EU:n 7. puiteohjelma

Tietoturva puiteohjelmassa

Tähän dokumenttiin on koottu ICT Work Programme (for ICT Research in FP7) 2007-2008 osalta tietoturvaa käsittelevä sisältö. Koko Work Programme on luettavissa ja ladattavissa osoitteesta: ftp://ftp.cordis.lu/pub/fp7/ict/docs/ict-wp-2007-08_en.pdf

Parhaan informaation seitsemännestä puiteohjelmasta löydät CORDIS –sivustolta osoitteesta: http://cordis.europa.eu/fp7/home_en.html tai Suomen EU T&K –sihteeristön kautta osoitteesta http://www.tekes.fi/eu/

CORDIS-sivustolta löytyy mm. tuorein dokumentaatio, sisältöä puiteohjelmalle ja hauille, ohjeistusta osallistumiselle ja mm. linkit projektipartnereiden hakemiselle.

Tekes järjestää myös Startti seitsemänteen puiteohjelmaan –tilaisuuden 11.-12.1.2007: TKK Dipoli, Otakaari 24, Espoo. Ilmoittautuminen sihteeristön sivuilta.

Tietoturva esiintyy ICT Työohjelmassa seuraavasti:

Tavoite 1.4. Turvalliset, käyttövarmat ja luotettavat infrastruktuurit

a) Verkkoinfrastruktuurien turvallisuus ja sietokyky
b) Turvallisuus ja luotettavuus dynaamisissa ja palautuvissa verkkoarkkitehtuureissa
c) Trusted computing –infrastruktuurit
d) Indentiteetin hallintaa ja yksityisyydensuojaa tehostavat työkalut
e) Tutkimus roadmapit; mittarit ja benchmarkit

Työohjelman budjetin jakautuminen tavoite 1.4. osalta on yhteensä 90 M€:

- Yhteistyöprojektit 80 M€
- Osaamisverkostot (Networks of Excellence) 6 M€
- Koordinointi- ja tukitoimenpiteet 4 M€

Nämä kuuluvat ensimmäiseen hakuun (ICT Call 1), joka julkaistiin 22.12. ja päättyy 8.5.2007 klo 17 (Brysselin aika). Koko ensimmäisen ICT haun budjetti on 1194 M€.

Tavoite 1.7 Kriittisten infrastruktuurien suojaaminen (joint call)

1. ICT teema
2. Turvallisuusteema
    a. Riskien arviointi ja jatkuvuuden suunnittelu liikenne- ja energiaverkoille
    b. Valmennuksen mallintaminen ja simulointi
    c. Tilannekuvan optimointi älykkäillä valvontajärjestelmillä (liikenne- ja energiaverkot)
    d. Kriittisten infrastruktuurien ICT-tuki kriisienhallintatilanteissa

Suuntaa antava budjetti tavoitteen 1.7 osalta on 40 M€:

- ICT teema 20 M€ ja turvallisuusteema 20 M€.

- Noin 90% kokonaisbudjetista jakautuu yhteistyöprojekteille kokoluokaltaan 2-5 M€, kesto 2-4 vuotta.
- Maksimissaan 10 % käytetään koordinointi- ja tukitoimenpiteisiin (keskikoko 0,5 M€).
- Mahdollisesti 1 M€ käytetään kansainväliseen yhteistyöhön.

Nämä kuuluvat ensimmäiseen SEC -hakuun (FP7-ICT.SEC-2007-1), joka julkaistaan 30.4.2007 ja päättyy 29.11.2007 klo 17 (Brysselin aika). Koko tämän haun budjetti on 40 M€.

Suomalaiset yhteyshenkilöt 7. puiteohjelman tieto- ja viestintäteknologioiden osalta ovat:

Anri Kivimäki, NCP
Tekes, puh. 010 60 28043

Kimmo Ahola, komiteajäsen
Tekes, puh. 010 60 55756

Kontaktihenkilö EU komissiossa on:
Jacques BUS, Jacques.Bus@ec.europa.eu, Head of Unit INFSO-D4, European Commission
Security, Dependability & Trust in the ICT-FP7 Work programme for 2007-2008.

Informaatiota löydät myös seuraavilta sivustoilta:
http://www.ist-securist.org/ (ICT Security & Dependability Taskforce)
http://www.esfors.org/ (European Security Forum for Web Services, Software and Systems)

Kooste Work Programme 2007 – 2008 –dokumentaatiosta tietoturvan osalta:

Challenge 1: Pervasive and Trusted Network and Service Infrastructures
With its strengths in communication equipment, devices, networks and eServices, Europe is well placed in the world-wide race to define and develop the network and service infrastructures of the future. These will generate new economic opportunities with new classes of networked applications, whilst reducing operational expenditures. The current internet, mobile, fixed and broadcasting networks and the related software service infrastructure need to progress accordingly in order to enable another wave of growth in the on-line economy and society over the next 15 years.

The challenge is to deliver the next generation of ubiquitous and converged network and service infrastructures for communication, computing and media. This entails overcoming the scalability, flexibility, dependability and security bottlenecks, as today's network and service architectures are primarily static and able to support a limited number of devices, service features and limited confidence. Such new infrastructures will permit the emergence of a large variety of business models capable of dynamic and seamless end-to-end composition of resources across a multiplicity of devices, networks, providers and service domains.

The future infrastructures envisaged will need to:

- Be pervasive, ubiquitous and highly dynamic. They have to offer almost unlimited capacities to users, by supporting a wide variety of nomadic interoperable devices and services, a variety of content formats and a multiplicity of delivery modes. They also have to support context awareness and the dynamic behaviour needed for applications with requirements that vary with time and context;
- Guarantee robustness, resilience, trust and security compatible with networks and software service platforms reaching a complexity and scale that are an order of magnitude greater than those of today's infrastructures;
- Support networked and managed business and service convergence across a multiplicity of environments such as the home, businesses, or nomadic situations.

This entails addressing the evolution from today's large legacy infrastructures towards new infrastructures by striking a balance between backward compatibility requirements and the need to explore disruptive architectures to build future internet, mobile, broadband, and associated service infrastructures.

The evolution drivers of this Challenge relate primarily to the technological evolution of ubiquitous mobile and broadband networks, the availability of dynamic services platforms, trust and security, in the context of converged and interoperable networked environments. In this respect, the proposed activity largely relates to the technological roadblocks and socioeconomic scenarios identified in the Strategic Research Agendas of the eMobility, NESSI, NEM and ISI European Technology Platforms.

Participation of organisations from third countries is encouraged for those research activities where mutual benefits can be demonstrated. This relates notably to i) the possibility of progressing through joint strategic research partnerships towards global consensus and standards; ii) opportunities for mutual benchmarking; iii) the exchange of best practices, including regulation and socio-economic issues as technological drivers; iv) large-scale validation of technologies and networked applications in a global context. The participation of third country partners and the selection of the most promising targeted regions are left to the initiative of the proponents.

Proposals for large scale integrating projects cutting across several of the objectives 1.1 to 1.5 of Challenge 1 and addressing interrelated objectives from an overall system perspective are encouraged. The intention is to significantly advance the state-of-the-art for each of the targeted objectives and to obtain a federating, multiplier and catalytic effect on the expected impacts.

Objective ICT-2007.1.4: Secure, dependable and trusted Infrastructures

Target outcome

a) **Security and resilience in network infrastructures**: building and preserving flexible, scalable and context-aware, secure and resilient architectures and technologies to enable dynamic management policies that ensure end-to-end secure transmission of data and services across heterogeneous infrastructures and networks, including dynamic networks of tiny insecure devices, and multiple provider, business and residential domains; real time detection and recovery capabilities against intrusions, malfunctions and failures;

b) **Security and trust in dynamic and reconfigurable service architectures** supporting assured and scale-free composition of services and service coalitions with managed operation across several administrative or business domains, enabling flexible business models;

c) **Trusted computing infrastructures** ensuring interoperability and end-to-end security of data and services; increased security and dependability in the engineering of software and service systems to ensure the design and development of trustworthy applications and services;

d) **Identity management and privacy enhancing tools** with configurable, context-dependent and user-controlled attributes in static and dynamically changing environments; **trust policies** for managing and assessing the risks associated to identity and private data.

e) Longer term visions and **research roadmaps**; **metrics and benchmarks** for comparative evaluation and open technology competitions, in support of certification and standardisation; international cooperation and co-ordination with developed countries; coordination with related national or regional programmes or initiatives and; coordination of FP7 projects addressing security, dependability, privacy and related ethical issues across different challenges and objectives of this work programme.

Expected Impact

- ICT users empowered to handle their digital identity and personal data and to protect their privacy, turning the European view on privacy into an economic advantage; strengthened trust in the use of networks, software and services for governments, businesses and consumers.
- A strong and competitive ICT security industry in Europe.
- Substantially improved security and dependability of networks and service infrastructures having a complexity and scale that are an order of magnitude greater than those of today's infrastructures.
- Wider use of metrics, standards, evaluation and certification methods and best practices in security of networks, infrastructures, software and services.

Funding schemes
a-d): CP (Collaborative Projects), NoE (Networks of Excellence); e) CSA (Coordination and Support Actions)

Indicative budget distribution13
90 M€:
- CP 80 M€ of which a minimum of 28 M€ to IP and a minimum of 28 M€ to STREP;
- NoE 6 M€;
- CSA 4 M€

Call
FP7-ICT-2007-1

13 Most of the amount for Call 1 is from the 2007 budget and is under the condition that the preliminary draft budget for 2007 is adopted without modifications by the budget authority. The remaining amount for Call 1 and the amounts for Calls 2, 3, FET-Open and the joint call with the security theme are expected to be covered by the 2008 budget for which a new financing decision to cover the budget for that year will be requested at the appropriate time.

Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection
(Joint Call between ICT and Security Themes FP7-ICT-SEC-2007-1)

The interoperability and interconnectivity of supply systems is one of the cornerstones of the functioning of our societies. The vulnerabilities in the intercommunication of systems, equipment, services and processes and their resilience against malicious attacks of terrorism and (organised) crime are elementary to the security of the citizens.

The objective of the joint call is to make key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare, or transportation systems more secure and dependable. The aim is to protect such critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.

The joint call is structured around two specific foci.

1. **Focus of the ICT Theme**
The first focus is called for by the *ICT* theme and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures so that they survive malicious attacks or accidental failures, guarantee integrity of data and continuous provision of responsive and trustworthy services, and support dynamically varying trust requirements. This includes:

a) Understanding and managing the interactions and complexity of interdependent critical infrastructures; mastering their vulnerabilities; preventing against cascading effects; providing recovery and continuity in critical scenarios (including research towards designing and building self-adapted and self-healing complex systems); security and dependability metrics and assurance methods for quantifying infrastructure interdependencies.

b) Designing and developing secure and resilient networked and distributed information and process control systems; systemic risk analysis and security configuration and management of critical information infrastructures and dynamic assurance frameworks for interconnecting them with critical infrastructures; availability of security forensics.

c) Developing longer term visions and research roadmaps; metrics and benchmarks for comparative evaluation in support of certification and standardisation; international cooperation and co-ordination with developed countries; coordination with related national or regional programmes or initiatives.

Funding schemes: a) and b): CP (STREP only); c) CSA

2. Focus of the Security Theme
The second focus is called for by the Security theme14 and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available transport and energy infrastructures that survive malicious attacks or accidental failures and guaranteeing continuous provision of services. The following topics are called:

Topic ICT-SEC-2007-1.0-01: Risk assessment and contingency planning for interconnected transport or energy networks
Technical content / scope: The task is to develop integrated frameworks and agreed, common methodologies for (a) global analyses and assessment of risks, failures and vulnerabilities of transport or energy infrastructures, and (b) management and contingency planning based on the compilation and analyses of emergency plans, to ensure interoperability between interconnected and interdependent heterogeneous transport or energy infrastructures.

Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic ICT-SEC-2007-1.0-02: Modelling and simulation for training
Technical content / scope: Security crises concerning cross-border interconnected European transport or energy infrastructures can lead to effects with high impacts of disruption. The task consists of modelling & simulation including scenario building for handling security incidents to support the training of crisis managers.*15*

Funding scheme(s): Collaborative project.

Topic ICT-SEC-2007-1.0-03: Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures
Technical content / scope: The task consists of developing tools that integrate smart surveillance information from interconnected and heterogeneous transport or energy infrastructures in order to build up high-level situation awareness. The objective is to enable optimized decision-making required for cross-border interoperable crisis management to ensure secure, resilient and always available transport or energy infrastructures.*16*

Funding scheme(s): Collaborative project.

14 For more details concerning these topics consult the Security Work Programme
15 See also COM(2005) 576 final. Green Paper on a European Programme for Critical Infrastructure Protection
16 Same as previous footnote

Topic ICT-SEC-2007-1.0-04: ICT support for first responders in crises occurring in critical infrastructures
Technical content / scope: The task consists of developing novel technologies for personal digital support systems as part of an integral, secure emergency management system to support first responders in crises occurring in various types of critical infrastructures under all circumstances. The action has to build upon ongoing research on emergency management, secure wireless ommunication, first responder technologies, etc. See as well topic *SEC-2007-4.3.4 Personal equipment* with a view to compatibility and complementarity*17*.

Funding scheme(s): Collaborative project.

Expected impact:
- Significant improvement in the security, performance, dependability and resilience of complex and interdependent critical infrastructures while considering as well organisational dynamics, human factors, societal issues and related legal aspects.
- Reinforce European industry's potential to create important market opportunities and establish leadership.
- Contribution to establishing, strengthening and preserving trust in the use of technologies for the protection of critical infrastructures. This includes creating sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding potential classification requirements, international co-operation needs, communication and implementation strategies etc.), in order to ensure acceptance of such technologies by relevant stakeholders.
- More effective protection through enhanced co-operation, coordination and focus across Europe, and contribution to the development and promotion of metrics, standards, evaluation and certification methods and best practice in security of critical infrastructures.

Indicative budget distribution13
- 40 M€: 20 M€ for specific focus 1 provided by the ICT theme and 20 M€ for specific focus 2 provided by the Security theme.
- A minimum of 90% of the call budget is foreseen to be allocated to collaborative projects of a typical size in the range of 2-5 M€ (total cost) and a duration of 2-4 years.
- Up to 10 % of the call budget is foreseen to be allocated to coordination and support actions (CSAs) of an average size of 0.5 M€.
- Out of the Security theme's budget, an indicative 1 M€ is available for international cooperation.

Call
FP7-ICT-SEC-2007-1

17 For more details concerning this topic consult the Security Work Programme

Call title: ICT Call 1
Call identifier: FP7-ICT-2007-1
Date of publication: 22 December 2006*40*
Closure date: May 8, 2007, at 17:00, Brussels local time*41*
Indicative budget39: 1194 M€
Topics called:

Challenge	Objectives	Funding schemes[42]
Challenge 1: Pervasive and Trusted Network and Service Infrastructures	ICT-2007.1.1 The network of the future	CP, NoE, CSA
	ICT-2007.1.2 Service and software architectures, infrastructures and engineering	CP, NoE, CSA
	ICT-2007.1.3 ICT in support of the networked enterprise	CP, CSA
	ICT-2007.1.4 Secure, dependable and trusted infrastructures	CP, NoE, CSA

40 The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.
41 At the time of the publication of the call, the Director-General responsible may delay this deadline by up to two months
42 Each proposal must indicate the type of funding scheme used (IP or STREP for CP, where applicable; CA or SA for CSA, where applicable – see Appendix 2)

	ICT-2007.1.5 Networked media	CP, NoE, CSA
Challenge 2: Cognitive systems, interaction, robotics	ICT-2007.2.1 Cognitive systems, interaction, robotics	CP, NoE, CSA (CA only)
Challenge 3: Components, systems, engineering	ICT-2007.3.1 Next generation nanoelectronics components and electronics integration	CP, NoE, CSA
	ICT-2007.3.2 Organic and large-area electronics and display systems	CP, NoE, CSA
	ICT-2007.3.3 Embedded systems design	CP (STREP only), NoE, CSA
	ICT-2007.3.4 Computing systems	CP (STREP only), NoE
Challenge 4: Digital libraries and content	ICT-2007.4.1 Digital libraries and technology-enhanced learning	CP, NoE, CSA
	ICT-2007.4.2 Intelligent content and semantics	CP, NoE, CSA
Challenge 5: Towards sustainable and personalised healthcare	ICT-2007.5.1 Personal health systems for monitoring and point-of-care diagnostics	CP (IP only), CSA
	ICT-2007.5.2 Advanced ICT for risk assessment and patient safety	CP, CSA
Challenge 6: ICT for mobility, environmental sustainability and energy	ICT-2007.6.1 ICT for the intelligent vehicles and mobility services	CP, CSA
Challenge 7: ICT for independent living and inclusion	ICT-2007.7.1 ICT and ageing	CP, CSA
Future and emerging technologies	ICT-2007.8.1 Nano-scale ICT devices and systems	CP, CSA (CA only)
	ICT-2007.8.2 Pervasive adaptation	CP, CSA (CA only)
	ICT-2007.8.3 Bio-ICT convergence	CP, CSA (CA only)
Horizontal support actions	ICT-2007.9.1 International-cooperation	CSA

Evaluation procedure:

- A one-stage submission procedure will be followed.
- The general eligibility criteria as well as evaluation criteria and sub-criteria (including weights and thresholds) for the different funding schemes are set out in Annex 2 to this work programme.
- Indicative evaluation and contractual timetable: It is expected that the contract negotiations for the shortlisted proposals will start as of June/ July 2007.
- Consortia agreements: Participants in all actions resulting from this call are required to conclude a consortium agreement.
- Particular requirements for participation, evaluation and implementation: See Appendix 1
- The forms of grant which will be offered are specified in Annex 3 to the Cooperation work programme.

Call title: ICT Call 2
Call identifier: FP7- ICT -2007-2
Date of publication*43*: May/June 2007
Closure date*44*: Sep/Oct 2007
Indicative budget39: 477 M€
Topics called:

Challenge	Objectives	Funding schemes[45]
Challenge 1: Pervasive and Trusted Network and Service Infrastructures	ICT-2007.1.6 New paradigms and experimental facilities	CP, NoE, CSA
Challenge 3: Components, systems, engineering	ICT-2007.3.5 Photonic components and subsystems	CP, NoE, CSA
	ICT-2007.3.6 Micro/nanosystems	CP, NoE, CSA
	ICT-2007.3.7 Networked embedded and control systems	CP (STREP only), NoE, CSA
Challenge 5: Towards sustainable and personalised healthcare	ICT-2007.5.3 Virtual physiological human	CP, NoE, CSA
Challenge 6: ICT for mobility, environmental sustainability and energy	ICT-2007.6.2 ICT for cooperative systems	CP, NoE, CSA
	ICT-2007.6.3 ICT for environmental management and energy efficiency	CP, CSA
Challenge 7: ICT for independent living and inclusion	ICT-2007.7.2 Accessible and inclusive ICT	CP, CSA

43 The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication.
44 At the time of the publication of the call, the Director-General responsible may delay this deadline by up to two months
45 Each proposal must indicate the type of funding scheme used (IP or STREP for CP, where applicable; CA or SA for CSA, where applicable)

Evaluation procedure:

- A one-stage submission procedure will be followed.
- The general eligibility criteria as well as evaluation criteria and sub-criteria (including weights and thresholds) for the different funding schemes are set out in Annex 2 to this work programme.
- Indicative evaluation and contractual timetable: It is expected that the contract negotiations for the shortlisted proposals will start as of December 2007/January 2008.
- Consortia agreements: Participants in all actions resulting from this call are required to conclude a consortium agreement.
- Particular requirements for participation, evaluation and implementation: See Appendix 1
- The forms of grant which will be offered are specified in Annex 3 to the Cooperation work programme.

Call title: Joint Call ICT & Security 1 (FP7-ICT-SEC-2007-1)
Call identifier: ICT-SEC-2007-1
Date of publication *54*: 30 August 2007
Deadline*55*: 29 November 2007, at 17.00 h Brussels local time
Indicative budget39: The indicative call budget is foreseen to be 40 M€, provided by the ICT theme (20 M€) for actions addressing the specific focus 1 and by the Security theme (20 M€) for actions addressing the specific focus 2.

Out of the Security theme's budget (20 M€), an indicative 1 M€ is available for international co-operation.

53 It is planned that the call will subsequently be extended beyond 31/12/2008, at which time:
- the fifth *full* and CA proposal cut-off date may be revised
- the sixth *full* and CA proposal cut-off date will be fixed
- the sixth end date for *short* proposal submission may be revised

54 The Director-General responsible for the call may publish it up to one month prior to or after the envisaged date of publication
55 Where the envisaged date of publication is either advanced or delayed, the deadline may be adjusted accordingly

Topics called:

Activity/ Area *ICT THEME*	Topics called	Funding Schemes
Pervasive and Trusted Network and Service Infrastructures / Critical Infrastructure Protection	ICT-SEC-2007.1.7: Technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures	*Collaborative project and Coordination and support action*

Activity/ Area *SECURITY THEME*	Topics called	Funding Schemes
Security systems integration, inter-connectivity and interoperability	Topic ICT-SEC-2007-1.0-01 Risk assessment and contingency planning for interconnected transport or energy networks	*Collaborative project and Coordination and support action*
	Topic ICT-SEC-2007-1.0-02 Modelling and simulation for training	*Collaborative project*
	Topic ICT-SEC-2007-1.0-03 Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures	
	Topic ICT-SEC-2007-1.0-04 ICT support for first responders in crises occurring in critical infrastructures	

Evaluation procedure:
A one-stage submission procedure will be followed.
Proposals will be evaluated in a single-step procedure.

Indicative evaluation and contractual timetable: Evaluations of proposals are expected to be carried out during the month of January 2008. It is expected that the contract negotiations for the shortlisted proposals will be open from March to July 2008.

Consortia agreements are required for *all* actions.

Particular requirements for participation, evaluation and implementation:
The minimum number of participating entities required, for all funding schemes, is set out in the Rules for Participation: For Collaborative projects, the minimum condition shall be the participation of 3 legal entities, each of which is established in a Member State or Associated Country and no two of which are established in the same Member State or Associated Country. For Coordination and Supporting Actions aiming at *supporting* research activities and policies the minimum condition shall be the participation of one legal entity. For Coordination and Supporting Actions aiming at *coordinating* research activities and policies the minimum condition shall be the participation of three legal entities, each of which is established in a Member State or Associated Country, and no two of which are established in the same Member State or Associated Country.

Proposers should indicate in which of the two specific foci of the call their proposal best fits. There will be a joint evaluation of proposals submitted under the two specific foci. During the evaluation, evaluators could move, in a transparent manner, proposals from one specific focus to the other, if they consider that a proposal would fit better there and that this would be to the benefit of the proposers.

Proposals must not contain any classified information (note that the proposed action itself *can* involve classified information). If classified inputs are required to carry out a proposed action or the output of the action needs to be classified, proposers have to ensure *and provide evidence* of the clearance of all relevant persons and facilities. Consortia have to clarify issues such as e.g. access to classified information or export or transfer control with the national authorities of their Member States / Associated Countries prior to submitting the proposal.

Proposals need to provide a *security aspect letter,* indicating the levels of classification required. Appropriate arrangements have to be included in the consortium agreement. Proposers addressing topics of the specific focus 2 and claiming that their proposal should receive Community funding up to 75% should demonstrate in the proposal that the required conditions (very limited market size and a risk of "market failure", the need for accelerated equipment development in response to new threats) apply. The final decision will be based on the recommendations of the relevant evaluation panel. Consortia are strongly encouraged to actively involve SMEs and end users. Their presence in the consortia will be judged under the evaluation criterion ‘Quality and efficiency of the implementation and the management’ with a view to meeting the main objectives of the theme.

The evaluation panel will comprise end users as well.
The general eligibility criteria as well as evaluation criteria and sub-criteria (including weights and thresholds) for the different funding schemes are set out in Annex 2 to this work programme.

Positively evaluated proposals involving sensitive and classified information, those involving international co-operation as well as those collaborative projects where 75% funding for all participants is foreseen will be flagged to the members of the Security Programme Committee configuration and dealt with according to its Rules for Procedure.

As a result of the evaluation, a ranked list of proposals retained for funding will be drawn up as well as a reserve list of proposals that may be funded in case budget becomes available during negotiations. The forms of grants which will be offered are specified in Annex 3 to the Cooperation work programme.

Appendix 2: Funding schemes

1. Collaborative projects (CP)
Support to research projects carried out by consortia with participants from different countries, aiming at developing new knowledge, new technology, products, *demonstration activities* or common resources for research. The size, scope and internal organisation of projects can vary from field to field and from topic to topic. Projects can range from small or medium-scale focused research actions to *large-scale* integrating projects for achieving a defined objective. *Projects may also be targeted to special groups such as SMEs.*

The Funding Scheme allows for two types of projects to be financed:
a) "*small or mediumscale focused research actions",* b) *"large-scale integrating projects*".

a) *Small or medium-scale focused research actions* (**STREP**)
Targeting a specific objective in a sharply focussed approach; they shall have a fixed overall work plan where the principal deliverables are not expected to change during the lifetime of the project.

Their content will consist of either of the following two, or a combination of the two:
a) a research and technological development project designed to generate new knowledge which would improve European competitiveness and/or address major societal needs
b) a demonstration project designed to prove the viability of new technologies offering potential economic advantage but which cannot be commercialised directly (e.g. testing of product-like prototypes) and naturally
c) project management activities.
Such type of projects could also include innovation-related activities, in particular with respect to the management of the knowledge produced and the protection of intellectual property.

b) *Large-scale integrating projects* (**IP**)
Larger scale actions, including a coherent integrated set of activities tackling multiple issues and aimed at specific deliverables; there will be a large degree of autonomy to adapt content and partnership and update the work plan, whereas appropriate.
Their content will consist of a combination of most or all of the following (indents a and/or b being a must):
a) objective-driven research and development, i.e. clearly defined scientific and technological objectives, aiming at a significant advance in the established state-ofthe- art; in addition, typically of multidisciplinary character
b) a demonstration project designed to prove the viability of new technologies offering potential economic advantage but which cannot be commercialised directly (e.g. testing of product-like prototypes)
c) innovation activities relating to the protection and dissemination of knowledge, socioeconomic studies of the impact of that knowledge, activities to promote the exploitation of the results, and, when relevant, "take-up" actions; these activities are inter-related and should be conceived and implemented in a coherent way
d) training of researchers and other key staff, research managers, industrial executives (in particular for SMEs), and potential users of the knowledge produced within the project. Such training activities should contribute to the professional development of the persons concerned
e) any other specific type of activity directly related to the project's objectives (as identified in the relevant work programme or call for proposals)
f) project management activities.

2. Networks of Excellence (NoE)
Support to *a Joint Programme of Activities* implemented by a number of research organisations integrating their activities in a given field, carried out by research teams in the framework of longer term co-operation. The implementation of *this Joint Programme of* Activities will require a formal commitment from the organisations integrating part of their resources and their activities.

The funding scheme will support the long-term durable integration of research resources and capacities (researchers, services, teams, organisations, institutions) in fields of strategic importance for European research, through the establishment of a single virtual centre of research, in order to

overcome demonstrable, detrimental fragmentation, thus strengthening European scientific and technological excellence on a particular research topic.

Networks of Excellence will aim at consolidating or establishing European leadership at world level in their respective fields by integrating at European level the resources and expertise needed for the purpose. This will be achieved through the implementation of a Joint Programme of Activities (JPA) aimed principally at creating a progressive and durable integration of the research capacities of the network partners while at the same time advancing knowledge on the topic.

Since Networks of Excellence are aimed at tackling fragmentation of existing research capacities, they should be implemented provided that:

- research capacity is fragmented in the (thematic) area being considered;
- this fragmentation prevents Europe from being competitive at international level in that area;
- the proposed integration of research capacity will lead to higher scientific excellence and
- more efficient use of resources.

The implementation of the Joint Programme of Activities will require a formal commitment from the organisations integrating part or the entirety of their research capacities and activities.

The Joint Programme of Activities (JPA) is the collective vehicle for achieving the durable integration of the research resources and capacities of the Network of Excellence. In order to do so, the JPA should consist of a coherent set of integrating activities that the participants undertake jointly. The JPA will have several components:

- activities aimed at bringing about the integration of the participants research activities on the topic considered, such as:
  - establishing mechanisms for co-ordinating and eventually merging the research
  - portfolios of the partners
  - staff exchange schemes
  - complete or partial relocation of staff
  - establishment of shared and mutually accessible research equipment, managerial
  - and research infrastructures, facilities and services
  - exploration of the legal requirements (facilitators/barriers) for durable integration,
  - setting up of joint supervisory bodies
  - measures for joint public relations …
- jointly executed research to support the durable integration, e.g. systemic development, or development of common tools, or at filling gaps in the collective knowledge portfolio of the network, in order to make the research facilities useable by the network. (NB: in addition to this research, participants in a network will pursue their “own institutional portfolio”, including research, development or demonstration in the area covered by the network itself. The latter research, development or demonstration activities are not part of the “joint programme of activities” and thus will not be part of the eligible costs of the network)
- activities designed to spread excellence, such as:
  - The main component of these activities will be a joint training programme for researchers and other key staff;
  - Other spreading of excellence activities may include: dissemination and communication activities (including public awareness and understanding of science), and, more generally, networking activities to help transfer knowledge to teams external to the network.
  - Spreading of excellence may also include the promotion of the results generated by the network; in such a context, networks should, when appropriate, include innovation-related activities (protection of knowledge generated within the network, assessment of the socio-economic impact of the knowledge and technologies used and development of a plan for dissemination and use of knowledge), as well as any appropriate gender and/or ethical related activities
- all the network’s activities should be carried out within a coherent framework for the management of the consortium linking together all the project components and maintaining communications with the Commission.

3. Coordination and support actions (CSA)
Support to activities aimed at coordinating or supporting research activities and policies (networking, exchanges, trans-national access to research infrastructures, studies, conferences, etc). These actions may also be implemented by means other than calls for proposals.

The Funding Scheme allows for two types of actions to be financed: a) "*co-ordination or networking actions",* b) *"specific support actions*"

a) *Coordination or networking actions* (**CA**)
Coordinating or networking actions will always have to be carried out by a consortium of participants, normally three from three different countries.

The coordination or networking actions cover the following activities:
the organisation of events - including conferences, meetings, workshops or seminars -, related studies, exchanges of personnel, exchange and dissemination of good practices, and, if necessary, the definition, organisation and management of joint or common initiatives together of course with management of the action.

The coordination and networking actions normally stretches over a longer period.

b) *Specific support actions* (**SA**)
Specific support actions may be carried out by a single participant, which can be based in any member state, associated country or a third country. Therefore there are no restrictions on the size of the consortium.

Although normally awarded following calls for proposals, there are also the possibilities to award specific support actions through public procurement carried out on behalf of the Community or to grant support to legal entities identified in the Specific Programmes or in the work programmes where the Specific Programme permits the work programmes to identify beneficiaries.

The objective of specific support actions are to contribute to the implementation of the Framework Programmes and the preparation of future Community research and technological development policy or the development of synergies with other policies, or to stimulate, encourage and facilitate the participation of SMEs, civil society organisations and their networks, small research teams and newly developed or remote research centres in the activities of the thematic areas of the Cooperation programme, or for setting up of research intensive clusters across the EU regions.

The specific support actions can be of different types covering different activities:

- monitoring and assessment activities, conferences, seminars, studies, expert groups, high level scientific awards and competitions, operational support and dissemination, information and communication activities, support for transnational access to research infrastructures or preparatory technical work, including feasibility studies, for the development of new infrastructures, support for cooperation with other European research schemes, the use by the Commission of external experts, management or a combination of these.