This feature increases the trust that users have in the information system, since they are assured of not losing the inserted data in case of a network failure.

Table 2
Features comparative analysis.

Country	Information system	Access type	Architecture	Offline work	Still working?
Singapore	ATOMS	Desktop	Centralized	No	Yes
	Desktop app	Desktop	–	–	No
	EFS	Web	–	–	Yes
	ICJS	Web	–	–	Yes
Brazil	State IS	Web	Centralized	–	No
	Country IS	Web	Centralized	–	Yes
Belgium Portugal	Phenix	Web	–	–	No
	Habilus	Desktop	–	No	Yes
	SITAF	Web	Distributed	No	Yes
	CITIUS	Web	Distributed	No	Yes
	CITIUS Plus	Web	Centralized	Yes	No
	SITAF 2.0	Web	–	–	No
	AGIC	Web	Centralized	–	No

4. On the modeling of e-government systems

In the e-government panorama, but still closely related to laws, there are also some relevant initiatives.

As an example, Austria developed a workflow management system for law management called eLaw. The base of the eLaw project was to provide access and help stakeholders during the definition or changes in the country's laws. With this system all stakeholders have access to the law under review, to all revisions and to their propositions in appropriate time, without conflicts in the responsibilities level, based on the concept of SoD (Separation of Duties) ([Schaad, Spadone, & Weichsel, 2005](#)). The SoD is a role-based access model, and these roles can be provided at a network level or at an operating system level or at the information system level.

With this information system, they prevent situations like (1) a single stakeholder completing all the steps necessary to create/change a law; (2) avoiding conflicts of interest, where a stakeholder submits a law review and has simultaneously the power to revoke/accept it; and (3) minimizing the confrontation risk between stakeholders, related with their responsibilities and competencies, avoiding public confrontation.

According to [Schaad et al. \(2005\)](#), the main benefits of this system are:

- 1 Increased visibility and transparency to the society, having more public information about the laws;
- 2 Decreased errors in law drafts, increasing the efficiency;
- 3 Decreased corruption, avoiding situations like (1) and (2);

Similar to Austria's initiative, Bungeni (Kiswahili word for "inside Parliament") is an initiative of UNDESA (United Nations Department of Economic and Social Affairs) ([UN DESA, 2012](#)) that enables the virtualization of parliament procedures. It shares the same benefits of the eLaw project, and at the time of this paper's writing, it will soon be available for test pilots.

Bungeni is an open source Parliamentary and Legislative Information System, "that aims at making Parliaments more open and accessible to citizens" ([Bungeni, 2012](#)). Its target are the African and the Latin American National Parliaments, in order to provide a digital solution for drafting, managing, consolidating and publishing legislative and parliament documents. The information system is based on a workflow management system, storing information using formats from open standards in XML and supported by a legal ontology.

As Ashok Hariharan presents ([Hariharan, 2012](#)), Bungeni is oriented to the user, with a user friendly text processor, although it is web based. Document's semantic meaning is implicit and added without user intervention. This tool can be modified to fit the specific needs of a national parliament.

At semantic level Bungeni uses the Akoma Ntoso ontology ([Akoma Ntoso, 2012](#)), a "simple technology-neutral electronic representations (in XML format) of parliamentary, legislative and judiciary documents". The Akoma Ntoso provides the ontology to promote the data interexchange between different providers, with the need to develop different data readers.

UNDESA is not the only organization working on legal standards. In fact, the Africa i-Parliaments Action Plan ([Africa i-Parliaments, 2012](#)) is member of a broader network, the LegalXML ([OASIS, 2008](#)), a working group focused on electronic filing of court documents. Also, since 2002 the LegalXML Group joined the OASIS consortium, which resulted in the OASIS LegalXML Group. The OASIS LegalXML group produces several open standards in some legal fields, like court filing, notary or legislative.

5. The Cape Verde experience

SIPP's design started in 2008 and the system was ready to be used by 2011. Following the actual tendencies in the development of e-justice information systems, its architecture is centralized and the

system's interface is web based. The information system is composed of two separate applications: the Workflow Service and the Web Application, as depicted in Fig. 9.

The workflow service is responsible for handling all the workflow related tasks, triggering and managing cross-workflow events. The main advantage of separating the business logic in workflows is the possibility of supporting simultaneously different workflows for the same process typology. This is important because when there is a legislative amendment, the new legal proceedings are initiated under the law but the legal proceedings that have not been completed or already filed maintain the procedure in force at the time of its development.

One of the features supported by the workflow service is the ability of versioning documents. Document versioning enables users to safely work on their documents online, saving changes and rolling back versions as needed. This feature tries to leverage between this e-justice information system and the traditional way to work with a case file, allowing the user to work on a given document online, just as if he was working on his regular document processing editor. In this case due to necessary care with the contents of the undisclosed document, the document is written and stored centrally in a secure way. With this approach the user has a tool that: (1) supports multiple versions of the same document; (2) does not require local storage, avoiding problems like document/computer theft or hardware failure and allowing the user to handle the document in different places but always maintaining the same safety criteria; and (3) has a secure mechanism that allows only the user to read and write on the working document.

SIPP applies a SoD policy, based on application roles. This feature is crucial to information system acceptance by the stakeholders and to increase the trust between users and the e-justice information system. This security enforcement allows the system to recognize the user role and actual permissions within a given case process and provides access to the process information only on the occasions foreseen on the Process Code.

Cape Verde being an archipelago, every island has to produce the electricity it needs. Unfortunately, electrical outages are frequent either by technical problems in electrical generation plants, or undersizing of the capacity of power plants, or simply lack of diesel to put the generators into operation. This is a liability to SIPP, because it can produce a service disruption, total or partial (depending on the outage location).

Cape Verde has a country wide governmental network that can be used in public facilities like schools, hospitals, courts, etc. The governmental network at the start of SIPP's project is depicted in Fig. 10. The two main cities are Praia, the capital on the Santiago Island, and Mindelo on S. Vicente Island and the connections among them are primordial. The 3rd most important island is Sal where the local economy is based on tourism. As illustrated, in the most remote islands and areas, this network has a very low connection speed. In the cases where the governmental network is not available or does not meet the desired connection speeds, users may contract private broadband DSL internet services, with download speeds of up to 4 Mbps.

In 2011, the Cape Verde authorities started a project to upgrade the governmental network to the latest broadband technology, linking all the islands in the country.

To secure data, we adopted the use of a PKI for the SIPP system. This PKI is based on a worldwide renowned Root CA, and the SIPP help desk team manages the issuing and revoking of certificates. Based on this PKI, users can sign final document versions and can encrypt and decrypt SIPP's working versions of documents, providing a bigger sense of security to the overall system.

SIPP has been in testing phase since June 2010, and will be put in production during 2012 in a definitive way as soon as the national parliament approves a legislative amendment that allows the processing and completion of legal proceedings electronically. The prototype's initial testing phase began in parallel with training the end users of the system: judges, prosecutors and judicial staff. The training was prepared with two distinct modules: (a) training of general ICT skills, and (b) specific training for each of the users of the system at his place of work and focusing on their specific needs. During the first training phase, the Justice agents received training in general ICT skills, like the use of productive tools, such as text processor or spreadsheet, e-mail, internet and document scanning. These general skills are the basics in using the SIPP information system, because the system is web based, with text processor features. The second phase of training plan was over SIPP. In this phase we use on-job assisted training, as discussed in Teixeira and Pinto (2012) so that the users could better understand how to accomplish several goals based on their courthouse roles. With this approach the users can practice with the new tool, and we can tune the information system, its interface and overall information processing, to better fit the real users' needs.

6. Risk factors

Justice systems work based on well-established procedures, carried out by justice related staff. These activities can be automated, standardized and computerized. E-justice information systems can help and ease the fulfillment of some of these tasks. However, as with all information systems, there are risk factors associated. In a so sensible area, like Justice, where people's future may be decided, the risk factors must be well known and considered.

Jaeger and Thompson (2003) present some risk factors in e-government information systems. They present challenges like:

1. providing reliable electricity and telecommunications networks;
2. issues related to language and communication;
3. good coordination between local, regional and national e-government initiatives;
4. the development of methods and performance indicators to assess the quality of e-services provided;
5. ensure the quality and utility of e-services provided;
6. the education of the general population for the benefits of use e-government services;
7. preventing the e-government from lessening responsiveness and responsibility of government officials.

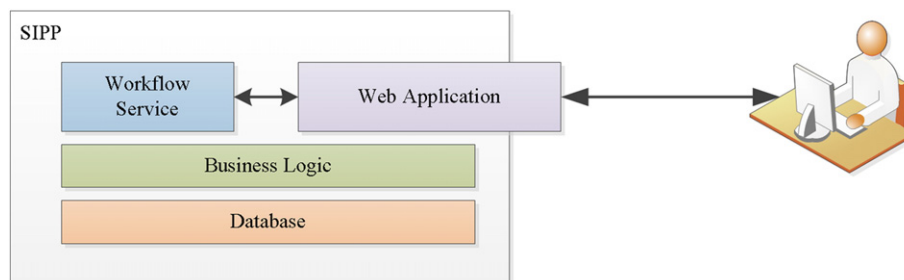
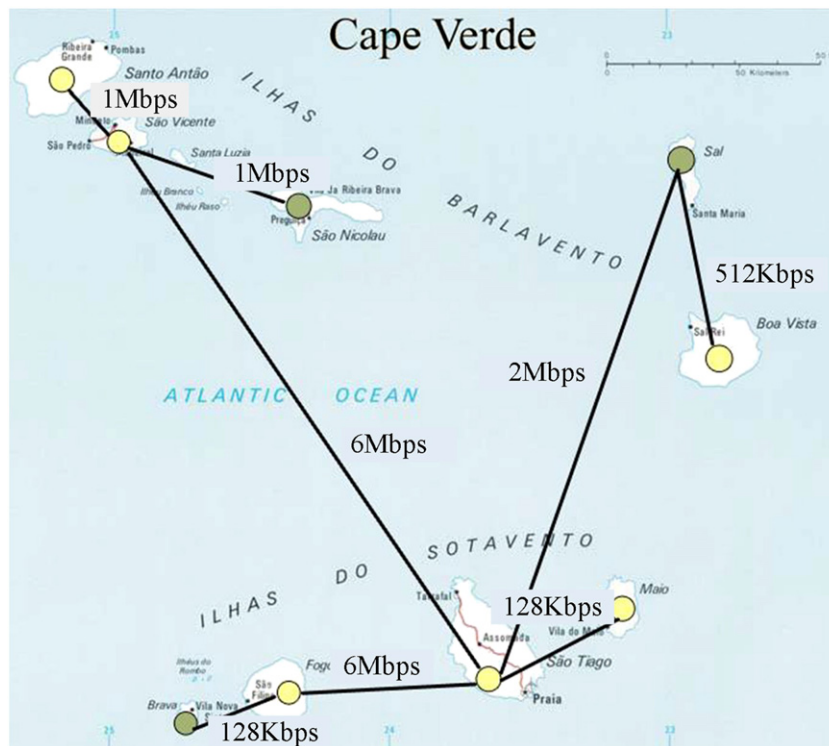


Fig. 9. SIPP's overall architecture.



Since e-justice information systems are a subset of the e-government information systems, they can be analyzed under the same issues.

Kuk's study (Kuk, 2003) concluded that the quality of e-services decreased due to poor or lack of internet access. Slow communication networks present a liability, because e-justice systems need to exchange high amounts of data, as official acts and documents with hundreds or thousands of pages, multimedia archives, like pictures of a crime scene, or live feeds from one court to another during trial, are some examples that can illustrate the added traffic over such network (Jaeger & Thompson, 2003; Kuk, 2003). As exposed in Section 2, governments of countries pointed as a key feature a good communication network. In a country like Singapore, it is easier to upgrade the communication network, because of the country's geography, and since it has one of the biggest GDP in the world. In a bigger country like Brazil, they adopted a strategy to upgrade the communications network between state capitals to 2 Gbps links and to ensure links between central courts and small claims courts in each state. In an archipelago like Cape Verde, the upgrade of the communications infrastructure is more complex than in continental countries. Each island must be considered separately and then it is necessary to plan an adequate inter-island infrastructure. For communicating within each island a type of WiMAX (Worldwide Interoperability for Microwave Access) infrastructure is being designed. Due to the curvature of the earth, it is impossible to establish radio links between the groups of islands in the North (S. Vicente, S. Antão and S. Nicolau) and in the South (Santiago, Maio, Fogo and Brava) nor Northeast (Sal and Boavista), so any update on the infrastructure will have to go through the placement of a set of physical paths between the groups of islands. According to current standards, this connection can be made into fiber optics or via a satellite link. The fiber optic link provides faster and cheaper communications than the satellite link and this is therefore used only as a backup system. Unfortunately the optical fiber path is often cut off by fishing boats nets leaving the communication between the islands dependent on satellite links.

Accurate planning of the design, development and maintenance stages of information systems presents a second risk factor, especially when working on a system that is designed to operate on a 24/7 basis. Also, when planning a substitution of legacy systems, or when new systems have to interact with such systems, the design team has to make a good evaluation of what the institution really needs. If the design and development teams do not take into consideration the changes occurred in the lapse of time between the original design and the upgrade, like the changes in the users' needs and the arrival of new technologies better fitted for a given task, this migration process will continue to develop over legacy software, possibly accumulating old mistakes. On the other hand, when dealing with the evolution of legacy systems, special care must be taken to understand and validate not only the previously business model rules, but also the new implementation of such rules. The same principle applies to the system's architecture: the evolution of a given system may or may not require a change in the application's architecture, depending on the users' and applications' needs. In Singapore, they evolved from desktop applications to web-based information systems because the justice system needed an information system with this architecture, with new technology. To mitigate this risk, SIPP has a modular architecture, as shown in [Fig. 9](#). This modularity, with clear distinction of presentation layer, business layer and process handling workflow layer, enables each layer to evolve accordingly to its needs. Given the constant evolution of the law, the workflows that regulate each process type may need to be changed. When such changes occur, depending of the type of change, there may be the need to simultaneously support the old process procedure regulations (for active processes) and the new process procedure regulations (for newly created processes). In other cases, the changes must be implemented in all the active workflow processes. The independence of the workflow layer enables us to make the necessary changes without affecting the other layers. During SIPP's development, there was a major change in the Criminal Code. One of the changes was a different way of calculating the proceedings costs of a given process. In terms of design and

development, this meant that there were several active rules or workflows for calculating costs, depending on parameters such as the filing date of the process.

The continuous development of new information systems poses another risk factor. If not properly conducted, it can create information systems islands and system fragmentation, with no data interexchange, which is vital in the Justice area. This situation occurred in Brazil, where they developed a national information system, but allowed the existence of custom information systems at the court level.

Still on the new information systems development subject, it is necessary to account for the interoperability within the country's e-government systems. Systems may require access to citizen's information, such as personal data, fiscal data or criminal record. This information must not be concentrated in one huge information system, but in smaller, dedicated information systems, with interfaces for authorized systems to query information. When systems are not capable of exchanging information with others, data and development efforts are doubled, making this a huge implementation risk, as stated by Fabri (2007).

There is also a risk that derives directly from enabling information exchange among systems: data confidentiality. With all our data available for query by other systems, what are the guarantees offered to the citizens, in terms of data protection? To minimize the exposure to such risk, and in the event of database attacks, we decided that it would be best to make data anonymous, by using local identifiers as a mere reference to the original information. This way, whenever we require the original citizen's information, our system will use the local identifier to request it to its original system holder. Since the identifiers (local and remote) differ, the attacker's will not have a direct, ease to link path among databases. This data protection mechanism increments the bandwidth consumption, but guarantees up to date information concerning the citizen.

In terms of system development and project leadership, conflicts among stakeholders may arise due to:

- the lack of knowledge on organized development efforts that try to answer the problems for different stakeholders, misleading a group of stakeholders to embrace an unnecessary second development effort
- the lack of perspectives on the development of an information system for all stakeholders, a group of stakeholders embrace an independent development of an information system to help solving their problems.

This situation happened in Portugal, where the ASJP tried to impose an information system to the courts – Tribunal XXI (Abrantes, 2005; Microsoft, 2005), without discussing the project with authorities and other stakeholders involved in the Justice. At the same time that the ASJP announced the Tribunal XXI, national authorities were planning and designing CITIUS that was soon released. CITIUS had a broader range in features and addressed more stakeholders, so ASJP's project was dropped. The abandoning of the ASJP project generated a considerable amount of users strongly against CITIUS, mainly from within members of that association.

Despite the inclusion of the end users' representatives in the production process being considered as a positive approach, if their influence in the process is overwhelming, then that is not so positive. This was reported by Langbroek and Tjaden (2009), concerning a Dutch project failure. The Dutchmen tried to develop a separated workflow management system for the appeals from the first instance court to the appeal courts, but it was called a failure in 2001 and had a cost of 13 million euros. The very same case is referred by Fabri (2007), where he points the lack of communication among the stakeholders as a possible reason for project failure in development or implementation phases.

Given such experience, and considering the overall benefits of having experienced stakeholders on the design team, the SIPP's design

team included representatives of judges, prosecutors and secretary staff, among others. With these members in the design team, the development team had more input and feedback from the users, and was able to develop and tune a prototype more accurate and closer to the users' perspectives. This prototype was then used in the meetings between the members of the design team, as a follow up and demonstration of the concepts already specified. This approach favored the discussion between peers with different visions about the necessary steps and data to fulfill a given task using the prototype. Using the stakeholder's visions on how to fulfill such task, the software architects were able to propose working approaches and operation steps with which all stakeholders would feel comfortable. Besides the practical advantages of such heterogeneous design team, the involvement of these stakeholders since the beginning enables them to see their ideas being implemented. This produces, more than a responsibility for what is implemented, an ownership (almost paternity like) feeling towards the system: With such feeling, the involved stakeholders would be excited and compelled to spread the word to their colleagues and defend the system's benefits from potential critics. This evangelism tends to provide better acceptance results than the mere imposition by ranks or by foreign agents. In SIPP, one of the follow-throughs of this feeling is the writing, by secretary members of the specialist group, of an annotated version of the Code of Process Cost. These members have been of invaluable help to accurately calculate all the different cost variations around the proceedings costs. With this task, they were even able to find inaccuracies on traditional calculation boards. Given their experience and insurance by SIPP's calculation engine, they have embraced the challenge of producing a book about the calculation of a process costs, according to the new Code. This annotated Code of Process Cost will explain the new rules and use SIPP's calculation engine and user interface to provide graphical examples. Similar challenges have been launched to the judges and prosecutors members of the specialists group.

From the user's point of view, the applications should adapt to the users and not the other way around. Poorly assembled UIs (User Interfaces) that do not follow accessibility and usability heuristics can be a nightmare to work with. The way data are organized and displayed is also an important factor. If the digital metaphor for process and document navigation is confused with mixed legal terms and wrong taxonomy, users can waste time, decreasing efficiency and productivity. These issues combined with traditional backlog problems can drag even more the process procedures. In our experience, and based on the previous issue, SIPP's prototype covers this risk. During the design meetings, the different inputs from the stakeholders allowed to tune the UI. This methodology ensured a better user experience to handle the different tasks involved in the system. The testing phase consolidated the prototype, and the number of potentials issues with SIPP decreased with the increase of the tests' feedback.

Interface and information presentation considerations may be extended to the printed versions of electronically submitted data. In this case, this information may be presented in a standardized way, regardless of its point of origin. In an effort to standardize documents in SIPP, the specialists participating in the design meetings proposed new document layouts and information templates to be used in the system. These layouts and templates were implemented, presented to the test users and refined to better suite everyone's perception of the information necessary within each document type. One of the most disruptive layouts presented was in fact the most applauded: the process cover. Traditionally, for each process phase the process would "gain" a need cover, that would be placed on top of the others. With a digital process, there is no need to replace covers. The new printed cover will contain the new information. On top of the traditional information already existing on paper, we added a new concept to the cover: a general process activity overview, with indication of dates and actions carried out. This way anyone holding a physical

copy of a process within SIPP can have a general idea of what has been going on in the process, without having to open it.

As referred, these information systems must work 24 h per day, 7 days per week. Thus, the infrastructure must be flexible, redundant and capable of recovery in case of disaster. Plans to recover in case of disaster must be taken, especially if there is the need to invest on building datacenters or buying more equipment for them. These decisions should consider the datacenter's nature and its goals. Questions about the location, the surrounding geography or geology and the likelihood of natural disasters should be analyzed carefully and fairly evaluated, since the data in these datacenters is vital. Another important decision is the amount of data that managers are aware that may be lost in the event of a disaster that might occur between backup operations. The answer to these questions should help on planning backup and restore solutions. In the Belgium case study, one reason pointed by the technical team as a major challenge was the catastrophic recovery scenario, and maybe for that unsolved reason the government stopped the project.

Good practice manuals refer that a secondary server, geographically distant from the main site, should be implemented to handle catastrophic situations where the main site is unavailable. Regular backups should also be transferred for this site. The computing resources on the secondary site may be more modest than the primary site. This site should activate itself, using the latest backups available, upon detecting the failure on the primary site. For SIPP we have implemented a secondary site on a different island. Regular database backups are transferred for the site.

Not only the communication network is a concern, but also the electrical network is important. These infrastructure networks need to be consistent and reliable. Electrical power is something that western citizens take almost for granted. However, in African developing countries, on islands with no rivers to build hydroelectric dams on and with wind and solar generators still scarce, the population is almost entirely supplied by diesel run public powerhouses. In Cape Verde, it is common to be without any electrical power for more than 24 h. In this case, the preventive measure was to ensure that the datacenter would have a backup generator, capable of running uninterruptedly for long periods. However, this measure covers only the datacenter. If a courthouse is without electricity, it will be unable to access SIPP. To solve this issue, the Cape Verde authorities have a project sponsored by the World Bank to upgrade the national electrical network, reducing the waste of energy and water, and reducing the oil dependency (*Radiotelevisão Caboverdiana*, 2012).

Data handling is a big issue on e-justice systems. As exposed in the case studies, all countries have concerns with their system's data security, integrity and confidentiality. These concerns target not only the datacenter and network security, by using firewalls, VPNs, and controlling the physical and virtual accesses, but they also target data and documents integrity. To ensure the user's identity, most case studies rely on a PKI. By using a PKI, data and documents can be digitally signed and verified, ensuring non-repudiation, integrity and authentication. This is vital because these data and documents have legal validity, and these decisions have impact on society. In this paper we analyzed two different PKI approaches. Singapore relies on a commercial PKI to issue certificate valid for the justice system, and Portugal and Brazil use the existent national PKI. The second approach has more risks, with protestors arguing that such PKI is a government initiative, and that in democracy the Justice and Government are separated. This conflict arose in Brazil, where the National Bar Association tried to stop the use of the national PKI. When using a PKI, documents and data can be ciphered/deciphered, increasing security. In Belgium they did not use this approach. In fact, they did not use any approach and pointed this as a problem to be solved. The lack of solution for such problem poses a huge security risk, which, along with the remaining threats found, put the Phenix's development to a halt. As with Singapore, SIPP relies on a commercial PKI to issue its certificates.

In the Justice system, Justice agents have different duties, and each duty has different requirements and needs. For example, a judge makes decisions and a court officer executes them. Based on that, e-justice systems have risks related to the execution of duties or actions and related to the permission of performing a task, or accessing a certain feature. To increase the trust in e-justice systems, these usually implement a SoD that works properly and ensures that the tasks and features available to the user at a given time are just the ones that he may execute. Similar to the Austrian eLaw system, SIPP implements a SoD based on application roles, separating the different duties related to the same process procedure type, and regulating the access to the different features when handling a process. The SoD concept is applied independently on the interface layer and on the data layer, with the user's identification being required when accessing the data layer. This way, the internal logical services can crosscheck if the given user is in fact entitled to perform the desired operation.

The introduction of IT in the justice system must also be considered as a risk factor. The simple usage of an information system to support regular operations must be legislated. These law changes are vital for the daily use of e-justice information systems, since the decisions made using them will have the same legal value of the paper based decisions. All of the case studies presented changed their laws to support the use of an information system to process procedures electronically. Currently, Cape Verdean authorities are preparing the necessary changes to the Law to introduce SIPP as a legally valid system to handle case files.

As with any fairly complex information systems development, for developing an e-justice system it is crucial to have a good and solid multidisciplinary team. Given its specificities, more than an overall picture of the system, the IT design team must have the ability to integrate and understand the inherent justice concepts. To better support the system's design, this team must integrate the representatives of as much justice stakeholders as possible, in an effort to cover the different points of view of what the system should/will be. It is important to have the fragmented vision from judges, prosecutors, lawyers and court officers, because they will use the system on a daily basis. Having these stakeholders in the developing team can help to understand each stakeholder's individual needs and to clarify the borderline interactions, avoiding future misunderstandings.

The type of the development (in-house or outsourced) can influence the information system's maintainability. This is a risk factor to consider, since it influences the long term support of any information system (from regular maintenance operations to the development of new features or bug corrections). In Portugal the several information systems were developed in-house, with the maintainability and the long term support ensured by the hired teams. In Singapore there was a shift from in-house development to outsourcing, with the outsourcing company resulting from a spin-off from the in-house development, so the information system knowledge necessary to support and maintain the system was therefore ensured.

The SIPP's project managers' initial idea was to follow the Singapore's development model, where a spin-off holding the knowledge of the development of the system would be created to support it. However, unlike Singapore, the initial development team was composed of two universities, Cape Verde University and Aveiro University. The reason to include two universities was twofold: the SIPP's development and the national knowledge capacity of the Cape Verde University. The Cape Verde University was at the time on its year one, and was struggling to find people with technical and academic background capable of teaching new classes. This struggle had impact on satellite projects where the Cape Verde University should be involved, such as the SIPP's development, because it was unable to hire additional staff to be exclusively dedicated to this project. Given this reality, the responsibility over the project's development lied solely on the University of Aveiro. This change had impact on the initial expectations regarding the system's

support: the spin-off should result from local knowledge acquired during the development of the system; and at this point, such knowledge can only be found within the University of Aveiro, in Portugal. Considering that the development is being made by a university, whose goal is to teach and research (and not to provide support) and that the creation of a spin-off to provide support overseas may not be feasible, the long term support to the system is still not guaranteed. This is an open issue that needs to be addressed by the system's managers as soon as possible.

Another associated risk factor is the IT skills from justice agents. These skills can be classified in two different aspects: (1) general ICT skills and (2) specific e-justice information system skills. A user lacks general ICT skills when he struggles on tasks like working with productivity tools, such as a text processor or spreadsheet, understanding how to use an e-mail client or on how to take advantage of search engines and internet websites. The specific information system skills relate to the understanding of the digital metaphor used to mimic the traditional process handling and to the grasp of the system's features. To avoid and minimize this risk, measures may be taken to help users to better use the system. This may be accomplished with end user training. Considering the end-user training methods review made by Gupta and Bostrom (2006), the planning of a training session must have in mind the targeted system or software. Given the requirements in general ICT knowledge and in system specific knowledge, training efforts should be divided in two distinct areas: a training plan to provide general ICT skills and a second training plan on the use of the information system. These plans should be incremental, and the success of the user's training measured in terms of learning outcomes. Depending on such outcomes, users may start the second training phase, or repeat (entirely or partially) the first training phase.

The second training phase in SIPP involved the understanding of the visual representation of processes' information and how to accomplish the required tasks. This phase is an ongoing process that tries to closely follow the development of the prototype system and enables us, as developers, to take action and rapidly adapt the interfaces upon user's feedback.

With the use of digital technologies, is easier to ignore parts of an e-mail or other digital document, not intentionally, but inadvertently (Jaeger & Thompson, 2003). This risk can compromise the public service provided to the society by the Justice, simply because the Justice agent is less responsive to citizens. Considering that in the digital world user's desks are not clogged with stacks of paper, it may be easy to miss important tasks. To minimize this liability, SIPP's interface presents at all times the tasks under the user's responsibility. Tasks are presented with a color code to better visualize its urgency.

Another risk related to information system's usage is relying in the information system, avoiding taking responsibilities related to their duties. Information systems are a tool to help with the work, to accomplish their tasks, but they do not replace the human intervention. Therefore, users involved with the information system must be aware and educated to change their mindset to the digital world, where the physical presence (of both people and case files) component is suppressed, so that the service quality may be the same (and preferably better) as if they were physically present.

Last but not least, the society needs to be aware of the benefits (Jaeger & Thompson, 2003) of the e-government initiative in general, and of the e-justice in particular. If these information systems have good quality, with features that are really needed, and with clear benefits in efficiency, citizens are impelled to take advantage of e-government information systems. This leads to a decrease in corruption, increasing the transparency between governments and society, creating more stable governance conditions. The people of Cape Verde spread over 9 islands (domestically) and have an estimated overseas community bigger than the Cape Verde inhabitants. This high level of community spread forced authorities to embrace technology enabled solutions that could reduce the distance between government service providers and citizens, making Cape Verde the 21st country (out of 53)

in the 2008 African e-Government ranking produced by Rorissa and Demissie (2010). The United Nations' 2008 report (United Nations, 2008) places Cape Verde as the leader of the E-Government Readiness for West Africa, which translates to the 6th place on the top ranked countries in Africa and to the 104th place of the overall E-Government Readiness Index 2008, indexed at 0.4158. More recently, the United Nations E-Government Survey 2010 (United Nations, 2010) places Cape Verde in the 6th position of the top ranked countries in Africa, making the 108th place of the World E-Government Development Ranking 2010, indexed at 0.4054. In the same report, Cape Verde ranks 92nd (of 189) on the Online Service Index and ranks 68th (of 157) on the e-participation index. In the United Nations e-Government Survey 2012 (United Nations, 2012), Cape Verde kept both the 1st position on the e-government development in Western Africa and the 6th place on the top ranked countries in Africa, with the 118th position in the World E-Government Development Ranking 2012, indexed at 0.4297. In the same report, Cape Verde ranks 89th in the Online Service Index and 23rd on the e-participation index. Cape Verde's evolution in terms of overall index (from 0.4158 to 0.4297) and of specific e-participation index (from 68th to 23rd) shows that the population, despite all the difficulties, is eager to take part and to take full advantage of the benefits of e-government initiative.

7. Conclusion and future work

This paper presented several approaches to worldwide experiences in the design, development and implementation of e-justice information systems. Upon evaluation of the case studies' outcome and what was crucial for such outcome, we presented SIPP, the e-justice system designed and implemented for the Cape Verde Justice.

Based on those experiences, we enumerated a set of risk factors associated with the development and implementation of such systems. Despite the experiences being worldwide, in different countries with different contexts, we demonstrated that they share the same risks factors.

One of the major risk factors is the initial design phase and the continuous development scrutiny. If the initial architecture is poorly planned due to misinterpretations of the requirements, the entire project may be at risk. Continuous scrutiny and presentation of working prototypes to the stakeholders will enable rapid corrections of any misinterpretations. Also, these prototypes give stakeholders and future users a preview of the overall system. With such preview, initial user expectations can be better understood and, if required, the development and design teams can make rapid behavior and user interface changes to better align with the users' point of view.

From the presented case studies, one of the least consistent parameters evaluated is the development team type: in-house or outsource. This lack of consistency is probably related with the country's philosophy and historical background on similar initiatives. More than the development model, the subsequent maintenance model adopted may also be of significant impact in terms of support and development of new features. As illustrated by the case studies presented, both models may succeed or fail, depending on factors as the overall information vision, leadership and technical skills. SIPP's maintenance model is still to be determined, since application maintenance support is not within the university's goals.

In e-justice systems, the knowledge gap between the design team and the users may impair the entire system. To handle such liability, the work performed by the design and development teams should be followed closely by a party of the different types of users that will use the system. During the development of SIPP, the design team performed extensive meetings with a group of specialists of the different areas: judges, prosecutors and secretary staff. To better interface with the design team, the development team and this specialist group, we included a specialist with legal background from University of Aveiro, that would act as a "translator" for complex

legal questions (for the IT teams) and also as a “translator” for some information system related aspects (for the specialist group).

The introduction of information systems as a tool to help in an organization structure changes the organization itself. People in the organization have to be aware of these changes. To avoid shocks related to the use of new information systems, people should take part in training sessions. The training sessions should cover two aspects: general ICT skills and specific information system skills. When the users' skills concerning general ICT reaches a given goal level, users may advance for the next phase (Teixeira & Pinto, 2012). Specific information system training must provide users skills on how to accomplish their day-to-day tasks using the system. Considering that systems evolve and users tend to forget some of the previously learnt abilities, the training plans should be refreshed when needed.

To what concerns the network infrastructure, all case studies pointed as a key feature a good and reliable communication infrastructure. The increase of volume of data interchange mandates a reliable network infrastructure, mainly due to features such as video conference and to the spread and mandatory use of e-justice information systems. In Cape Verde they are upgrading the governmental network to the latest technology in broadband network, covering almost all islands. With this investment, all islands may use the e-justice information system without the need of using commercial DSL connections, thus helping on lowering the operational costs of the justice system.

After the design, development and implementation of SIPP, we started the design and development of the continuation of Cape Verde's e-justice information system. This new iteration will enable the digital handing of civil matters, based on the Civil Process Code, and relying on the framework developed for SIPP.

References

- Abrantes, M. (December 20). Câmara Corporativa: “Tribunal XXI”. Retrieved May 8, 2012 from <http://corporacoes.blogspot.pt/2005/12/tribunal-xxi.html>.
- Africa i-Parliaments (2012). Africa i-Parliaments – Site. (Africa i-Parliaments). Retrieved April 14, 2012 from <http://www.parliaments.info/>.
- Akoma Ntoso (2012). Akoma Ntoso – Site. (Akoma Ntoso). Retrieved April 14, 2012, from <http://www.akomantoso.org/>.
- Andrade, A., & Joia, L. (2010). Organizational structure and ICT strategies in the Brazilian Justice. *Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance ICEGOV '10*. Pequim.
- Barra, M. C. (2006). *Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) e a Formação do Estado Eletrônico. Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) e a Formação do Estado Eletrônico*, 261, Brasília, Brasil: Universidade de Brasília, Instituto de Ciências Sociais, Departamento de Sociologia.
- Bungeni (2012). Bungeni – Site. (Bungeni). Retrieved April 14, 2012 from <http://www.bungeni.org>.
- Coelho, M. A. (November 1 – 4). ICP-Brasil – The Brazilian PKI. *Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards*. Montréal, Canada: International Civil Aviation Organization.
- Conselho Nacional de Justiça (2013). “Portal CNJ - Relatórios,”. Retrieved 16 January 2013, from <http://www.cnj.jus.br/programas-de-a-a-z/eficiencia-modernizacao-e-transparencia/pj-justica-em-numeros/relatorios>
- Conselho Superior da Magistratura Judicial (2010). *Relatório sobre a situação da Justiça*. Praia, Cabo Verde: Conselho Superior da Magistratura Judicial.
- Direcção-Geral da Política de Justiça (2005). *Breve Guia Prático do SITAF. Reforma do Contencioso Administrativo*. Lisboa, Portugal: Direcção-Geral da Política de Justiça. (Retrieved November 21, 2011, from http://rca.meticube.com/_RCA/Documents/GuiaSITAF.pdf).
- Economist Intelligence Unit (2011). *Democracy index 2011*. London: Economist Intelligence Unit.
- Fabri, M. (2007). Comparing the use of information and communication technologies in European Public Prosecution Offices. *Information and communication technology for the public prosecutor's office* (pp. 1–28). Bologna: Clueb s.c.a.r.l ISBN: 978-88-491-3037-9.
- Gabinete de Acompanhamento da Informatização nos Tribunais (GAIT/ASJP) (2009). *Primeiros Seis Meses de Utilização do CITIUS - Inquérito de Avaliação à Funcionalidade e Eficiência - Relatório Preliminar*. Associação Sindical dos Juizes Portugueses Lisboa: Associação Sindical dos Juizes Portugueses.
- Gupta, S., & Bostrom, R. P. (2006). *End-user training methods. Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research*. Forty four years of computer personnel research: achievements, challenges & the future – SIGMIS CPR '06. New York, New York, USA: ACM Press, 172 <http://dx.doi.org/10.1145/1125170.1125217>.
- Hariharan, A. (2012). *Legislative XML creation with Bungeni editor. Achieving Greater Transparency in Legislatures through the Use of Open Document Standards* (Washington D. C. Retrieved from <http://www.ictparliament.org/attachements/XMLmeeting/Day2B2-Hariharan.pdf>).
- Instituto das Tecnologias de Informação na Justiça (2004). *Sistema de Informação dos Tribunais Administrativos e Fiscais - SITAF*. Lisboa: Instituto de Informática - Ministério das Finanças. Retrieved November 21, 2011, from Prémio Fernandes Costa - Edição de 2004 - Instituto de Informática. http://www.inst-informatica.pt/o-instituto/resenha-historica/eventos/premio-fernandes-costa/premio-fernandes-costa-edicao-de-2004/2004_SITAF.pdf.
- Instituto Nacional de Estatística de Cabo Verde (2011). *Apresentação dos Resultados Definitivos do Recenseamento Geral da População e Habitação - RGPH 2010*. Praia, Cabo Verde: INECV.
- ITI (November 17). Estruturalcp < Certificacao < TWiki. Retrieved November 19, 2011, from http://www.iti.gov.br/twiki/pub/Certificacao/Estruturalcp/Estrutura_completa.pdf.
- Jaeger, P. T., & Thompson, K. M. (2003). E-government around the world: Lessons, challenges, and future directions. *Government Information Quarterly*, 20, 389–394.
- Kuk, G. (2003). the digital divide and the quality of electronic service delivery in local government in the United Kingdom. *Government Information Quarterly*, 353–363.
- Langbroek, P. M., & Tjaden, M. I. (2009). Organising data exchange in the Dutch criminal justice chain. *Transylvanian Review of Administrative Sciences*, 28(Special Issue), 8–26.
- Magnus, R. (1999). *e-Justice: The Singapore Story*. Singapore: National Center for State Courts.
- Martínez, A. C., & Abat, P. F. (Eds.). (2009). *E-Justice: Information and Communication Technologies in the Court System*. Hershey, Pennsylvania, United States of America: IGI Global.
- Microsoft (November 23). Microsoft Imprensa|Comunicados. (Microsoft). Retrieved May 9, 2012 from <http://www.microsoft.com/portugal/presspass/comunicados.aspx?ID=65>.
- Ministério da Justiça (Dezembro 30). *Diário da República - I Série B, Portaria n.º 1417/2003 de 30 de Dezembro de 2003*. Lisboa, Portugal: Imprensa Nacional - Casa da Moeda.
- Ministério da Justiça (2008a). *Diário da República, 1.ª série - N.º 118, Portaria n.º 457/2008 de 20 de Junho de 2008*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Ministério da Justiça (2008b). *Diário da República, 1.ª série - N.º 26, Portaria n.º 114/2008 de 6 de Fevereiro de 2008*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Ministério da Justiça (2010a). *Diário da República, 1.ª série - N.º 131, Portaria n.º 471/2010 de 8 de Julho de 2010*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Ministério da Justiça (2010b). *Diário da República, 1.ª série - N.º 68, Portaria n.º 195-A/2010 de 8 de Abril de 2010*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Neves, C. (2009). O CITIUS: legalmente opcional, mas praticamente indispensável. *Boletim da Ordem dos Advogados* (60/61), 54–56.
- OASIS (2008). Legal XML. (OASIS) Retrieved November 2011, 23, from <http://www.legalxml.org/>.
- OECD (2003). *The e-Government Imperative*. Paris, France: OECD Publications Service. <http://dx.doi.org/10.1787/19901054>.
- Orzessek, M., & Sommer, P. (1997). *ATM & MPEG-2: Integrating Digital Video Into Broadband Networks* (1 ed.). Upper Saddle River, New Jersey, Estados Unidos da América: Prentice Hall.
- Presidência do Conselho de Ministros (2006). *Diário da República - I Série-A, Decreto-Lei n.º 116-A/2006 de 16 de Junho de 2006*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Presidência do Conselho de Ministros (2011). *Diário da República, 1.ª série - N.º 45 - 4 de Março de 2011*. Lisboa: Imprensa Nacional - Casa da Moeda.
- Rádiatelevisão Caboverdiana (February 4). Banco Mundial empresta 40 milhões de euros a Cabo Verde para reforma do sector da energia. Retrieved April 23, 2012, from http://www.rtc.cv/index.php?paginas=13&id_cod=15781.
- Rorissa, A., & Demissie, D. (2010). An analysis of African e-Government service websites. *Government Information Quarterly*, 27(2), 161–169.
- Santos, B. S. (2005). Os tribunais e as novas tecnologias de comunicação e de informação. *Sociologias*, 7(13), 82–109. <http://dx.doi.org/10.1590/S1517-45222005000100004>.
- Schaad, A., Spadone, P., & Weichsel, H. (2005). *A case study of separation of duty properties in the context of the Austrian “elaw” process*.
- SIC (2011). *Jornal da Noite Edição 13-12-2011 (1ª parte)*. Lisboa: SIC (Retrieved from <http://sicnoticias.sapo.pt/programas/jornaldanoite/article1059819.ece?option=writcomment>).
- Silva, M. (Maio 4). A Informática nos Tribunais. Retrieved November 2008, 3, from <http://noticia.nesi.com.pt/?p=189>
- Singapore Network Services Pte Ltd (Junho 15). Break through with CrimsonLogic - it makes better sense. Retrieved October 26, 2011, from <http://info.efs.com.sg/Download/WKCGSGUrr.PDF>.
- Subordinate Courts. (n.d.). Years In Review. Retrieved Outubro 18, 2011, from <http://app.subcourts.gov.sg/Data/Files/Media/YearsInReview.wmv>.
- Teixeira, C., & Pinto, J. S. (2012). Assisted on job training. In S. Kofuji (Ed.), *E-Learning/Book 4*. InTech.
- TelecomSpace (2011). *Asynchronous Transfer Mode|TelecomSpace. (TelecomSpace)*. (Retrieved Outubro 19, 2011).
- UN DESA (2012). UN DESA|United Nations Department of Economic and Social Affairs. (UN DESA) Retrieved April 14, 2012, from http://www.un.org/en/development/desa/index.html?utm_source=redirect&utm_medium=online&utm_campaign=redirect
- United Nations (2008). *E-Government Survey 2008*. New York: United Nations.
- United Nations (2010). *E-Government Survey 2010*. New York: United Nations.
- United Nations (2012). *E-Government Survey 2012*. New York: United Nations.
- Velicogna, M. (2007). Justice systems and ICT. What can be learned from Europe? *Utrecht Law Review*, 3(1), 129–147.

- Velicogna, M., Errera, A., & Derlange, S. (2011). e-Justice in France: the e-Barreau experience. *Utrecht Law Review*, 7(1), 163–187.
- Vuyst, B., & Fairchild, A. (2006). The Phenix project: a case study of e-justice in Belgium. *ICEC '06 Proceedings of the 8th international conference on Electronic commerce*. Fredericton, New Brunswick.
- Wever, W. (2009). E-justice perspectives at the GCC. *15th GCC e-Government and e-Services Forum*. Dubai.

João Rosa, MSc student in Masters in Information Systems.

Research interests: System modeling and architecture, workflow based systems, semantic web and e-government.

Cláudio Teixeira, Assistant researcher, PhD in Computer Science (2009); 5 year Degree in Telematics and Computers Engineering (2003).

Research interests: Integration of information systems, value added services, system modeling and architecture, XML based information systems, dynamically configured web portals, cloud computing and e-government.

Joaquim Sousa Pinto, Assistant Professor, PhD in Electronics Engineering (1997); 5 year Degree in Electronics and Telecommunications Engineering (1985).

Research interests: Digital Libraries, Information Systems, Cloud Computing.