FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA E DA TECNOLOGIA

Concurso

Projectos de investigação científica e de desenvolvimento tecnológico em todos os domínios científicos

SAPIENS Proj99

Formulário de candidatura electrónico

Título do projecto
Democracia Electrónica

Project Title
Electronic democracy

Área Disciplinar Principal
Engª Electrotécnica e Informática - Sistemas Robóticos, Inteligentes e de Informação

Projecto Nº
0

Data de recepção
0

1. Identificação do Projecto / Project Identification

1.1.1. Título do projecto
Democracia Electrónica

1.1.2. *Project Title*
Electronic democracy

1.1.3. Área Disciplinar Principal
Engª Electrotécnica e Informática - Sistemas Robóticos, Inteligentes e de Informação

1.1.4. Palavras Chave
Votação electrónica
Segurança
Sistemas distribuídos
Sistemas de suporte a grupos

1.1.5. *Keywords*
Electronic voting
Security
Distributed systems
Group support systems

1.1.6. Objectivos Sócio-Económicos
Desenvolvimento Social e Serviços Sociais

1.2. Investigador Responsável pelo projecto

1.2.1. Nome Completo
Paulo Jorge Pires Ferreira

1.2.2. Nº Bilhete de Identidade 6934614

1.2.3. Morada Institucional
INESC - Rua Alves Redol N. 9, 6 Andar

1.2.4. Localidade
Lisboa

1.2.5. Código Postal 1000

1.2.6. Telefone 213100230 **Fax** 213145843

1.2.7. Email paulo.ferreira@inesc.pt

1. Identificação do Projecto / Project Identification

1.3.1. Duração do projecto em meses *(Project duration in months)* 36

1.3.2. Data de Início do projecto *(Project starting date)* 01/09/2000

1.3.4. Financiamento solicitado *(Requested funding)* *s* 11640 **contos**

1.3.5. Unidade de investigação responsável pelo projecto *(Principal research unit)*
Instituto de Engenharia de Sistemas e Computadores - INESC Lisboa

2. Instituições participantes / Participating Institutions

2.1. Instituição Proponente *(Prime Contractor)*

2.1.1. Denominação
Instituto de Engenharia de Sistemas e Computadores - INESC

2.2. Financiamento solicitado à FCT *(requested funding)*

Descrição *(Description)*	**1º Ano *(1st Year)***	**2ºAno *(2nd Year)***	**3ºAno *(3rd Year)***	***Total***
Recursos humanos *(Human resources)*	0	0	0	0
Aquisição de serviços e manutenção *(Acquisition of services and maintenance)*	500	500	500	1500
Missões *(Missions)*	1000	1000	1000	3000
Consultores *(Consultants)*	0	0	0	0
Despesas Gerais *(Orverheads)*	520	420	380	1320
Outras Despesas Correntes *(Other current expenses)*	400	200	200	800
TOTAL - Despesas Correntes *(TOTAL - current expenses)*	2420	2120	2080	6620
Equipamento *(Equipment)*	700	400	200	1300
TOTAL	3120	2520	2280	7920

2. Instituições participantes / Participating Institutions

2.1. Instituições que participam no projecto - além da instituição proponente *(Institutions that participate in the project - other than Prime Contractor)*

Denominação
Universidade de Lisboa - Fundação da Faculdade de Ciências

2.2. Financiamento solicitado à FCT *(requested funding)*

Descrição *(Description)*	**1º Ano *(1st Year)***	**2ºAno *(2nd Year)***	**3ºAno *(3rd Year)***	***Total***
Recursos humanos *(Human resources)*	0	0	0	0
Aquisição de serviços e manutenção *(Acquisition of services and maintenance)*	100	100	100	300
Missões *(Missions)*	500	500	500	1500
Consultores *(Consultants)*	200	0	0	200
Despesas Gerais *(Orverheads)*	260	180	180	620
Outras Despesas Correntes *(Other current expenses)*	200	100	100	400
TOTAL - Despesas Correntes *(TOTAL - current expenses)*	1260	880	880	3020
Equipamento *(Equipment)*	300	200	200	700
TOTAL	1560	1080	1080	3720

3. Orçamento / Budget

3.1. Financiamento global solicitado à FCT *(Overall funding requested to FCT)*

Descrição *(Description)*	**1º Ano *(1st Year)***	**2ºAno *(2nd Year)***	**3ºAno *(3rd Year)***	***Total***
Recursos humanos *(Human resources)*	0	0	0	0
Aquisição de serviços e manutenção *(Acquisition of services and maintenance)*	600	600	600	1800
Missões *(Missions)*	1500	1500	1500	4500
Consultores *(Consultants)*	200	0	0	200
Despesas Gerais *(Orverheads)*	780	600	560	1940
Outras Despesas Correntes *(Other current expenses)*	600	300	300	1200
TOTAL - Despesas Correntes *(TOTAL - current expenses)*	3680	3000	2960	9640
Equipamento *(Equipment)*	1000	600	400	2000
TOTAL	4680	3600	3360	11640

3.2. Plano de financiamento *(Finance plan)*

Descrição *(Description)*	**1º Ano *(1st Year)***	**2ºAno *(2nd Year)***	**3ºAno *(3rd Year)***	***Total***
Financimento solicitado à FCT *(Requested funding)*	4680	3600	3360	11640
Financiamento próprio *(Own funding)*	0	0	0	0
Outro financiamento público *(Other public-sector funding)*	0	0	0	0
Outro financiamento privado *(Other private funding)*				

	0	0	0	0

TOTAL DO PROJECTO *(PROJECT TOTAL)*

	4680	3600	3360	11640

4. Instalações e Equipamento / Facilities and Equipment

4.1. Discriminação do equipamento a adquirir

4.1.1. Tipo de equipamento *(equipment item)*
PCs (4)

4.1.2. Fabricante e modelo *(manufacturer and model)*
Not applicable

4.1.3. Preço *(cost)* 1600 **Contos**

4.1.4. Justificação do financiamento solicitado para a rubrica acima descrita:
(Justification of the funding requested, for the described budget item)
Three of the PCs will support the development of the voting system.
The other PC will be used for testing and providing voting services.

4. Instalações e Equipamento / Facilities and Equipment

4.2. Instalações *(Facilities)*

The facilities to be used are provided by INESC - Lisboa, in the Distributed Systems Group, and LASIGE.

4. Instalações e Equipamento / Facilities and Equipment

4.3. Equipamento Principal *(Equipment)*

The equipment for the project will be acquired with the funding provided.

4.4. Outros Recursos *(Other resources)*

Basic secretarial support will be provided at INESC Lisboa and FCUL.

5. Equipa de Investigação / Research Team

5.1.1. Nome Completo *(full name)*
Paulo Jorge Pires Ferreira

5.1.2. Numero de Bilhete de Identidade
6934614

5.1.3. Unidade de Investigação *(research unit)*
Instituto de Engenharia de Sistemas e Computadores - INESC Lisboa

5.1.4. Cargo
Investigador

5.1.5. Doutorado *(doctor degree)*
Sim

5.1.6. % de tempo completo no projecto *(% of full time in project)*
25

5.1.7. Pessoa mês no projecto *(person month in project)*
9

5. Equipa de Investigação / Research Team

5.1.1. Nome Completo *(full name)*
Nuno Miguel Vicente de Pina Gonçalves

5.1.2. Numero de Bilhete de Identidade
9520056

5.1.3. Unidade de Investigação *(research unit)*
Laboratório de Sistemas Informáticos de Grande-escala

5.1.4. Cargo
Investigador

5.1.5. Doutorado *(doctor degree)*
Não

5.1.6. % de tempo completo no projecto *(% of full time in project)*
20

5.1.7. Pessoa mês no projecto *(person month in project)*
4

5. Equipa de Investigação / Research Team

5.1.1. Nome Completo *(full name)*
Pedro Alexandre de Mourão Antunes

5.1.2. Numero de Bilhete de Identidade
5665723

5.1.3. Unidade de Investigação *(research unit)*
Laboratório de Sistemas Informáticos de Grande-escala

5.1.4. Cargo
Investigador

5.1.5. Doutorado *(doctor degree)*
Sim

5.1.6. % de tempo completo no projecto *(% of full time in project)*
20

5.1.7. Pessoa mês no projecto *(person month in project)*
6

5. Equipa de Investigação / Research Team

5.1.1. Nome Completo *(full name)*
André Ventura da Cruz Marnôto Zúquete

5.1.2. Numero de Bilhete de Identidade
6854047

5.1.3. Unidade de Investigação *(research unit)*
Instituto de Engenharia de Sistemas e Computadores - INESC Lisboa

5.1.4. Cargo
Investigador

5.1.5. Doutorado *(doctor degree)*
Não

5.1.6. % de tempo completo no projecto *(% of full time in project)*
100

5.1.7. Pessoa mês no projecto *(person month in project)*
36

5. Equipa de Investigação / Research Team

5.1.1. Nome Completo *(full name)*
Carlos Nuno da Cruz Ribeiro

5.1.2. Numero de Bilhete de Identidade
7335100

5.1.3. Unidade de Investigação *(research unit)*
Instituto de Engenharia de Sistemas e Computadores - INESC Lisboa

5.1.4. Cargo
Investigador

5.1.5. Doutorado *(doctor degree)*
Não

5.1.6. % de tempo completo no projecto *(% of full time in project)*
100

5.1.7. Pessoa mês no projecto *(person month in project)*
36

5. Equipa de Investigação / Research Team

5.2. Curriculum Vitae

5.2.1. Name
Paulo Jorge Pires Ferreira

5.2.2. Place of Birth Portugal

5.2.3. Data of Birth 07/09/1965

5.2.4. Nationality Portuguese

5.2.5. Institutional Address
INESC
Rua Alves Redol 9, 6 Andar

5.2.6. Telephone 213100230 **Fax** 213145843

6.5.7. Email paulo.ferreira@inesc.pt

5.2.8. Main scientific area of research
Distributed Operating Systems

5.2.9. Other Scientific areas of interest
Large-scale distributed data sharing, replication and consistency protocols, distributed garbage collection, persistence by reachability

5.2.10. Academic degrees, fields of study, awarding institutions, dates in reverse chronological order
PhD, Informatics (distributed systems), Université Pierre et Marie Curie, 1996
MsC, Informatics (distributed systems), Instituto Superior Técnico, 1992
Licenciatura, Electrotecnical Engineering, Instituto Superior Técnico, 1988

5.2.11. Present Position, institution, starting date
Leader of the Distributed Systems Group at INESC (since Jan. 99) and Professor at IST (since 1997)

5.2.12. Previous positions, institutions, dates in reverse chronological order
President of Scientific Council, ISCTE, 1992, 1990
Associate Professor, ISCTE, 1990
Teaching Assistant, Faculdade de Letras and ISPA, 1976

5.2.13. Prizes

5.2.14. Publications
PerDiS: design, implementation, and use of a PERsistent DIstributed Store
Paulo Ferreira, Marc Shapiro, Xavier Blondel, Olivier Fambon, João Garcia, Sytse Kloosterman, Nicolas Richer, Marcus Roberts, Fadi Sandakly, George Coulouris, Jean Dollimore, Paulo Guedes, Daniel Hagimont, and Sacha Krakowiak.

Book chapter in Recent Advances in Distributed Systems, eds. S. Krakowiak and S.K. Shrivastava, Springer Verlag LNCS vol. 1752.

PerDiS: An Infrastructure for Cooperative Engineering in Virtual Entrepises in a Virtual Enterprise
Fadi Sandakly, João Garcia, Paulo Ferreira, and Patrice Poyet
PROVE'99, IFIP/PRODNET Working Conference on Infrastructures for Industrial Virtual Enterprises, Porto (Portugal), October 1999

The PerDiS FS: A Transactional File System for a Distributed Persistent Store
João Garcia, Paulo Ferreira and Paulo Guedes
Eigth ACM Sigops Workshop, Sintra, Portugal, September 1998

Modelling a Distributed Cached Store for Garbage Collection: the algorithm and its correctness proof
Paulo Ferreira and Marc Shapiro
ECOOP'98, Brussels, Belgium, July 1998

Parallel Operating Systems
João Garcia, Paulo Ferreira, and Paulo Guedes
Book chapter in Handbook on Parallel and Distributed Processing, 1999.

5. Equipa de Investigação / Research Team

5.2. Curriculum Vitae

5.2.1. Name
Pedro Alexandre de Mourão Antunes

5.2.2. Place of Birth Lisboa

5.2.3. Data of Birth 17/05/1964

5.2.4. Nationality Portugal

5.2.5. Institutional Address
Informatics Dep., Sciences Fac., Univ. of Lisboa
Campo Grande, 1749-016 Lisboa

5.2.6. Telephone 217500124 **Fax** 217500084

6.5.7. Email paa@di.fc.ul.pt

5.2.8. Main scientific area of research
Electronic Meeing Systems

5.2.9. Other Scientific areas of interest
Computer Supported Cooperative Work, Groupware, Systems Analysis, Human-Computer Interaction

5.2.10. Academic degrees, fields of study, awarding institutions, dates in reverse chronological order
Ph.D. in Electrical and Computer Engineering, From Instituto Superior Técnico, 1997
Msc. in Electrical and Computer Engineering, From Instituto Superior Técnico, 1991
Degree in Electrical and Computer Engineering, From Instituto Superior Técnico, 1987

5.2.11. Present Position, institution, starting date
Professor, Informatics Department, Sciences Faculty, University of Lisboa, since nov. 1999

5.2.12. Previous positions, institutions, dates in reverse chronological order
Professor, Informatic Eng. Department, Instituto Superior Técnico, 1998-1999
Professor, Electrical and Comp. Eng. Department, IST, 1997-1998
Teaching Assistant, Electrical and Comp. Eng. Department, IST, 1989-1996
Researcher at INESC, 1989-96

5.2.13. Prizes

5.2.14. Publications
[1] P. Antunes, T. Ho. Facilitation Tool - A Tool to Assist Facilitators Managing Group Decision Support Systems. Nineth Workshop on Information Technologies and Systems (WITS '99). Charlotte, North Carolina. December 1999.
[2] P. Antunes, T. Ho, L. Carriço. A GDSS Agenda Builder for Inexperienced Facilitators.

Proceedings of the 10th EuroGDSS Workshop. Copenhagen, Denmark. June 1999. ISBN: 90-5638-043-5.
[3] T. Ho, P. Antunes. Developing a Tool to Assist Electronic Facilitation of Decision-Making Groups. Fifth International Workshop on Groupware, CRIWG ’99. IEEE Press. Cancun, Mexico. September 1999. ISBN: 0-7695-0268-7.
[4] C. Costa, T. Ho, P. Antunes. Facilitating Organisational Activities Using Plans and Audits. 1st International Conference on Enterprise Information Systems. Setubal, Portugal. March 1999. ISBN: 972-98050-0-8.
[5] P. Antunes, C. Costa, M. Duque, N. Guimarães, J. Jesuino, H. Stadler. On the Design of Group Decision Processes for Electronic Meeting Rooms. Fourth International Workshop on Groupware, CRIWG '98. Buzios, Brazil. September 1998.
[6] P. Antunes. A System for Supporting and Managing Same-Time/Different-Place Group Interactions. Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '98). ACM Press. L'Aquila, Italy. May 1998.
[7] N. Guimarães, P. Antunes, A. Pereira. The Integration of Workflow Systems and Collaboration Tools. Workflow Management Systems and Interoperability. A. Dogac, L. Kalinichenko, M. Ozsu, A. Sheth (Editors). Lecture Notes in Computer Science, Springer-Verlag. Instanbul, Turky. August 1997. ISBN: 3540644113.
[8] P. Antunes, N. Guimarães, J. Segovia, J. Cardenosa. Beyond Formal Processes: Augmenting Workflow with Group Interaction Techniques. Conference on Organizational Computing Systems (COOCS '95). ACM Press. San Jose, California. August 1995. ISBN: 0-89791-706-5.

7. Indicadores Previstos / Expected Indicators

7.1. Indicadores de realização previstos para o projecto

Unidade: em número

Descrição *(Description)*	**1º Ano *(1st Year)***	**2ºAno *(2nd Year)***	**3ºAno *(3rd Year)***	***Total***
A - Publicações *(Publications)*				
Livros *(Books)*	0	0	0	0
Artigos em revistas internacionais *(Papers in international journals)*	0	0	1	1
Artigos em revistas nacionais *(Papers in national journals)*	0	0	0	0
B - Comunicações *(Communications)*				
Em encontros científicos internacionais *(in international meetings)*	1	2	2	5
Em encontros científicos nacionais *(in national meetings)*	0	0	0	0
C - Relatórios *(Reports)*	1	1	1	3
D - Organização de seminários e conferências *(Organization of seminars and conferences)*	0	0	0	0
E - Formação Avançada *(Advanced training)*				
Teses de Doutoramento *(PhD theses)*	0	0	1	1
Teses de Mestrado *(Master theses)*	0	0	2	2
Outras *(Others)*	0	0	0	0
F - Modelos *(Models)*	0	0	0	0
G - Aplicações computacionais *(Software)*	0	0	1	1
H - Instalações piloto *(Pilot plants)*	0	0	0	0
I - Protótipos laboratoriais *(Prototypes)*	0	0	1	1

J - Patentes *(Patents)*

	0	0	0	0

L - Outros *(Others)*

	0	0	0	0
	0	0	0	0
	0	0	0	0

8. Anexo Técnico / Technical Addendum

8.1. Resumo do projecto

A crescente banalização da ligação pessoal à Internet cria naturalmente novas possibilidades de interacção entre pessoas, e entre pessoas e instituições. Tal é o caso das eleições, onde comunidades de pessoas, devidamente credenciadas e autorizadas, contribuem obrigatória ou voluntariamente num processo de escolha. A maioria dos processos de votação credíveis baseiam-se
normalmente numa confirmação presencial da identidade dos votantes por entidades supostamente idóneas, e em procedimentos de apuramento isentos, devidamente acompanhados por entidades reguladoras unanimemente aceitas. Este projecto tem como objectivo desenvolver sistemas de votação
electrónica como meio de expressar a vontade de comunidades de uma sociedade digital, que impossibilita o recurso ao contacto físico entre os diversos intervenientes no processo de votação.

Um sistema de votação electrónica levanta diversas questões, que foram divididas em três níveis. Em primeiro lugar, o aspecto de mercado, ou seja, a configuração do sistema para responder a múltiplas necessidades e solicitações. A este nível, o aspecto fundamental a explorar pelo projecto é o desenvolvimento de diversos pacotes com diferentes requisitos de mercado. A título de exemplo, os pacotes poderiam destinar-se a: (1) fornecer mecanismos de auscultação do mercado que
permitissem diminuir os desajustes entre produtores de bens e a vontade dos seus consumidores; (2)
servir as necessidades de movimentos de opinião, já hoje activos na sociedade digital mas sem meios credíveis de expressar a vontade democrática; e (3) substituir, com vantagens logísticas, os sistemas de votação tradicionais em urna, tipicamente adoptados pelos sistemas associativos e políticos.

Num segundo nível o projecto irá considerar os aspectos algorítmicos da votação electrónica. Os diversos pacotes de mercado exemplificados acima devem ser construídos a partir de componentes reutilizáveis, em particular bibliotecas de algoritmos de votação, e bibliotecas de mecanismos de aquisição de dados dos utentes. Muitos algoritmos de votação são conhecidos. Aqui, o que o projecto tem de interessante a explorar são formas diversas e talvez múltiplas de votação (v.g. o fraccionamento de votos por diversas alternativas ou a escolha do processo de apuramento de resultados).

O nível final a considerar pelo projecto aborda os protocolos de interacção que suportam todo o sistema. Estes têm de contemplar todos os aspectos da segurança, porque o mercado da votação electrónica exige uma grande confiança pelos seus possíveis utentes. Essa confiança requer, por um
lado, que a entidade reguladora do sistema seja credível, o que levanta problemas técnicos importantes no que se refere à comunicação segura, anonimato, fiabilidade e transparência no funcionamento do sistema. Por outro lado, a credibilidade do resultado de uma votação depende da correcta participação dos votantes, sendo portanto imprescindível autenticar os utentes e evitar utilizações ilícitas.

8. Anexo Técnico / Technical Addendum

8.2. Project's summary

The widespread connection of people to the Internet creates a natural potential for developing and improving interactions between people, and between people and organizations. One of such interactions is voting, were communities of persons, with proper credentials and authorizations, contributed mandatory or voluntarily in a choice process. Most credible voting processes rely on physical confirmation of people's identity by appropriate entities, and on impartial counting procedures supervised by regulatory organizations unanimously accepted. This project aims at developing electronic voting systems for expressing the opinion of communities in the digital society, which prevents physical interaction between all participants in the voting process.

An electronic voting system raises several issues, which were subdivided in three layers. At a first layer, the market one, the system should match several needs and expectations. At this layer the main issues are to design and provide different packets tailored for specific market needs. The following examples outline some possible packets: (1) provide mechanisms to become aware of market opinions in order to reduce mismatches between producers of goods and the desires of their consumers; (2) support opinion movements, already active in the digital society but lacking credible means to express democratic willingness; and (3) replace, simplifying logistics, traditional ballot systems typically used in associative or political systems.

In a second layer the project will consider the algorithmic aspects of the electronic voting. The different market packets above referred should be built from a set of reusable components, namely libraries of voting algorithms and libraries of mechanisms for gathering data from users. There are many well-known voting algorithms, but in this project we aim at providing innovative, or even multiple, voting schemes (e.g. to split votes by several alternatives, or to choose the votes' counting procedure).

The final layer considered by the project deals with the interaction protocols required by the electronic voting system. These protocols must take in consideration security issues, as the acceptance of electronic voting requires strong confidence levels by potential users' communities. Such confidence requires, on one side, credible regulatory organizations. This raises several technical issues, concerning the overall system's behavior, in the fields of secure communication, anonymity, fault-tolerance and transparency. On the other side, credible voting results depends on the correct participation of people. This means that the electronic voting system must authenticate users and prevent illicit interactions.

8. Anexo Técnico / Technical Addendum

8.3. Descrição do projecto *(Project's Description)*

8.3.1. Objectivos *(Objectives)*

The main goals of the project are to evaluate market needs towards credible electronic voting, and to study and develop effective and realistic solutions to satisfy market needs. These solutions should be built upon libraries of components, and these components should model basic algorithms of voting procedures, like how to vote or how to count votes. To implement these algorithms for conducting a credible voting process it is necessary to provide protocols assuring a given level of confidence. Such confidence implies that special care should be devoted to data security, people authentication and authorization, transparency/surveillance of the counting procedures, and fault tolerance against involuntary or malicious service disruptions.

8.3.2. O Projecto e os objectivos do IR a longo prazo *(The project and the long term objectives of the PI)*

The main research area is the study and design new security policies and mechanisms to achieve the
necessary confidence levels in large-scale electronic voting processes. This policies and mechanisms
must be tailored to specific voting scenarios, as they depend on the community of people that may vote and on the kind of alternatives proposed to scrutiny.

8.3.3. Repercussões éticas, sociais e ambientais *(Ethic, social and environment impacts)*

We do not anticipate any negative impact on ethical, social or ambiental issues. On the contrary, the voting solutions design within the project will take special care with ethical and social impact, because such impact is a key issue in the adoption of the proposed solutions by a community of target users.

8.3.4. Relação com o estado da arte *(Relationship with the state of the art)*

Arrow's classic book "Social Choice and Individual Values" has the following declaration: "In a capitalist democracy there are essentially two methods by which social choices can be made: voting, typically used to make "political" decisions, and the market mechanism, typically used to make "economic" decisions."

Voting methods are extensively discussed in many classic books such as [Ross55] and [Black58]. Electronic voting systems reflect the traditional electoral process, as we know it: prior to an election, organizers determine who is eligible to vote. This involves a formal registration period and an announcement. Once the election begins, administrators validate the credentials of those attempting to vote. This procedure also involves keeping track of who has already voted. After validating each voter, the administrators collect the voted ballots and, finally, the ballots are counted to determine the election result.

Although electronic voting may open new ways of making decisions, they may be compromised if not carefully designed. The security of the whole electoral process must be guaranteed: only eligible voters may register, and only once; voters must be authenticated; only a single vote may be submitted (if that is the voting method); and, finally, the whole counting process must be certified.

Recently, we have seen the emergence of electronic voting systems with these characteristics on the Internet, e.g. VoteBot and eVot [Cranor2000]. For instance, the Election.com company, a global Internet election company, provides several services concerning voting procedures (Ballot Design, Internet Ballot, Absentee Ballots, and Voter Registration) [Elections]. Electronic voting systems reduce the time and cost of elections, which allows to increase their frequency. This small change has already instigated significant modifications in the ways people make decisions. One notable example is given by [Whitworth99]. According to their view, voting is not the inevitable final step of the rational decision-making process but, instead, is a method to increase group unity, reduce inter-personal conflicts and speed decision making. Such perspective has been applied to small groups with significant results, but remains untested in broader contexts.

In terms of secure protocols for enforcing credible voting processes there are several algorithms, briefly resumed in [Schneier96]. These algorithms have different requirements to fulfill different functionalities: some require a trusted, unique and central tabulating and legitimation service; others split these services by different organizations; others do not require any centralized services. Each of these algorithms is suitable for a particular set of voting models, which are defined by several socio-logic aspects, like: the voting community, the options subject to scrutiny; the lobbies for any of the options, etc.

8.3.5. Relação com outros projectos *(Relationship with other projects)*

The INESC Distributed Systems Group has been involved in several projects concerning the security in distributed system. The team developed an architecture for providing security for remote communications used by legacy applications using two novel cryptographic techniques [Zúquete96,Zúquete97a,Zúquete97b,Zúquete97c]. The team is also developing a security framework which is able to express simultaneously several complex security policies, including history- and obligation-based policies [Ribeiro99].

The LASIGE Team has been involved in several projects related with the current proposal. The most relevant one is a project designated "Decision and Creativity in Electronic and Natural Groups," financed by PRAXIS. The project developed an electronic decision room and run more than 100 meetings, many using voting procedures. In another project, designated "Facilitation Tool," the LASIGE Team developed two voting tools that may be run over the Internet: "Opinion Meter" and "Criteria Meter". These tools were part of a collection of tools dedicated to facilitate remote meetings by small groups of
people.

8.3.6. Difusão de resultados *(Diffusion of results)*

Diffusion activities will involve three main areas: (1) production of research papers, (2) free distribution of software, and (3) Internet access to experimental voting systems by means of ordinary Internet tools, like WWW browsers or e-mail managers.

8. Anexo Técnico / Technical Addendum

8.3. Descrição do projecto - Plano Geral *(Project's Description - Work plan)*

8.3.7. Identificação da tarefa *(task identification)* 1

8.3.8. Designação da tarefa *(Task denomination)*
Service Level

8.3.9. Investigadores Intervenientes *(Researchers)*
Paulo Ferreira, André Zúquete, Pedro Antunes, Nuno Gonçalves

8.3.10. Duração da tarefa em meses *(Task duration - months)* 12

8.3.11. Pessoas * mês *(Person * month)* 21

8.3.12. Resultados esperados *(Expected results)*
Identification of several usefull electronic voting models.
Identification of some critical aspects of the voting models, like the registration of people eligible to vote
and the selection of the entities that supervise voting, vote counting, and publishing of results.

8.3.13. Descrição da tarefa *(Task description)*
Voting systems are complex socio-technical systems, linking multiple users and different organizations, dealing with ethical issues, while posing strong technical requirements.

At least, we can find three different levels of analysis that must be considered when characterizing a voting system: organizational needs, voting services and external qualities. The organizational needs characterize the different kinds of political initiatives that jump-start voting systems, such as petitions, creation of lobbies, groups of interest, and generic or specific committees. Less demanding corporate initiatives, for instance business inquiries, must also be analyzed to completely characterize the organizational needs.

Voting services typify the processes that must be carried out in order to accomplish organizational needs. At this level we include ballot design, casting ballots over the Internet, signing petitions, distributing information among interest groups and providing registration services. Finally, the third level of analysis considered, external qualities, characterizes the different dependencies on the voting services. These dependencies are related with the protection of individual voters (security, privacy), organizational demands (time and cost) and also public needs (e.g. increase participation in voting processes).

In a context as complex as the one previously exemplified, it is extremely beneficial to develop systems analysis in close collaboration with the interested parties (users, service providers, politicians, etc.). This task is dedicated to categorize the needs and expectations of a voting system in a participatory way. The participatory approach will rely on group support systems. A significant number of computer-supported meetings with interested parties will be organized and conducted by the project team. The results of these meetings will be consolidated in a service level model of the voting system.

8. Anexo Técnico / Technical Addendum

8.3. Descrição do projecto - Plano Geral *(Project's Description - Work plan)*

8.3.7. Identificação da tarefa *(task identification)* 2

8.3.8. Designação da tarefa *(Task denomination)*
Voting System

8.3.9. Investigadores Intervenientes *(Researchers)*
André Zúquete, Carlos Ribeiro, Pedro Antunes, Nuno Gonçalves

8.3.10. Duração da tarefa em meses *(Task duration - months)* 12

8.3.11. Pessoas * mês *(Person * month)* 26

8.3.12. Resultados esperados *(Expected results)*
Identification of voting algorithms.
Definition and implementation of components for supporting different kinds of electronic voting procedures, like how to express a vote or how to count votes.

8.3.13. Descrição da tarefa *(Task description)*
This task is dedicated to develop a component-based architecture for the voting system, assembling different services from a small set of reusable and configurable components.

The architecture of the voting system specifies three major software components: Agents, Processes and Results. Agents may be of two different kinds, sponsors and electors. Sponsors encapsulate the set of functionalities that support the creation and design of ballots, launching petitions and arranging committees and groups. Similarly, electors encapsulate the set of functionalities that support casting ballots, signing petitions or entering/leaving groups. The Agents component will primarily rely on Internet technology to interconnect users and the voting system. One significant goal, although hard to realize and quantify, that this component must accomplish is to increase the participation of users in the voting processes.

The second architectural component, the electoral Process, implements the algorithmic aspects of the electronic voting. There are many well known voting algorithms, e.g. single majority, two-round majority, approval voting, alternative voting, voting by veto, etc. Most of these algorithms will be implemented and properly encapsulated within different electoral Processes. Reusability of subcomponents will be attempted to minimize software development. The Results architectural component is dedicated to accomplish one major purpose: the dissemination and archival of results. This component will be further divided into front-end and back-end subcomponents of the voting system, the former dedicated to deliver voting results to users and the later responsible for a trustworthy repository of ballots. Note that this component is not dedicated to counting of votes, since counting is intrinsically associated to voting algorithms.

8. Anexo Técnico / Technical Addendum

8.3. Descrição do projecto - Plano Geral *(Project's Description - Work plan)*

8.3.7. Identificação da tarefa *(task identification)* 3

8.3.8. Designação da tarefa *(Task denomination)*
Voting Protocols

8.3.9. Investigadores Intervenientes *(Researchers)*
André Zúquete, Carlos Ribeiro, Nuno Gonçalves

8.3.10. Duração da tarefa em meses *(Task duration - months)* 12

8.3.11. Pessoas * mês *(Person * month)* 23

8.3.12. Resultados esperados *(Expected results)*
Application of existing or new security-related protocols and algorithms to the voting algorithms defined in the previous task.

8.3.13. Descrição da tarefa *(Task description)*
This task is dedicated to develop security-related algorithms and protocols to enforce the correctness of the overall voting process. These algorithms and protocols will be designed to support the voting algorithms designed in the previous task.

The security issues of correct voting processes can be divided in three main areas: (1) authenticate people in order to grant or deny their vote, (2) provide some degree of privacy to hide choices of the voting people, and (3) guaranty the availability of the voting process and the correctness of the result.

The first area deals with authentication and authorization of people in a distributed system. Typical authentication systems use two kinds of mechanisms: (i) secret data sharing, or (ii) public data sharing, using private/public key pairs. The first mechanism is more simple an practical to manage, but does not scale well [Kerberos]. The second mechanism scales better but typically requires a complex managing infra-structure (PKI -- Public Key Infrastructure) [PEM]. Therefore, one of the challenges of this task is to design and implement authentication mechanisms well-suited for particular voting processes.

The second area deals with privacy concerns of the voting people. This means that no untrusted entity should be able to determine the choice of any other voter, or even determine who voted. The problem of voters' privacy is complex, as it depends on many aspects of the system -- e.g. how people is authenticated, how they get voting clearance, how they express their vote, how voting results are computed and published, if voters can correct miscounts without revealing their vote, etc. Therefore, one goal of this task is to identify a minimal set of techniques capable of providing voter's privacy in multiple configurations of the voting system. Furthermore, privacy should be assured even when authenticating user's data, like with blind signatures [Chaum83].

The third area deals with trust relationships between all entities participating in a voting process and fault-tolerance. Simpler systems require few trust requirements and fault-tolerance support, but are also highly vulnerable to simpler problems. More complex systems require many

trust requirements and fault-tolerance mechanisms, therefore being capable of providing a better service. A goal of this task is to provide solutions for different kinds of trust relationships and fault-tolerance required by the voting system components, designed in the previous task, and by the voters' confidence requirements.

8. Anexo Técnico / Technical Addendum

8.3. Descrição do projecto - Plano Geral *(Project's Description - Work plan)*

8.3.7. Identificação da tarefa *(task identification)* 4

8.3.8. Designação da tarefa *(Task denomination)*
Voting Experience

8.3.9. Investigadores Intervenientes *(Researchers)*
André Zúquete, Carlos Ribeiro

8.3.10. Duração da tarefa em meses *(Task duration - months)* 12

8.3.11. Pessoas * mês *(Person * month)* 21

8.3.12. Resultados esperados *(Expected results)*
Public access to electronic voting services using ordinary Internet tools.

8.3.13. Descrição da tarefa *(Task description)*
This task intends to provide several secure voting systems to small or large communities of people by
means of ordinary Internet tools, like WWW browsers or e-mail managers.

8. Anexo Técnico / Technical Addendum

8.4. Resultados de projectos anteriores financiados *(Outputs of previously funded projects)*

8.4.1. Título do projecto ***(Project title)***
PerDiS

8.4.2. Entidade financiadora ***(Funding entity)***
ESPRIT

8.4.3. Código de identificação do projecto ***(Project identification)*** Esprit IV - 22533

8.4.4. Financiamento total concedido ***(Total funding)*** 48.000.000 PTE

8.4.5. Período coberto ***(period covered)*** **de** ***(from)*** 01/12/1996 **a** ***(to)*** 30/11/1999

8.4.6. Elementos da equipa de investigação da presente candidatura envolvidos no projecto ***(Reseach team members involved in the project)***
Prof. Paulo Ferreira

8.4.7. Publicações resultantes de projectos anteriores ***(Publications resulting from previous projects)***
Recent Advances in Distributed Garbage Collection
Marc Shapiro, Fabrice le Fessant, and Paulo Ferreira
Book chapter in Recent Advances in Distributed Systems, eds. S. Krakowiak and S.K. Shrivastava, Springer Verlag LNCS vol. 1752. To be published during 2000.

PerDiS: design, implementation, and use of a PERsistent DIstributed Store
Paulo Ferreira, Marc Shapiro, Xavier Blondel, Olivier Fambon, João Garcia, Sytse Kloosterman, Nicolas Richer, Marcus Roberts, Fadi Sandakly,
George Coulouris, Jean Dollimore, Paulo Guedes, Daniel Hagimont, and Sacha Krakowiak
Book chapter in Recent Advances in Distributed Systems, eds. S. Krakowiak and S.K. Shrivastava, Springer Verlag LNCS vol. 1752. To be published during 2000

The PerDiS FS: A Transactional File System for a Distributed Persistent Store
João Garcia, Paulo Ferreira and Paulo Guedes
Eigth ACM Sigops Workshop, Sintra, Portugal, September 1998.

8.4.8. Sumário de projectos anteriores ***(Abstracts of previous projects)***
It was developed a system with transactions, security, and garbage collection capable of supporting CAD applications over wide-area networks. A real application was ported to the platform. This application is a CAD tool for the building industry (developed by a Germam company) and the results were vere encouraging.

The most important scientific results were obtained in the area of distributed garbage collection and wide-area relaxed transactions (adapted to loosely coupled networks) with new algorithms being designed, implemented and tested.

Currently, there are some European companies interested on taking the results from the project and apply them to an industrial product.

8. Anexo Técnico / Technical Addendum

8.4. Resultados de projectos anteriores financiados *(Outputs of previously funded projects)*

8.4.1. Título do projecto ***(Project title)***
COOP

8.4.2. Entidade financiadora ***(Funding entity)***
FCT

8.4.3. Código de identificação do projecto ***(Project identification)*** Praxis XXI

8.4.4. Financiamento total concedido ***(Total funding)*** 12.700.000 PTE

8.4.5. Período coberto ***(period covered)*** **de** ***(from)*** 01/01/1997 **a** ***(to)*** 31/12/1999

8.4.6. Elementos da equipa de investigação da presente candidatura envolvidos no projecto ***(Reseach team members involved in the project)***
Prof. Paulo Ferreira

8.4.7. Publicações resultantes de projectos anteriores ***(Publications resulting from previous projects)***
Parallel Operating Systems
João Garcia, Paulo Ferreira, and Paulo Guedes
Book chapter in Handbook on Parallel and Distributed Processing, 1999

Two-Level Recovery for Distributed Shared Memory, Manuel Costa and Paulo Guedes. ERSADS' 97 - 2nd European Research Seminar on Advances in Distributed Systems, Zinal, Switzerland, March 1997.

PPF Case Study:Fitting a Distributed Garbage Collection Algorithm to a Persistent Distributed Store Architecture, Xavier Blondel, Paulo Ferreira and Marc Shapiro. OOPSLA'97 Workshop on Garbage Collection, October 1997.

Efficient and Flexible Object Sharing, Miguel Castro, Paulo Guedes, Manuel Sequeira, and Manuel Costa. Proceedings of the International Conference on Parallel Processing, August 12-16, 1996.

Lightweight Logging for Lazy Release Consistent Distributed Shared Memory, Manuel Costa, Paulo Guedes, Manuel Sequeira, Nuno Neves, and Miguel Castro. Proceedings of the Second Symposium on Operating Systems Design and Implementations (OSDI´96), October 28-31, 1996, Seattle, Washington, USA.

8.4.8. Sumário de projectos anteriores ***(Abstracts of previous projects)***
It was developed a prototype based on distributed shared memory with several consistency policies adapted to a large variety of cooperative applications. This system was improved with fault-tolerance by means of a transactional mechanism. Finally, it was developed an application demonstrative of the capabilities of the system.

M.Sc. Thesis
Fault-Tolerance in a Release-Consistent Distributed Shared Memory System, Manuel Costa, Master's Thesis, Instituto Superior Técnico, February 1997.

Disconnected Operation in a Distributed Object System, Filipe Madeira, Master's Thesis, Instituto Superior Técnico, May 1997.

A Transactional System for Cooperative Applications in Loosely Coupled Networks, João Coelho Garcia, Master's Thesis, Instituto Superior Técnico, Awaits defense.

8. Anexo Técnico / Technical Addendum

8.4. Resultados de projectos anteriores financiados *(Outputs of previously funded projects)*

8.4.1. Título do projecto ***(Project title)***
OSIRIS

8.4.2. Entidade financiadora ***(Funding entity)***
FCT

8.4.3. Código de identificação do projecto ***(Project identification)*** Praxis XXI

8.4.4. Financiamento total concedido ***(Total funding)*** 6.000.000 PTE

8.4.5. Período coberto ***(period covered)*** **de** ***(from)*** 01/01/1997 **a** ***(to)*** 31/12/1998

8.4.6. Elementos da equipa de investigação da presente candidatura envolvidos no projecto ***(Reseach team members involved in the project)***
Eng. André Zúquete

8.4.7. Publicações resultantes de projectos anteriores ***(Publications resulting from previous projects)***
Transparent Authentication and Confidentiality for Datagram Sockets
André Zúquete and Paulo Guedes.
ERSADS '97 - 2nd European Research Seminar on Advances in Distributed Systems.
March 1997. Zinal, Switzerland.

Efficient Stream Cipher with Variable Internal State
André Zúquete and Paulo Guedes.
SAC '97 - 4th Annual Workshop on Selected Areas in Cryptography.
August 11-12, 1997. Carleton University, Ottawa Ontario, Canada.

Efficient Error-Propagating Block Chaining
André Zúquete and Paulo Guedes.
6th IMA Conference on Cryptography and Coding.
December 17-19, 1997.

8.4.8. Sumário de projectos anteriores ***(Abstracts of previous projects)***
It was developed a secure communication system called PES (Privacy Enhanced Sockets) that allows legacy applications to communicate securely without being modified.

It was also installed, analysed and configured a firewall that was used in the Distributed Systems Group at INESC. Numerous statistics were obtained allowing the study of most common important security attacks.

M.Sc. Thesis
A Security Module for Extensible Filesystem Architectures, Luis Manuel Aidos Ferreira, Master's Thesis, Instituto Superior Técnico, Awaits defense.

PhD Thesis

Secure Communication, André Zúquete, PhD Thesis, Instituto Superior Técnico, Awaits defense.

8. Anexo Técnico / Technical Addendum

8.4. Resultados de projectos anteriores financiados *(Outputs of previously funded projects)*

8.4.1. Título do projecto ***(Project title)***
Cognitive Mapping of the Negotiation Processes

8.4.2. Entidade financiadora ***(Funding entity)***
PRAXIS

8.4.3. Código de identificação do projecto ***(Project identification)*** PCSH/P/PSI/77/96

8.4.4. Financiamento total concedido ***(Total funding)*** 9.250.000 PTE

8.4.5. Período coberto ***(period covered)*** **de** ***(from)*** 01/09/1997 **a** ***(to)*** 31/08/1999

8.4.6. Elementos da equipa de investigação da presente candidatura envolvidos no projecto ***(Reseach team members involved in the project)***
Prof. Pedro Antunes

8.4.7. Publicações resultantes de projectos anteriores ***(Publications resulting from previous projects)***
[1] L. Carriço, P. Antunes, N. Guimarães. Visual Reflection: Language, Action and Feedback. Proc. of the Visual Languages '99 Symp. IEEE Press. Tokyo, Japan. Sept. 1999
[2] J. Carvalho, J. Tomé. Fuzzy Mechanisms for Causal Relations. Proc. of the IFSA99, 8th Int. Fuzzy systems Association World Congress, Taiwan, 1999
[3] J. Carvalho, J. Tomé. Rule Based Fuzzy Cognitive Maps and Fuzzy Cognitive Maps – A Comparative Study. Proc. of the NAFIPS99, 1999
[4] J. Carvalho, J. Tomé. Rule Based Fuzzy Cognitive Maps – Fuzzy Causal Relations. Conf. on Computational Intelligence for Modelling, Control and Automation – CIMCA, 1999
[5] L. Carriço, N. Guimarães. Integrated MultiViews. Journal of Visual Languages and Computing, Special Issue on Visual Navigation: Methods and Tools. Academic Press, July 1998
[6] L. Carriço, N. Guimarães. Manipulating Concept Maps with Constrainned Regions. In Proc. of the AVI'98 Conf. L'Aquila, Italy, May 1998

8.4.8. Sumário de projectos anteriores ***(Abstracts of previous projects)***
The objective of the project Cognitive Mapping of the Negotiations Processes is the study of the cognitive aspects involved in negotiation in organisations, using the theory and methodology of cognitive maps, supported by dedicated computational tools. It is, therefore, an interdisciplinary project combining teams from Social and Computer Sciences.
A primary project contribution is a better comprehension of the causal reasoning underlying the strategies developed by negotiators, thus providing the means to improve the negotiation support systems and enhance the managers negotiation expertise.
In practical terms, the project accessed the cognitive maps of negotiators before the negotiation and after its completion, confronting them with their initial plans and the recorded negotiation process itself. This approach was applied to several typical scenarios, with expert and non-expert negotiators, using decision support systems.

8. Anexo Técnico / Technical Addendum

8.4. Resultados de projectos anteriores financiados *(Outputs of previously funded projects)*

8.4.1. Título do projecto ***(Project title)***
Decision and Creativity in Electronic and Natural Groups

8.4.2. Entidade financiadora ***(Funding entity)***
PRAXIS

8.4.3. Código de identificação do projecto ***(Project identification)*** 2/21/CSH/675/95

8.4.4. Financiamento total concedido ***(Total funding)*** 20.905.000 PTE

8.4.5. Período coberto ***(period covered)*** **de** ***(from)*** 01/09/1997 **a** ***(to)*** 31/08/1999

8.4.6. Elementos da equipa de investigação da presente candidatura envolvidos no projecto ***(Reseach team members involved in the project)***
Prof. Pedro Antunes

8.4.7. Publicações resultantes de projectos anteriores ***(Publications resulting from previous projects)***
[1] P. Antunes, T. Ho. Facilitation Tool - A Tool to Assist Facilitators Managing Group Decision Support Systems. Works. on Inf. Systems and Tech. Charlotte, North Carolina. Dec. 1999
[2] C. Costa, P. Antunes, J. Dias. GDSS: Limitações e Oportunidades. Conf. Especializada Sistemas e Tecnologias de Informação: Desafios para o Século XXI. Univ. Católica, Lisboa. Out. 1999
[3] P. Antunes, C. Costa, M. Duque, N. Guimarães, J. Jesuino, H. Stadler. On the Design of Group Decision Processes for Electronic Meeting Rooms. CLEI Journal, 2(1). 1999
[4] T. Ho, P. Antunes. Developing a Tool to Assist Electronic Facilitation of Decision-Making Groups. 5th Int. Works. on Groupware, CRIWG '99. IEEE Press. Cancun, Mexico. Sep. 1999. ISBN: 0-7695-0268-7
[5] P. Antunes, T. Ho, L. Carriço. A GDSS Agenda Builder for Inexperienced Facilitators. Proc. of the 10th EuroGDSS Works. Copenhagen, Denmark. June 1999. ISBN: 90-5638-043-5
[6] C. Costa, T. Ho, P. Antunes. Facilitating Organisational Activities Using Plans and Audits. First Int. Conf. on Enterprise Inf. Systems. Setubal, Portugal. March 1999. ISBN: 972-98050-0

8.4.8. Sumário de projectos anteriores ***(Abstracts of previous projects)***
The main goal of project Decision and Creativity in Electronic and Natural Groups was to set up an electronic meeting room at INDEG, a public institute owned by ISCTE. The creation of such an electronic meeting room pursued two fundamental purposes: (1) provide an infrastructure to teach topics related to management sciences; and (2) demonstrate the environment to companies with links to the institute. Another purpose, of major importance to the project team, was to execute scientific experiments with the room, particularly in what concerned the effects of software usage on decision-making processes.
The room is operational and, in fact, it is the one of its kind operational in Portugal, although risking being dismantled. It should also be noted that the teams proposing this project are the only ones active in EMS research field in Portugal.
The project produced many other significant results: More than 100 electronic meetings; 15 people trained as facilitators; Masters and Graduation works of 7 students; 1 Ph.D. work; development of 2

Masters courses in 2 Universities (IST, FCUL).

8. Anexo Técnico / Technical Addendum

8.5. Referências bibliográficas *(Bibliographic References)*

Team References

[Antunes99]
P. Antunes and T. Ho, Facilitation Tool - A Tool to Assist Facilitators Managing Group Decision Support Systems, Works. on Inf. Systems and Tech. Charlotte, North Carolina. Dec. 1999

[Ho99]
T. Ho and P. Antunes, Developing a Tool to Assist Electronic Facilitation of Decision-Making Groups, 5th Int. Works. on Groupware, CRIWG '99. IEEE Press. Cancun, Mexico, Sep. 1999, ISBN: 0-7695-0268-7

[Ribeiro99]
C. Ribeiro and P. Guedes, Verifying workflow processes against organization security policies. In Proceedings of the 8th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 190-191, Standford, California, June 16-18 1999. IEEE Computer Society, IEEE Computer Society.

[Zúquete96]
Transparent Authentication and Confidentiality for Stream Sockets, IEEE Micro, 16 (1996), pp. 34-41.

[Zúquete97b]
Efficient Stream Cipher with Variable Internal State, in SAC '97 - 4th Annual Workshop on Selected Areas in Cryptography, Ottawa, Canada, Aug. 1997.

Cited References

[Black58]
D. Black, The Theory of Committees and Elections, Cambridge University Press, 1958.

[Chaum83]
D. Chaum, Blind signatures for untraceable payments, in Proceedings of Crypto 82, Plenum Press, New York, 1983, pp. 199-203.

[Cranor96]
L. Cranor, Electronic Voting: Computerized polls may save money, protect privacy, http://www.acm.org/crossroads/xrds2-4/voting.html

[Cranor2000]
L. Cranor, Electronic Voting Hot List, http://www.ccrc.wustl.edu/~lorracks/sensus/hotlist.html

[Elections]
Elections.com web page, http://Election.com

[Emerson98]
P.J. Emerson, Beyond the Tyranny of the Majority: Voting Methodologies in Decision-Making and

Electoral Systems, The Borda Institute, 1998.

[Kerberos]
J. G. Steiner, C. Neuman, and J. I. Schiller, Kerberos: An Authentication Service for Open Network Systems, in Proc. of the USENIX Winter Conf., Dallas, Texas, USA, Feb. 1988, pp. 191-202.

[PEM]
J. Linn, Privacy Enhancement for Internet Electronic Mail, RFC 1421, 1422, 1423 and 1424, Feb. 1993, available via the DDN Network Center.

[Ribeiro99]
C. Ribeiro and P. Guedes, Verifying workflow processes against organization security policies. In Proceedings of the 8th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 190-191, Standford, California, June 16-18 1999. IEEE Computer Society, IEEE Computer Society.

[Ross55]
J. Ross, Elections and Electors, Eyre and Spottiswoode, 1955.

[Schneier96]
B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc., second ed., 1996.

[Schofield96]
Norman Schofield, Ed., Collective Decision-Making: Social Choice and Political Economy, Kluwer, 1996.

[Tullock98]
Gordon Tullock, On Voting, The Locke Institute, 1998.

[Whitworth99]
B. Whitworth and R. McQueen, Voting Before Discussiong: Computer Voting as Social Communication, Proc. of the 32nd Hawaii Intern. Conf. On Systems Science, 1999.

[Zúquete96]
Transparent Authentication and Confidentiality for Stream Sockets, IEEE Micro, 16 (1996), pp. 34-41.

[Zúquete97c]
Efficient Error-Propagation Block Chaining, in 6th IMA Int. Conf. on Cryptography and Coding (LNCS 1355), M. Darnell, ed., Berlin, Dec. 1997, Springer-Verlag.

[Zúquete97b]
Efficient Stream Cipher with Variable Internal State, in SAC '97 - 4th Annual Workshop on Selected Areas in Cryptography, Ottawa, Canada, Aug. 1997.

[Zúquete97a]
Transparent Authentication and Confidentiality for Datagram Sockets, in ERSADS '97 - 2nd European Research Seminar on Advances in Distributed Systems, Zinal, Switzerland, Mar. 1997, pp. 216-221.

8. Anexo Técnico / Technical Addendum

8.6. Artigos anteriores *(Previous papers)*

Endereços de Internet onde estão depositados os artigos
(URLs where the papers are placed)

8.6.1. Artigo 1
http://www.di.fc.ul.pt/~paa/papers/wits-99.pdf

8.6.2. Artigo 2
http://www.di.fc.ul.pt/~paa/papers/criwg-99.pdf

8.6.3. Artigo 3
http://www.gsd.inesc.pt/~cnr/ribeiro.pdf

8.6.4. Artigo 4
http://www.gsd.inesc.pt/~avz/IEEE.june.96.html

8.6.5. Artigo 5
http://www.gsd.inesc.pt/~avz/SAC97.html

Termo de responsabilidade

Investigador Responsável

Declaro assumir a liderança científica do projecto e as responsabilidades decorrentes de uma boa execução do mesmo.

Nome Paulo Jorge Pires Ferreira

Data

Assinatura

Unidade de Investigação e Desenvolvimento responsável pelo projecto

Como coordenador da Unidade de I&D Instituto de Engenharia de Sistemas e Computadores - INESC Lisboa declaro que esta unidade assume a responsabilidade do projecto e assegura as condições necessárias para a sua boa execução

Nome

Data

Assinatura (com carimbo ou selo branco)

Instituição Proponente

A Instituto de Engenharia de Sistemas e Computadores - INESC instituição proponente declara que são verdadeiras todas as informações contidas no presente formulário e que tomou conhecimento do articulado constante no Regulamento de Projectos de investigação Científica e de Desenvolvimento Tecnológico. Compromete-se a prestar as condições necessárias para uma boa execução do projecto, de acordo com o programa de trabalhos e meios apresentados, assim como a inscrever no seu orçamento as verbas necessárias à execução do projecto de acordo com os valores indicados.

Nome

Data

Assinatura (com carimbo ou selo branco)

Termo de responsabilidade

Instituição Participante

A (O) Universidade de Lisboa - Fundação da Faculdade de Ciências
declara que são verdadeiras todas as informações contidas no presente formulário e que tomou conhecimento do articulado constante no Regulamento de Projectos de investigação científica e de desenvolvimento tecnológico. Compromete-se a prestar as condições necessárias para uma boa execução do projecto, de acordo com o programa de trabalhos e meios apresentados, assim como a inscrever no seu orçamento as verbas necessárias à execução do projecto de acordo com os valores indicados.

Nome

Data

Assinatura (com carimbo ou selo branco)