

Concursos de Projectos de I&D Proposals for R&D Projects

► [Voltar à descrição do projecto](#)
Back to project description

► [Instruções para consultar e imprimir esta página](#)
Instructions to view and print this page

► [Imprimir esta página](#)
Print this page

Visão global da candidatura

Application form overview

(**Nota importante:** Atenção que o formulário desta página não é o requerido para a formalização da candidatura. Para esse efeito deverá ser impresso o FORMULÁRIO PRÓPRIO DE CANDIDATURA FEDER, já preenchido pela aplicação, disponibilizado no acto de lacragem juntamente com o TERMO DE RESPONSABILIDADE)

(**Important notice:** The application form available in this page is not appropriate for formal submission. For that purpose use the FORMULÁRIO PRÓPRIO DE CANDIDATURA FEDER, already filled in by the system, available at the act of submission together with the TERMO DE RESPONSABILIDADE.)

Ocultar todos os formulários da candidatura

Hide all forms for this application

Referência do projecto

Project reference

POSI/EIA/57038/2004

1. Identificação do projecto

1. Project description

Financiamento solicitado

Requested funding

98.076,00 Euros

Área científica principal

Main Area

Engenharia Informática

No caso de considerar imprescindível a avaliação do seu projecto numa outra área científica proponha qual:

Área científica Secundária

Secondary area

Título do projecto (em português) 

Project title (in portuguese)

E-Voto - Uma Nova Arquitectura para Lidar com o Risco em Sistemas de E-Voto

Título do projecto (em inglês)

Project title (in english)

E-Voting – A new Architectural Framework for Handling Risk in E-Voting Systems

Palavra-chave 1 

Votação Electrónica

Keyword 1

Electronic Voting

Palavra-chave 2

Sistemas Eleitorais Nacionais

Keyword 2

National Election Systems

Palavra-chave 3

Sistemas Complexos

Keyword 3

Complex Systems

Palavra-chave 4

Riscos de Sistemas

Keyword 4

Systems Risks

Objectivos sócio-económicos

Socio-economic objectives

Indústria - Equipamento e aparelhos electrónicos

Data de início do projecto

Starting date

01-01-2005

Duração do projecto em meses 

Duration in months

36

2. Instituições participantes

2. Participating institutions

-

Instituição Proponente

Principal Contractor

Fundação da Faculdade de Ciências (FFC/FC/UL)

Campo Grande - Edifício C4
1700-066Lisboa

Instituições Participantes

Participating Institutions

Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática (ADETTI)

Edifício ISCTE - Avenida das Forças Armadas
1600-082Lisboa

Instituto das Tecnologias de Informação da Justiça (ITIJ/MJ)

Av. Casal Ribeiro, 16
1049-068Lisboa

Instituto de Engenharia de Sistemas e Computadores (INESC/IST/UTL)

Rua Alves Redol, 9
1000-029Lisboa

Instituto de Engenharia Electrónica e Telemática de Aveiro (IEETA/UA)

Campus Universitário de Santiago
3810-193Aveiro

Unidade de Investigação

Principal Research Unit

Laboratório de Sistemas Informáticos de Grande Escala (LASIGE/FC/UL)

Bloco C5, Piso 1, Campo Grande
1749-016Lisboa

Instituição de Acolhimento

Host Institution

Faculdade de Ciências (FC/UL)

Campo Grande - Edifício C5
1700-000Lisboa

3. Orçamento

3. Budget

-



Instituição Proponente

Principal Contractor

Fundação da Faculdade de Ciências

DESCRIÇÃO

DESCRIPTION

	2004	2005	2006	2007	2008	TOTAL
Recursos Humanos 	0	0	4620	0	0	4620
Human resources						
Missões 	0	1500	1500	3000	0	6000
Missions						
Consultores 	0	0	0	0	0	0
Consultants						
Aquisição de serviços e manutenção 	0	1000	500	500	0	2000
Acquisition of services and maintenance						
Outras despesas correntes 	0	1400	1400	1400	0	4200
Other current expenses						
Despesas gerais 	0	1080	1604	960	0	3644
Overheads						
Total despesas correntes	0	4980	9624	5860	0	20464
Total current expenses						
Equipamento 	0	2000	500	400	0	2900
Equipment						
TOTAL	0	6980	10124	6260	0	23364

Instituições Participantes

Participating Institutions

Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática

DESCRIÇÃO

DESCRIPTION	2004	2005	2006	2007	2008	TOTAL
Recursos Humanos Human resources	0	0	0	0	0	0
Missões Missions	0	1500	1500	3000	0	6000
Consultores Consultants	0	0	0	0	0	0
Aquisição de serviços e manutenção Acquisition of services and maintenance	0	1000	2810	2810	0	6620
Outras despesas correntes Other current expenses	0	400	400	400	0	1200
Despesas gerais Overheads	0	980	1042	1322	0	3344
Total despesas correntes Total current expenses	0	3880	5752	7532	0	17164
Equipamento Equipment	0	2000	500	400	0	2900
TOTAL	0	5880	6252	7932	0	20064

Instituto das Tecnologias de Informação da Justiça

DESCRIÇÃO DESCRIPTION	2004	2005	2006	2007	2008	TOTAL
Recursos Humanos Human resources	0	0	0	0	0	0
Missões Missions	0	1500	1500	3000	0	6000
Consultores Consultants	0	0	0	0	0	0
Aquisição de serviços e manutenção Acquisition of services and maintenance	0	500	500	1000	0	2000
Outras despesas correntes Other current expenses	0	400	400	400	0	1200
Despesas gerais Overheads	0	580	880	960	0	2420
Total despesas correntes Total current expenses	0	2980	3280	5360	0	11620
Equipamento Equipment	0	500	2000	400	0	2900
TOTAL	0	3480	5280	5760	0	14520

Instituto de Engenharia de Sistemas e Computadores

DESCRIÇÃO DESCRIPTION	2004	2005	2006	2007	2008	TOTAL
Recursos Humanos Human resources	0	4620	0	0	0	4620
Missões Missions	0	1500	1500	3000	0	6000
Consultores Consultants	0	0	0	0	0	0
Aquisição de serviços e manutenção Acquisition of services and maintenance	0	500	1000	500	0	2000
Outras despesas correntes Other current expenses	0	400	400	400	0	1200
Despesas gerais Overheads	0	1804	680	860	0	3344
Total despesas correntes Total current expenses	0	8824	3580	4760	0	17164
Equipamento Equipment	0	2000	500	400	0	2900
TOTAL	0	10824	4080	5160	0	20064

Instituto de Engenharia Electrónica e Telemática de Aveiro

DESCRIÇÃO DESCRIPTION	2004	2005	2006	2007	2008	TOTAL
Recursos Humanos Human resources	0	4620	0	0	0	4620
Missões Missions	0	1500	1500	3000	0	6000
Consultores Consultants	0	0	0	0	0	0

Aquisição de serviços e manutenção	0	500	1000	500	0	2000
Acquisition of services and maintenance						
Outras despesas correntes	0	400	400	400	0	1200
Other current expenses						
Despesas gerais	0	1804	680	860	0	3344
Overheads						
Total despesas correntes	0	8824	3580	4760	0	17164
Total current expenses						
Equipamento	0	2000	500	400	0	2900
Equipment						
TOTAL	0	10824	4080	5160	0	20064

Orçamento Global

Global budget

DESCRIÇÃO	2004	2005	2006	2007	2008	TOTAL
DESCRIÇÃO						
DESCRIPTION						
Recursos Humanos	0	9240	4620	0	0	13860
Human resources						
Missões	0	7500	7500	15000	0	30000
Missions						
Consultores	0	0	0	0	0	0
Consultants						
Aquisição de serviços e manutenção	0	3500	5810	5310	0	14620
Acquisition of services and maintenance						
Outras despesas correntes	0	3000	3000	3000	0	9000
Other current expenses						
Despesas gerais	0	6248	4886	4962	0	16096
Overheads						
Total despesas correntes	0	29488	25816	28272	0	83576
Total current expenses						
Equipamento	0	8500	4000	2000	0	14500
Equipment						
TOTAL	0	37988	29816	30272	0	98076

Plano de financiamento

Finance plan

DESCRIÇÃO	2004	2005	2006	2007	2008	TOTAL
DESCRIÇÃO						
DESCRIPTION						
Financiamento solicitado à FCT	0	37988	29816	30272	0	98076
Requested funding						
Financiamento próprio	0	0	0	0	0	0
Own funding						
Outro financiamento público	0	0	0	0	0	0
Other public-sector funding						
Outro financiamento privado	0	0	0	0	0	0
Other private funding						
Total do Projecto	0	37988	29816	30272	0	98076
Total of the project						

4. Justificação do orçamento

4. Budget justification

-

4.1. Justificação dos recursos humanos

4.1. Human resources justification

Tipo	Nº de pessoas	Duração	Custo envolvido (€)
(BIC) Bolsa de Iniciação à Investigação Científica	3	12	13860

Justificação

Three partners (FCUL, INESC and IEETA) will use one BIC each to work on tasks T1, T2 and T3, which address the security-related, usefulness-related and community-related risks. These tasks involve prototype development, and the BICs will be applied to support these particular activities.

Custo total: 13860

4.2. Justificação de missões

4.2. Mission justification

Tipo	Local	Nº de deslocações	Custo envolvido (€)
Participação em congressos	Europe/USA	20	30000

Justificação

Four missions are expected per partner (at a unitary cost of 1500 Euros) for the project duration. These missions will support the dissemination of the project results in significant international conferences.

Custo total: 30000

4.3. Justificação de consultores **7**

4.3. Consultants justification

(vazio)

(void)

4.4. Justificação de aquisição de serviços e manutenção **7**

4.4. Acquisition of services and maintenance justification

Tipo	Custo envolvido (€)
Services	14620

Justificação

One partner (ADETTI) will be involved in prototype development in tasks T2 and T3 and will contract external services to support these activities, at a cost that was set to be equal to a BIC (4620 Euro). Other service costs are residual and will cover mostly PC maintenance: 500 Euros per partner/year (1000 when prototype development efforts are more substantial).

Custo total: 14620

4.5. Justificação de outras despesas correntes **7**

4.5. Current expenses justification

Tipo de despesa	Custo envolvido (€)
Current expenses	9000

Justificação

The proposed costs per partner are residual: 400 Euros per year (except the coordinator, with additional 1000 Euros). Most of these expenses cover the acquisition of bibliography, express mail, etc.

Custo total: 9000

4.6. Justificação do Equipamento **7**

4.6. Equipment justification

4.6.1. Equipamento já disponível para a execução do projecto

4.6.1 Available equipment

(vazio)

(void)

4.6.2. Discriminação do equipamento a adquirir

4.6.2. List of new equipment requested

Tipo de equipamento	Fabricante	Modelo	Custo envolvido (€)
4 PCs	(white line)	Desktop	6000

Justificação

4 PCs (1 per partner) are necessary to support BICs (and external services provider, in the case of ADETTI) prototype development in tasks T1-4. The cost of a PC has been set at 1500 Euro.

TFT displays, PDA, etc.	Misc	Misc	8500
-------------------------	------	------	------

Justificação

The proposed costs per partner are residual: 500 Euros in the first 2 years and 400 Euros in the last year. They will cover miscellaneous equipment necessary for prototype development, like TFT displays, PDA, special keyboards, UPS or special PC boxes used in e-voting machines.

Custo total: 14500

5. Equipa de investigação

5. Research team

-

5.1 Lista de membros (13)

5.1. Members list (13)

Nome	Função	Grau académico	%tempo
Name	Role	Academic degree	%time
Pedro Alexandre de Mourão Antunes	Inv. Responsável	DOUTORAMENTO	25
João Manuel Macedo Ferreira Dias	Investigador	AGREGAÇÃO	10
Paulo Jorge Pires Ferreira	Investigador	DOUTORAMENTO	10
Luís Manuel Pinto da Rocha Afonso Car...	Investigador	DOUTORAMENTO	10
Carlos Manuel Jorge da Costa	Investigador	DOUTORAMENTO	10
Carlos Nuno da Cruz Ribeiro	Investigador	DOUTORAMENTO	10
Filipe José Ferreira Simões	Investigador	LICENCIATURA	30
CARLOS JOSÉ CORREDOURA SERRÃO	Investigador	MESTRADO	10
Rui Luís Rocha Pinto	Investigador	LICENCIATURA	30
André Ventura da Cruz Marnôto Zúquete	Investigador	DOUTORAMENTO	10
Rui Filipe Lopes Joaquim	Investigador	LICENCIATURA	10
Oscar Manuel Martins Alves da Veiga	Outro		10
Maria Amélia dos Santos Damas	Outro		10

(O curriculum vitae de cada membro da equipa está disponível clicando no nome correspondente)

(Curriculum vitae for each research team member is available by clicking on the corresponding name)

5.2. Lista de membros a contratar durante a execução do projecto (3)

5.2. Members list to hire during project's execution (3)

Membro da equipa Team member	Função Role	Duração Duration	%tempo %otime
(BIC) Bolseiro de Iniciação à Investigação Científica 1	Bolseiro	12	100
(BIC) Bolseiro de Iniciação à Investigação Científica 2	Bolseiro	12	100
(BIC) Bolseiro de Iniciação à Investigação Científica 3	Bolseiro	12	100

6. Projectos financiados

6. Funded projects

-

Lista de projectos financiados (1)

Funded projects list (1)

Referência	Título	Estado
POSI/SRI/34392/2000	Democracia Electrónica	Em curso

(Os detalhes de cada projectos estão disponíveis clicando na referência correspondente)

(Details for each project are available by clicking on the corresponding reference)

7. Indicadores previstos

7. Expected indicators

-

Indicadores de realização previstos para o projecto

Expected output indicators

DESCRIÇÃO DESCRIPTION	2004	2005	2006	2007	2008	Total
A - Publicações Publications						
Livros Books	0	0	0	0	0	0
Artigos em revistas internacionais Papers in international journals	0	2	2	2	0	6
Artigos em revistas nacionais Papers in national journals	0	0	0	1	0	1
B - Comunicações Communications						
Comunicações em encontros científicos internacionais Communications in international meetings	0	2	2	2	0	6
Comunicações em encontros científicos nacionais Communications in national meetings	0	1	1	1	0	3
C - Relatórios Reports	0	2	3	5	0	10
D - Organização de seminários e conferências Organization of seminars and conferences	0	0	1	1	0	2
E - Formação avançada Advanced training						
Teses de Doutoramento PhD theses	0	0	0	0	0	0
Teses de Mestrado Master theses	0	2	1	1	0	4
Outras Others	0	0	0	0	0	0
F - Modelos Models	0	2	2	3	0	7
G - Aplicações computacionais Software	0	0	0	0	0	0
H - Instalações piloto Pilot plants	0	0	0	0	0	0
I - Protótipos laboratoriais Prototypes	0	2	2	2	0	6
J - Patentes Patents	0	0	0	0	0	0
L - Outros Other						
List of recommendations and best practices	0	1	2	2	0	5
	0	0	0	0	0	0
	0	0	0	0	0	0

Acções de divulgação da actividade científica

Scientific activity spreading actions

(Estimula-se a apresentação e propostas neste âmbito que possibilitem a aproximação da actividade científica ao

grande público)

(It is strongly desired the presentation of proposals within this subject that will approach science to the general public.)

Demonstration of prototypes will be set up within the Ministry of Justice (ITIJ) and Ministry of Internal Affairs (STAPE). Other potential targets being considered include UMIC (which organized the 2004 European Elections e-voting project) and members of the Portuguese house of representatives.

8. Anexo técnico

8. Technical addendum



8.1. Resumo

8.1. Abstract

Resumo (em português)

Abstract (in portuguese)

A introdução de votação electrónica (e-voto) nos Sistemas Eleitorais Nacionais tem recentemente recebido um interesse significativo em diversos países (e.g. EUA, UK, Portugal). Os estudos realizados até hoje claramente demonstram que este tipo de sistema é percebido como tendo um elevado nível de risco.

Como investigadores em sistemas complexos, engenharia organizacional e de software, tentamos analisar os problemas associados aos sistemas de e-voto, relacionando-os com as arquitecturas e componentes do sistema e procurando novas formas de desenvolver sistemas com risco reduzido.

Este problema é um desafio, dado que será necessário identificar as múltiplas dimensões que caracterizam os sistemas de e-voto e riscos associados. Estes riscos não surgem de uma única área de investigação, mas antes têm uma natureza fortemente multidisciplinar.

Este projecto não se propõe resolver 1 ou 2 temas bem conhecidos, e.g. segurança, deixando os restantes por resolver. Ao invés, a nossa perspectiva é que uma nova arquitectura tem de ser desenvolvida, capaz de resolver a natureza intrinsecamente complexa dos sistemas de e-voto. Esta nova abordagem tem de ser multidisciplinar, dado que os problemas se dividem por diversas áreas, como a de sistemas distribuídos, segurança da informação, IHC, design de software ou organizationalware. Esta nova abordagem tem também de ser visionária, dado que a maioria dos problemas dos sistemas de e-voto são de larga-escala em diversas dimensões (utilizadores, componentes, requisitos, riscos).

A nossa proposta consiste numa arquitectura de componentes de alto nível concebida para lidar com o risco em sistemas de e-voto.

Este projecto integra equipas das seguintes áreas:

- Especificação de arquitecturas de sistemas complexos (ADETTI, ITIJ, STAPE) - Com especialistas em Sistemas Eleitorais Nacionais, organizationware e análise e modelação de sistemas complexos
- Design de sistemas (FCUL) - Com especialistas no desenvolvimento de sistemas socio-técnicos complexos, novas técnicas de análise e design, como design participativo e prototipagem de baixa fidelidade
- Interação Humano-Computador (FCUL) - Com especialistas em IHC, engenharia de usabilidade, acessibilidade e interação multimodal
- Segurança de informação (IEETA, ADETTI, INESC) - Com especialistas na concepção e construção de sistemas de informação seguros e mecanismos de autenticação forte
- Sistemas distribuídos (INESC, IEETA) - Com especialistas em sistemas de larga-escala, tecnologia Internet e protocolos de votação segura

Duas instituições importantes participam no projecto: ITIJ, pertencente ao Ministério da Justiça, fornecedor tecnológico do Sistema Eleitoral Nacional; e STAPE, responsável pelo Sistema Eleitoral Nacional (NOTA: O STAPE participa como observador, pois tem limitações legais à participação em projectos FCT).

O projecto será organizado de acordo com 3 áreas de preocupação: 1) riscos relacionados com segurança; 2) riscos relacionados com a comunidade; e 3) riscos relacionados com a utilidade.

Resumo (em inglês)

Abstract (in english)

The introduction of electronic voting (e-voting) in National Election Systems has recently received a significant interest in several countries (e.g. USA, Canada, UK, Portugal). The studies conducted until today clearly demonstrate that this type of system is perceived as having a high level of risk.

As researchers in the complex systems, organization and software engineering fields, we are trying to analyze the problems associated to general e-voting systems, relating them with the system architecture and components, and finding new ways to deploy systems with reduced risk levels.

This problem is a challenging one, since it will be necessary to identify the multiple dimensions that characterize e-voting systems and associated risks. These risks do not roll up from one specific research topic, but rather have a strong multidisciplinary nature.

This project does not aim at tackling one or two well-known issues, e.g. security, but leaving the whole problem unsolved. On the contrary, our perspective is that a whole new integrated architecture must be developed, one that

is capable to tackle the intrinsic complex nature of e-voting systems. This new approach must be multidisciplinary, since problems with e-voting lay in different research areas, such as distributed systems, information security, HCI, software design or organizationware. This new approach must also be visionary, since most of the problems with e-voting are large-scale in several dimensions (users, components, requirements, risks).

Our proposed solution will consist of an architectural framework with high-level components conceived for handling risk in e-voting systems.

This project will integrate teams from the following research areas:

- Complex systems architecture specification (ADETTI, ITIJ, STAPE) – With specialists in National Election Systems, organizationware and complex systems analysis and modeling
- Software systems design (FCUL) – With specialists in the development of complex socio-technical systems, new analysis and design techniques such as participatory design and low-fidelity prototyping
- Human-computer interaction (FCUL) – With experts in HCI, usability engineering, accessibility and multimodal interactions
- Information security (IEETA, ADETTI, INESC) – With experts in designing and building information security systems and strong authentication mechanisms
- Distributed systems (INESC, IEETA) – With specialists in large-scale systems, Internet technology and secure voting protocols

Two important partners participate in the project: ITIJ, from the Ministry of Justice, technology provider for the National Election System; and STAPE, direct responsible for the National Election System (NOTE: STAPE will participate as observer, given that, as a ministerial structure, it has contractual limitations to participate in FCT projects).

The project will be organized according to three major areas of concern: 1) security-related risks; 2) community-related risks; and 3) usefulness-related risks.

8.2. Objectivos

8.2. Objectivos

Descrição dos Objectivos do Projecto

Project Objectives (description)

The objective of this project is to develop an innovative architectural framework for handling risk in e-voting systems, addressing 3 areas of concern:

- Security-related risks concern the design and realization levels. Our aim is to understand how analysis/design techniques can translate security requirements into architectural components. The project will explore misuse-cases to assess security risks
- Community-related risks address the realization and use levels. Our aim is to understand how the architecture can increase auditability and trust. The project will explore 2 types of awareness mechanisms: (1) external, allowing the community to perceive that the system works as expected; and (2) internal, allowing experts to probe the architectural components to verify their behavior
- Usefulness-related risks concern the design and use levels. Our aim is to understand how to integrate the multitude of user needs and user interface requirements into architectural components. The project will explore mobility issues and multimodal interfaces

Descrição dos Objectivos do Investigador Responsável

Principal Investigator Objectives (description)

The Principal Investigator research activities address the design, development, assessment and dissemination of organizational and complex socio-technical systems, involving multiple users and multiple risk factors such as safety, productivity, health, economic and technical. The Principal Investigator also teaches these topics in the Systems Analysis and Design, Human-Computer Interaction and Computer Supported Cooperative Work graduate and post-graduate courses. Inline with the project objectives, the Principal Investigator aims to further explore the impact of humans and communities of practice on systems use, as well as their implications to the development of more "humanistic" systems design techniques (or, as others have said, more "ecological" design techniques).

8.3. Estado da Arte

8.3. State of the Art

Descrição do Estado da Arte

State of the Art (description)

We present in [11] a survey of current e-voting systems, devices, projects and experiments. In [19] we analyze in detail the requirements of e-voting systems. Another recent survey is [24].

Since it is impractical to present a state-of-the-art of all topics related to e-voting in 3000 characters, we adopted to cite only: 1) official e-voting projects where research is not a goal; and 2) recent e-voting projects where research is a fundamental goal.

1)

UK is studying the implementation of e-voting in UK. So far, the general results identify many problems with e-voting and demand further innovation and experimentation [7].

IEEE is developing voting standards. So far, security, reliability, and usability issues are addressed in preliminary reports [14].

In USA several state authorities, like California [1], are studying e-voting. At federal level, the Federal Election Commission has developed a draft with standards to ensure reliability, accuracy, and integrity of e-voting [6].

Brazil was the first country in the world to rely 100% on e-voting. The system has been evaluated by several independent experts from Unicamp, SBC and COPPE/UFRJ. These reports identify many problems with the system, notably the lack of security, auditability and software quality.

2)

Caltech/MIT set up the Voting Technology Project to study the implications of e-voting in USA after the Florida problem. One research issue recently addressed concerns voting bias introduced by human-machine interfaces.

CyberVote was a project funded by the EU. Several documents were published concerning security techniques, architectural and ergonomic issues. The research analyzed multiplatform and multi-device architectures [25].

Avin Rubin [23] has recently analyzed the Diebold system and identified several security vulnerabilities in current e-voting technology.

[1] California Internet Voting Task Force. A Report on the Feasibility of Internet Voting. Jan 2000

[6] Federal Election Commission. Voting System Standards. Jul 2001

[7] E-Voting Research Team. The Implementation of Electronic Voting in the UK. Office of the e-Envoy. May 2002

[11] A Monteiro, N Soares, R Oliveira, P Antunes, Sistemas Electrónicos de Votação, FCUL, Out 2001

[14] IEEE Voting Equipment Standards Project 1583, Dec 2003

[19] R Pinto, F Simões, P Antunes, Estudo dos Requisitos para um Sistema de Votação Electrónica, FCUL, Mar 2004

[23] T Kohno, A Stubblefield, A Rubin, D Wallach, Analysis of an Electronic Voting System, Proc. IEEE Symp. on Security and Privacy, May 2004

[24] D Gritzalis (ed), Secure Electronic Voting, ADVANCES IN INFORMATION SECURITY: V7, Kluwer, 2002

[25] CyberVote, An Innovative Cyber Voting System for Internet Terminals and Mobile Phones, IST-1999-20338

8.4. Resultados e Repercussões

8.4. Results and Repercussions

Divulgação de Resultados (descrição)

Diffusion of Results (description)

Considering the multidisciplinary approach, the project will deliver very different types of results:

- An architectural framework with a set of high-level components tackling the various risks associated to e-voting systems
- A set of high-level components offering security-related properties
- Research results from the development and experimentation of the security-related components
- A set of high-level components offering external (the community) and internal (expert evaluators, auditors) awareness
- Research results from the development and experimentation of the awareness components
- Research results from the use of misuse-cases for security assessment and system design
- A set of high-level components addressing the universal human-computer interface requirements for e-voting systems
- Research results from the prototype development and experimentation of the usefulness-related components
- A collection of recommendations and best practices for the design, implementation, deployment and assessment of e-voting systems

Repercussões (descrição)

Repercussions (description)

As researchers in the complex systems, organization and software engineering fields, we try to understand how to deploy systems with reduced risk levels. The case of e-voting is a very challenging one because system properties are very interdependent and risks have a strong multidisciplinary nature. We support these observations with some examples.

For a start, there are many concerns about the security and robustness of e-voting systems. Many security, fault-tolerance, robustness and other techniques have been developed to address this issue. However, e-voting are massively distributed systems subject to the malicious intentions of a large number of organized hackers for a short period of time. E-voting systems cannot rely on trusted users, components, communication channels, operating systems or applications. Furthermore, many solutions are so complex that originate usability problems that paradoxically put e-voting systems at risk. Thus, the risks are significantly different from other large-scale systems.

Several studies also identify major concerns about the difficulty to satisfy the requirements of secrecy and auditability. This is the case, for instance, of the Brazilian e-voting system. As a pioneer, the Brazilian system is an excellent case study, showing that the secrecy and auditability of the whole voting process is questionable. The problem is that auditability must span across the whole development process, from analysis, design, implementation, testing and use. Thus, the whole software development methodology and system architecture must be redesigned to accommodate auditability features.

Researchers have also analyzed e-voting systems from the HCI point of view, highlighting many convenience and usability problems. One example of a challenging problem is accessibility, basically because designers must work with an open collection of user profiles, including illiterates, blind persons, etc.

Another example, one that expands from the human- to the community-centered perspectives, concerns transparency. E-voting systems are at high risk because the community may not perceive how the system operates and thus may question its use to the point of rejection. The recent discussions about the use of paper receipts are exemplary of the impact of these risks.

Our perspective is that the approach proposed by this project may have a profound impact on the development of complex systems in general, because it is based on completely new assumptions about the nature and purpose of the system: more driven by usefulness than functional requirements; more focused on tackling the community suspicions and fears; addressing risk throughout the whole design, development and deployment process.

Note that this project has a potential high impact because STAPE and ITIJ are both in charge of the Portuguese National Election System.

8.5. Regionalização

8.5. Regionalization

Região	Porcentagem
Region	Percent
Norte	15
Centro	14
Lisboa e Vale do Tejo	15
Alentejo	14
Algarve	14
Região Autónoma dos Açores	14
Região Autónoma da Madeira	14

Descrição

Description



E-Voting is an issues that has significant local and regional impact. First of all, by its own nature, e-voting systems must necessarily assure regional and local coverage. Second, the project addresses the mobility of voters, aiming at decreasing voters abstency. Finally, but not least important, the project addresses usability and accessibility issues. Technical solutions addressing usability and accessibility aim to overcome problems that have significant local and regional correlations, such as age and computer literacy.

8.6. Tarefas

8.6. Tasks

Lista de tarefas (6)

Task list (6)

Designação da tarefa 	Data de início	Data de fim	Pessoas * mês 
Task denomination	Start date	End date	Person * months
Task 1 – Security-related risks	01-01-2005	31-12-2005	18
Task 4 – Integrated perspective	01-01-2005	31-12-2007	24
Task 6 – Coordination and project manage...	01-01-2005	31-12-2007	4
Task 2 – Usefulness-related risks	01-07-2005	30-06-2006	18
Task 3 – Community-related risks	01-01-2006	31-12-2006	18
Task 5 – Legal issues	01-01-2006	31-12-2007	4

(Os detalhes de cada tarefa estão disponíveis clicando na designação correspondente)

(Details for each task are available by clicking on the corresponding denomination)

8.7. Referências Bibliográficas

8.7. Bibliographic references

Ano Publicação

Year Publication

2004	http://www.gsd.inesc.pt/~pjpf/REVS-lebre-IADIS-2004.pdf
2003	http://www.gsd.inesc.pt/~pjpf/REVS-journal-IADIS-2003.pdf
2004	http://www.di.fc.ul.pt/~paa/reports/di-fcul-tr-04-2.pdf
2001	http://www.di.fc.ul.pt/~paa/reports/di-fcul-tr-01-9.pdf
2003	http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/s/Serr=atilde=o:Carlos.html

8.8. Artigos Anteriores

8.8. Previous Articles

Ano Artigo (endereço na Internet - URL)

Year Paper (Link in the Internet - URL)

2003	http://www.di.fc.ul.pt/~paa/papers/criwg-03-wf.pdf
2003	http://www.di.fc.ul.pt/~paa/papers/group-03.pdf
2001	http://www.di.fc.ul.pt/~paa/papers/gdn-01.pdf
2003	http://www.di.fc.ul.pt/~paa/papers/criwg-03-pv.pdf
2002	http://www.di.fc.ul.pt/~paa/papers/coordination-02.pdf



15-07-2004 18:00:22



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCE



POCTI

Programa Operacional
Ciência, Tecnologia e Inovação

Programa Operacional "Ciência, Tecnologia, Inovação"



Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)
Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

Pedro Alexandre de Mourão Antunes

Carlos Manuel Jorge da Costa

(BIC) Bolseiro de Iniciação à Investigação Científica 1

Paulo Jorge Pires Ferreira

Filipe José Ferreira Simões

André Ventura da Cruz Marnôto Zúquete

Carlos Nuno da Cruz Ribeiro

Rui Filipe Lopes Joaquim


Descrição da tarefa

Task description

Designação da tarefa

Task denomination

Task 1 – Security-related risks

Data de início	Data de fim	Duração (em meses)	Pessoas * mês nesta tarefa 
Start date	End date	Duration (in months)	Person * month in this task
01-01-2005	31-12-2005	12	18

Resultados esperados

Expected results

1.1 Definition of security-related architectural components

1.2 One prototype validating the security-related architectural components

1.3 2 publications discussing and presenting results on the application of misuse-cases

1.4 List of recommendations and best practices related to security-related architectural components

Descrição da tarefa

Task description

1.1 Definition of security-related risks

1.2 Definition of security-related architectural strategies

1.3 Definition of security-related architectural components

1.4 Experiment the application of misuse-cases in several scenarios related to e-voting

1.5 Prototyping and validation

1.6 Risk assessment, recommendations and best practices

The overall objective of this task is to bring together two very different perspectives necessary to deploy secure e-voting systems: 1) handling risks at the high-level design (system and architecture); and 2) handling risks at the component design and realization levels. Different high- and low-level strategies must be combined to support fundamental e-voting system properties, like privacy, authenticity, singularity, vote integrity, system integrity, fault-tolerance, intrusion tolerance, etc. For instance, the combination of the "divide and conquer" strategy and "secure channels" may reduce the risk of breaking anonymity, since several components would have to be simultaneously compromised. Other high- and low-level alternatives will be explored and combined, such as patterns, grid architectures and object replication.

This task will also tackle security-related risks at the analysis level. In particular, the applicability of a recent analysis technique, designated misuse-case analysis (as opposed to use-cases, defined by UML), will be studied in detail.



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCES 



Programa Operacional "Ciência, Tecnologia, Inovação"



Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)
Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

Pedro Alexandre de Mourão Antunes

Carlos Manuel Jorge da Costa

(BIC) Bolseiro de Iniciação à Investigação Científica 2

Luís Manuel Pinto da Rocha Afonso Carriço

CARLOS JOSÉ CORREDOURA SERRÃO

João Manuel Macedo Ferreira Dias

Rui Luís Rocha Pinto


Descrição da tarefa

Task description

Designação da tarefa

Task denomination

Task 2 – Usefulness-related risks

Data de início	Data de fim	Duração (em meses)	Pessoas * mês nesta tarefa 
Start date	End date	Duration (in months)	Person * month in this task
01-07-2005	30-06-2006	12	18

Resultados esperados

Expected results

3.1 Definition of usefulness-related architectural components

3.2 Definition of universal user profile

3.3 Low-fidelity prototypes of e-voting system user interfaces

3.4 2 publications discussing and presenting results from experiences with the prototypes

3.5 List of recommendations and best practices related to usefulness-related architectural components

Descrição da tarefa

Task description

3.1 Definition of usefulness-related risks

3.2 Definition of usefulness-related architectural components

3.3 Mobility

3.4 Universal user profile

3.5 Multimodalities

3.6 Accessibility and fairness

3.7 Low-fidelity prototyping and validation

3.8 Risk assessment, recommendations and best practices

The objective of this task is to bring together two very different perspectives necessary to deploy useful e-voting systems: 1) handling risks at the high-level design (user interface); and 2) handling risks in a way that users and the community in general accept the system. The perspective underlying this task is that usability (ease of use, ease of learning) is not sufficient to guarantee success of the e-voting system, since more broad issues, like usefulness (how users value the system), must be considered as well.

This task will address the usability, accessibility and convenience properties of e-voting systems. In particular, this task will analyze how to support the mobility of voters, in order to decrease abstention. This task will also develop a universal user profile, integrating the multitude of users' characteristics and identifying the multiple interaction modalities that should be available to users (using aural, visual and tactile channels) and corresponding user interface components.

Finally, this task will also focus on tackling user interface solutions for e-voting systems that guarantee several important properties, such as accessibility (use by people with different characteristics) and fairness (the user interface should not favor any candidates, independently of channel resolution). Low-fidelity prototypes of these user-interfaces will be developed and experimented during this task.



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCE



POCTI

Programa Operacional
Ciência, Tecnologia e Inovação

Programa Operacional "Ciência, Tecnologia, Inovação"

POSI

Programa Operacional
Sociedade da Informação

Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)

Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

Pedro Alexandre de Mourão Antunes

(BIC) Bolseiro de Iniciação à Investigação Científica 3

Paulo Jorge Pires Ferreira

CARLOS JOSÉ CORREDOURA SERRÃO

André Ventura da Cruz Marnôto Zúquete

Carlos Nuno da Cruz Ribeiro

Maria Amélia dos Santos Damas

Oscar Manuel Martins Alves da Veiga

Rui Filipe Lopes Joaquim


Descrição da tarefa

Task description

Designação da tarefa 

Task denomination

Task 3 – Community-related risks

Data de início	Data de fim	Duração (em meses)	Pessoas * mês nesta tarefa 
Start date	End date	Duration (in months)	Person * month in this task
01-01-2006	31-12-2006	12	18

Resultados esperados 

Expected results

2.1 Definition of community-related architectural components

2.2 Definition of several external and internal awareness mechanisms

2.3 Several mock-ups of the external and internal awareness mechanisms

2.4 2 publications discussing and presenting results from the application of the awareness mechanisms

2.5 List of recommendations and best practices related to community-related architectural components

Descrição da tarefa

Task description

2.1 Definition of community-related risks

2.2 Definition of community-related architectural components

2.3 External awareness

2.4 Internal awareness

2.5 Construction of awareness mock-ups and validation

2.6 Risk assessment, recommendations and best practices

The objective of this task is to bring together two very different perspectives necessary to deploy acceptable e-voting systems: 1) handling risks in a way that users and the community in general accept the system; and 2) handling risks at the component design and realization levels. The underlying assumption for this task is that many times there is not much dialectical debate and collaboration between the practitioners that develop systems and the theorists that try to make sense of these systems according to their impact and roles within the community.

Many risks associated to e-voting systems, including dependability, auditability, traceability, system transparency and process transparency, depend not only on the technical features and performance of the system but also on the positive and negative perceptions that individuals and the community construct about them. This task will explore two different approaches to reduce these risk levels: 1) increase external awareness, by delivering feedback to users about how the system is operating; and 2) increase internal awareness, by supporting mechanisms that allow experts (auditors or other official entities) to reach individual architectural components in order to verify if they are operating as expected. Examples of external awareness mechanisms include "lights" showing that the voting machine is locked/unlocked, "counters" displaying the number of cast votes, "smartcards" guaranteeing that the voters' identifications and votes are physically separated, or "paper receipts" guaranteeing that votes can be recounted. Examples of internal awareness include features built in components to trace votes, analyze sent

messages, etc. Other innovative awareness mechanisms will be explored and prototyped.



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCES



Programa Operacional "Ciência, Tecnologia, Inovação"



Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)
Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

Pedro Alexandre de Mourão Antunes

Carlos Manuel Jorge da Costa

Luís Manuel Pinto da Rocha Afonso Carriço

Paulo Jorge Pires Ferreira

Filipe José Ferreira Simões

CARLOS JOSÉ CORREDOURA SERRÃO

João Manuel Macedo Ferreira Dias

André Ventura da Cruz Marnôto Zúquete

Rui Luís Rocha Pinto

Carlos Nuno da Cruz Ribeiro

Maria Amélia dos Santos Damas

Oscar Manuel Martins Alves da Veiga

Rui Filipe Lopes Joaquim

Descrição da tarefa

Task description

Designação da tarefa

Task denomination

Task 4 – Integrated perspective

Data de início Data de fim Duração (em meses)

Start date End date Duration (in months)

01-01-2005 31-12-2007 36

Pessoas * mês nesta tarefa 

Person * month in this task

24

Resultados esperados

Expected results

4.1 Vision

4.2 Scenarios and storyboards

4.3 Architectural framework

4.4 Risk assessment

4.5 Prototypes

4.6 4 publications discussing and presenting experimental results

4.7 Consolidated list of recommendations and best practices

Descrição da tarefa

Task description

4.1 Visioning

4.2 Scenarios and storyboards

4.3 Integration of architectural framework

4.4 Risk assessment

4.5 Prototypes

4.6 Experiments

4.7 Consolidation of recommendations and best practices

The ambitious objective of this task is to develop an innovative architectural framework for high-risk and complex systems. This architectural framework will be based on completely new assumptions about the target systems: more driven by usefulness than functional requirements; more focused on tackling the community suspicions and fears; addressing risk throughout the whole design, development and deployment process.

These assumptions derive directly from the results obtained with tasks 1-3 plus a series of project activities taken in parallel by the team.

This task will include brainstorming sessions, aiming to define a vision for the future e-voting architecture and define

a set of scenarios of use and corresponding storyboards. Lateral thinking will be used to identify new ideas and radical approaches to e-voting systems, such as the examples shown in the following preliminary list:

- Making the system more complex, e.g. by communicating "fake" messages, thus lowering the probability of someone hacking a "real" message
- Architecting the system with more interdependent components, so that attacks would only be possible by coalitions and access to multiple components
- Making the system massively redundant to avoid denial of service attacks, for instance using grid technology
- Using public lights, counters, audio signals and other physical/logical awareness devices that show to the community that the system is operating as intended
- Using visualization techniques to animate the flow of votes through the system, from voting to counting
- Studying alternatives to precinct and internet voting, relying on public services such as supermarkets to provide limited control to voting devices
- Studying the use of augmented reality devices (such as e-paper) in user-interfaces to increase usability and accessibility

The results obtained from tasks 1-3 will be consolidated into a coherent architectural framework. A risk assessment of the architectural framework will be performed, in order to identify its potential benefits. Prototypes will be developed. Based on the identified scenarios, several experiments will be performed to experiment and evaluate the framework (using both quantitative and qualitative data). Finally, this task will also consolidate the collection of recommendations and best practices obtained during the project.



POCTI

Programa Operacional
Ciência, Tecnologia, Inovação

POSI

Programa Operacional
Sociedade da Informação

Financiamento de Fundos Estruturais e de Fundos Nacionais do MCES



Programa Operacional "Ciência, Tecnologia, Inovação"

Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)
Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

João Manuel Macedo Ferreira Dias

Maria Amélia dos Santos Damas

Oscar Manuel Martins Alves da Veiga


Descrição da tarefa

Task description

Designação da tarefa

Task denomination

Task 5 – Legal issues

Data de início	Data de fim	Duração (em meses)	Pessoas * mês nesta tarefa 
Start date	End date	Duration (in months)	Person * month in this task
01-01-2006	31-12-2007	24	4

Resultados esperados

Expected results

5.1 List of recommendations

5.2 1 publication discussing the architectural framework from the legal point of view

Descrição da tarefa

Task description

5.1 Legal context of e-voting

5.2 Legal context of the architectural framework

5.3 Recommendations

The objective of this task is to analyze the legal implications of the current and future e-voting systems. Currently, there are many legal constraints to voting processes and technology, e.g. the process is limited to precinct voting, voters are limited to vote on a designated place, etc. Considering that the framework proposed in this project opens up the possibilities for voting processes that may be very different from the current one, this task aims at identifying where law may have to be readjusted to allow such new approaches.

The project will focus on two specific issues: 1) the legal context of voting, i.e. what specific legal limitations must be adapted to permit, for instance, Internet voting; and 2) the legal context of the framework, in particular considering legal aspects related to auditing activities, restricted access by privileged users, intrusion detection, anonymity guarantees, etc. This task will deliver a list of recommendations concerning these issues.



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCES 

POCTI

Programa Operacional

CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Programa Operacional "Ciência, Tecnologia, Inovação"



Programa Operacional Sociedade da Informação

Concursos de Projectos de I&D Proposals for R&D Projects

Tarefa

Task

► [Fechar esta janela](#)
Close this window

Referência do projecto

Project reference

POSI/EIA/57038/2004

Membros da equipa de investigação que participam nesta tarefa

Members of the research team who participate in this task

Nome

Name

Pedro Alexandre de Mourão Antunes

Paulo Jorge Pires Ferreira

João Manuel Macedo Ferreira Dias

André Ventura da Cruz Marnôto Zúquete

Maria Amélia dos Santos Damas

Descrição da tarefa

Task description

Designação da tarefa

Task denomination

Task 6 – Coordination and project management

Data de início Data de fim Duração (em meses)

Start date End date Duration (in months)

01-01-2005 31-12-2007 36

Pessoas * mês nesta tarefa 

Person * month in this task

4

Resultados esperados

Expected results

6.1 Kick-off review summary

6.2 Components review summary

6.3 Prototypes, mock-ups and experiments review summary

6.4 Recommendations review summary

6.5 Risks review summary

6.6 Results review summary

6.7 Project web site with results

Descrição da tarefa

Task description

6.1 Kick-off

6.2 Review components

6.3 Review prototypes, mock-ups and experiments

6.4 Review recommendations

6.5 Review risk assessments

6.6 Dissemination of results

This task is dedicated to review the progression of the project towards its goals at particularly important project steps, like component definitions, prototype developments and experiments. These review activities will be executed in parallel with tasks 1-5. This task is also responsible for organizing the dissemination of results obtained from the project.



Financiamento de Fundos Estruturais e de Fundos Nacionais do MCES



Programa Operacional "Ciência, Tecnologia, Inovação"



Programa Operacional Sociedade da Informação