**Date d'ouverture de l'appel à projets de recherche :**
**Vendredi 12 Janvier 2007**

# Programme
# "Sécurité et Sûreté Informatique"

## SESUR

# Appel à projets 2007

## Date limite d'envoi des projets de recherche :
## Mardi 27 mars 2007 à midi

Mots clés :
1. Sécurité des systèmes d'information
2. Sûreté des systèmes informatisés
3. Justification de la confiance
4. Aspects sociétaux de l'informatique sécuritaire

La mise en œuvre de l'appel à projets est réalisée par le CEA, qui a été mandaté par l'ANR pour assurer la conduite opérationnelle de l'évaluation et l'administration des dossiers d'aide.

# INFORMATIONS IMPORTANTES

Dates :

Date limite d'envoi des projets sous forme électronique : Mardi 27 mars 2007 à midi, à l'adresse :
anr-sesur@cea.fr

et

Date limite d'envoi des projets sous forme papier : Mardi 3 avril 2007 à minuit (cachet de la poste faisant foi), à l'adresse :
DPg/ANR-CI – Appel à projets SESUR 2007
CEA/Saclay
Boîte 61 - Bât. 474
91191 Gif-sur-Yvette Cedex

Contacts :

Correspondants dans l'unité support de l'ANR (CEA/Délégation ANR Informatique et Simulation) :

- pour toute information concernant l'appel à projets (AAP) :
  Françoise ANGRAND, anr-sesur@cea.fr, 01-69-08-73-81
  Valérie BELLE, valerie.belle@cea.fr, 01-69-08-96-35
- pour toute information de nature administrative et financière :
  Pascal PAVEL, pascal.pavel@cea.fr, 01-69-08-53-41
- site web : http://www-anr-ci.cea.fr (FAQ)

Responsable de programme ANR : Bertrand BRAUNSCHWEIG

Il est recommandé aux déposants :

1. de lire attentivement l'ensemble du présent document et le règlement relatif aux modalités d'attribution des aides de l'ANR avant de déposer un projet de recherche,
2. de ne pas attendre la date limite d'envoi des projets pour réaliser leur soumission de projet de recherche par voie électronique,
3. de consulter si besoin les correspondants de l'unité support mentionnés ci-dessus (de préférence par courrier électronique) ainsi que la FAQ maintenue sur le site web de l'unité support.

---

*Le présent document constitue le corps de l'appel à projets 2007 "Sécurité et Sûreté informatique", il est associé à un ensemble de fiches "modèle" à utiliser pour constituer les dossiers de soumission. L'ensemble de ces documents, sont disponibles à partir de la page du présent appel à projets sur le site web de l'ANR (http://www.agence-nationale-recherche.fr). Ce site donne également accès aux documents de référence de l'ANR, dont le "Règlement relatif aux modalités d'attribution des aides de l'ANR" applicable au présent appel à projets.*

*Ce document comporte en annexe la définition de termes fréquemment utilisés. Une * signale dans le texte les termes pour lesquels le lecteur est invité à se reporter à la définition en annexe.*

## Sommaire


1 Contexte et objectif de l'appel à projets ..... 4
1.1 Contexte ..... 4
1.2 Objectifs du programme ..... 5
1.3 Objectifs de l'appel à projets ..... 5
2 Champ de l'appel à projets ..... 7
2.1 Axes thématiques ..... 7
2.1.1 Axe 1 : " Sécurité des systèmes d'information " ..... 7
2.1.2 Axe 2 : " Sûreté des systèmes informatisés " ..... 8
2.1.3 Axe 3 : " Justification de la confiance " ..... 10
2.1.4 Axe 4: " Aspects sociétaux de l'informatique sécuritaire " ..... 11
2.2 Caractéristiques des projets attendus ..... 12
2.2.1 Caractéristiques nécessaires ..... 12
2.2.2 Autres caractéristiques ..... 13
3 Critères d'éligibilité et de sélection des projets ..... 14
3.1 Critères d'éligibilité ..... 14
3.2 Critères d'évaluation et de sélection ..... 14
4 Modalités de financement des projets ..... 16
5 Modalités relatives aux pôles de compétitivité ..... 17
6 Modalités de soumission ..... 18
6.1 Dossier de soumission ..... 18
6.1.1 Informations générales relatives au projet (fiches A, C et D) ..... 18
6.1.2 Description technique détaillée du projet (fiche B) ..... 18
6.1.3 Lettres d'engagement ..... 19
6.2 Informations pratiques pour la soumission, dates limites ..... 19
7 Annexes ..... 21
7.1 Procédure de sélection ..... 21
7.2 Modalités relatives aux pôles de compétitivité ..... 22
7.3 Définitions ..... 23
7.3.1 Définitions relatives aux différents types de recherche ..... 23
7.3.2 Définitions relatives à l'organisation des projets ..... 23
7.3.3 Définitions relatives aux structures ..... 24
7.3.4 Autres définitions ..... 24
7.4 Suivi des projets et diffusion des résultats obtenus ..... 25
7.4.1 Suivi des projets ..... 25
7.4.2 Diffusion des résultats obtenus ..... 25
7.5 Modèles de lettre d'engagement ..... 26
7.6 Grille d'expertise ..... 28

# 1 Contexte et objectif de l'appel à projets

## 1.1 Contexte

La sécurité est depuis toujours une composante cruciale de l'activité humaine en concernant aussi bien la sécurité des personnes que celle des biens et des informations. Mais la situation est aujourd'hui profondément différente de celle d'hier. En effet, l'informatisation de la plupart des activités humaines ne fait que commencer et il est clair que nous vivons actuellement une révolution au moins aussi importante que la révolution industrielle du XIXe siècle. Des conséquences de cette évolution majeure concernent :

- l'urbanisation numérique globale et la quantité extraordinaire de données qui deviennent explicitement accessibles ;
- l'informatisation des systèmes technologiques critiques et/ou complexes ;
- notre dépendance de plus en plus importante envers les logiciels et matériels associés ;
- l'accessibilité aux informations numériques et leur transport ;
- les nouvelles utilisations permises par le développement du corpus des connaissances informatiques ;
- la maîtrise individuelle et sociale des éléments issus de cette révolution.

Une seconde caractéristique fondamentale des questions sécuritaires posées par l'informatisation globale est la transversalité des disciplines concernées. Un exemple typique concerne les protocoles de communication utilisant des primitives cryptographiques. Un procédé cryptographique aussi bon soit-il ne peut être considéré indépendamment de son contexte logique d'utilisation ni de la façon dont il va être matériellement implanté. Cette interdépendance des éléments de sécurité au sens large se retrouve partout, depuis la combinaison classique entre matériel et logiciel, jusqu'à la mise en œuvre juridique tant au niveau national qu'international et passant par l'ergonomie de la sûreté et de la sécurité.

*L'informatisation globale repose donc les questions de sécurité avec une acuité considérable. C'est pourquoi nous adressons ici les questions de la recherche en Sécurité et Sûreté Informatique (SESUR).*

Les questions de sécurité et de sûreté ont été évoquées dans de nombreux rapports, dont début 2006, celui du député Pierre Lasborde "La sécurité des systèmes d'information. Un enjeu majeur pour la France"[1] et plus récemment celui du groupe de travail "recherche et développement" de la commission interministérielle pour la sécurité des systèmes d'information (CISSI) "Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information"[2]. Tous ces documents[3] soulignent l'importance de la maîtrise des éléments fondamentaux de la sécurité et leurs conséquences majeures tant au niveau économique qu'au niveau des citoyens et de l'état.

[1] http://www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf
[2] http://www.ssi.gouv.fr/fr/sciences/fichiers/rapports/rapport_orientation_ssi_2006.pdf
[3] On trouvera aussi à l'url http://setin.loria.fr plusieurs rapports étrangers.

## 1.2 Objectifs du programme

L'objectif de ce programme initié avec les appels à projets Sécurité des Systèmes embarqués et Intelligence Ambiante (SSIA) en 2005 et Sécurité et Informatique (SETIN) en 2006 est de dynamiser la recherche sur l'ensemble des aspects de la sécurité et de la sûreté des systèmes informatiques et des systèmes technologiques complexes (aspects scientifiques, juridiques, stratégiques et sociétaux). Les défis à relever sont interdépendants et pourront être abordés spécifiquement ou plus globalement. Ils concernent :

- la **sécurité des systèmes d'information** au sens large. Ici, la sécurité comprend en particulier celle des systèmes, des logiciels, des protocoles, des architectures globales, des composants matériels, des réseaux tant filaires ou optiques que radios, des équipements d'extrémités, des moyens de stockage de l'information. Il s'agira de développer les concepts et techniques permettant d'innover, de mieux comprendre, de maîtriser ces questions. Par ailleurs, il faudra prendre en compte les caractères distribué, ouvert, mobile, ubiquitaire, de beaucoup de systèmes qui complexifient le problème et la recherche de solutions.
- la sécurité des informations et des systèmes est étroitement liée à leur sûreté. Il s'agira donc de développer toutes les recherches en **sûreté de fonctionnement des systèmes technologiques critiques et/ou complexes**. En effet, les méthodes, outils et techniques utilisés pour protéger un système contre les effets de certaines actions délibérées ou pour résister aux fautes accidentelles (physiques, de conception, d'interaction) par prévention et/ou par tolérance, ainsi que l'évaluation de mesures de la sûreté (fiabilité, disponibilité, *etc*.) et celle de la sécurité ont des différences, mais aussi des points communs qu'il est souhaitable d'exploiter dans les systèmes ayant les deux types d'exigences.
- la **confiance, sa mise en place et sa justification**. Les recherches permettant d'aller vers des propriétés prouvables, communicables et vérifiables concernent tous les domaines de la sécurité et contribuent fondamentalement à l'établissement de la confiance. Il s'agira de développer les concepts et les systèmes tant logiques qu'expérimentaux permettant ces validations. Il faudra également aborder la découverte et l'analyse des vulnérabilités en comprenant bien dans quel environnement législatif et éthique cela doit avoir lieu.
- les **aspects sociétaux** intégrant les questions juridiques, législatives, politiques, éthiques fondamentalement concernés par l'élaboration et la mise en place de solution de sécurité et de sûreté. Il s'agit ici d'avoir une recherche pluri-thématique alliant les solutions techniques aux aspects sociétaux ainsi que d'élaborer les éléments de stratégie de politique internationale en sécurité et informatique.

## 1.3 Objectifs de l'appel à projets

Le but de cet appel à projets est de développer des recherches aussi bien de type recherche fondamentale* que de type recherche industrielle*, réalisées par des équipes issues d'organismes de recherche* ou d'entreprises*. Il s'inscrit en complémentarité avec les appels à projets lancés en 2007 par l'ANR dans le cadre des programmes Technologies Logicielles, Télécommunications, Audiovisuel et Multimédia. L'appel à projets sollicite donc des projets novateurs, se situant au meilleur niveau international et contribuant à faire avancer significativement la recherche dans les domaines mentionnés et à renforcer ainsi la place de la France dans ces thématiques de recherche sur les scènes européenne et internationale. Compte tenu des objectifs et positionnements stratégiques décrits ci-dessus, les thèmes de cet appel à projets sont les suivants :

- Sécurité des systèmes d'information ;
- Sûreté des systèmes informatisés ;
- Justification de la confiance ;
- Aspects sociétaux de l'informatique sécuritaire.

*Cet appel vise à couvrir certains points couverts de façon insatisfaisante lors des appels précédents. Ceux-ci dont détaillés au § 2.2.2.*

Une des participations attendues des entreprises est la fourniture d'accès à des systèmes d'information à des fins de recherche, développement et expérimentation sur des applications représentatives.

# 2 Champ de l'appel à projets

## 2.1 Axes thématiques

Étant donné le caractère ouvert de cet appel à projets, les descriptions ci-dessous n'ont pas vocation à être exhaustives. Les quatre thèmes sont par essence fortement complémentaires et la structuration proposée a pour objectif d'en faciliter la présentation. Les projets devront préciser lors de la soumission le(s) champs thématique(s) couvert(s).

### *2.1.1 Axe 1 : " Sécurité des systèmes d'information "*

*Cet axe thématique couvre le domaine "classique" de la sécurité des systèmes d'information: conception de mécanismes, dispositifs, composants, architectures, systèmes, réseaux, protocoles, etc. pour la sécurité.*

Parmi les vulnérabilités induites par la mise en place d'une société profondément informatisée, on trouve tout particulièrement les programmes ou matériels informatiques défectueux i.e. incorrects (bogues) ou hostiles (virus, vers, ...), qui mettent en scène des personnes ou des systèmes inattentionnés, défaillants ou perturbés (sans intention préalable) ou malintentionnés (hostiles), dans un contexte où ils interagissent avec des systèmes (ensemble matériel et logiciel) interconnectés par de multiples canaux de communications. La mise en cause de la sécurité peut provenir non seulement de l'intention de perturber par des actions de sabotage ou de vandalisme des informations ou des services, mais aussi de l'intention de s'approprier illégalement ou de modifier des valeurs monétaires ou des informations économiques, privées, politiques, militaires, policières, etc.

Les enjeux sécuritaires de l'informatique sont omniprésents depuis notre vie quotidienne jusqu'à l'organisation des entreprises, des états et des organisations internationales. Dans ce contexte, les points suivants soulèvent des questions de recherche tant fondamentale qu'appliquée.

Les bases de données constituent un enjeu fondamental puisqu'elles centralisent les connaissances et les compétences des entreprises et des administrations ainsi qu'une quantité croissante de données à caractère personnel. La protection de la confidentialité, de l'intégrité et de la disponibilité des données, l'authentification des accès, la traçabilité des opérations et le contrôle des croisements de données sont des problématiques cruciales

Dans notre vie sociale, la sécurité informatique est amenée à jouer un rôle toujours plus important, par exemple via le vote numérique. De même les données médicales ou juridiques doivent être entourées d'une garantie de confidentialité claire et robuste, la signature électronique doit être garantie en qualité immédiate, mais aussi, de façon fondamentale, dans le temps.

La cryptologie est bien sûr une problématique importante et ses développements sont cruciaux en lien avec ses mises en œuvre coopératives par exemple dans les protocoles et sur les réseaux. Des systèmes de cryptographie quantique doivent être développés pour tirer profit des lois de la physique et fournir la sécurité à long terme. Ceci exige un effort d'intégration, de déploiement des technologies quantiques dans les infrastructures existantes de sécurité. Des techniques de cryptographie classique doivent être modélisées et améliorées en raison de la menace naissante des attaques cryptanalytiques posées par des dispositifs de traitement de l'information quantique.

La biométrie permet une certaine identification. Améliorer ses performances sans alourdir ses interfaces est une problématique importante. Elle permet aussi de mieux contrôler les accès. Mais l'impact sur la vie privée et les libertés individuelles reste à comprendre, à mesurer et à contrôler.

L'informatisation globale concerne bien sûr la sécurité de tous les types de réseaux et de leurs protocoles. Dans le contexte d'une interconnexion totale et permanente et une diffusion massive d'objets autonomes et connectables, il faut assurer une sécurité locale en environnement potentiellement critique (i.e. dans les mains de l'attaquant). Les cartes à puce sont jusqu'à maintenant les objets critiques les plus connus, mais il faut généraliser aux téléphones, terminaux divers et variés, consoles de jeux, baladeurs MP3, capteurs domotiques et environnementaux et, maintenant, aux nouveaux objets nano-technologiques. Cette notion d'objet critique dans les mains de l'attaquant nécessite des développements sécuritaires matériels seuls capables d'implémenter l'idée du "coffre-fort portable".

L'émergence actuelle de "plateformes de confiance," consistant en systèmes logiciels couplés aux matériels appropriés permet d'assurer un degré de sécurité important sur l'accès aux logiciels et aux données. Cela peut par exemple permettre la diffusion de médias tels que musiques, films ou informations[4] de façon fortement contrôlée. L'un des écueils est qu'alors le contrôle de la machine (et donc de ses programmes et de ses données) peut échapper totalement à son utilisateur, par exemple lors de son identification. La conception de tels systèmes, l'étude des systèmes existants, leurs liens fondamentaux avec les couches basses des systèmes et avec le matériel doivent être approfondis.

Pour faire face aux erreurs, aux intrusions et autres anomalies survenant pendant la vie opérationnelle des systèmes informatiques et des systèmes informatisés, il est nécessaire de mettre en place des moyens de détection, de protection et de résilience. La conception et la validation de ces moyens nécessitent à leur tour une bonne connaissance des comportements anormaux auxquels ils seront confrontés. Le recueil de données permettant de caractériser ces comportements revêt alors un intérêt particulier pour lequel il faudra développer des méthodes permettant d'accélérer la collecte de données pertinentes. Il peut s'agir, par exemple, du recueil de données d'attaques et d'intrusions réelles, de l'injection d'erreurs et de fautes simulées, ou encore, de la génération de conditions extrêmes d'utilisation des interfaces fonctionnelles.

Enfin, l'émergence de nouveaux modèles de sécurité tant au niveau symbolique que calculatoire devra être étudiée.

*Les communautés scientifiques concernées par ces thèmes sont en particulier celles de l'informatique, des mathématiques, de l'automatique, des statistiques et de l'apprentissage, de l'électronique et des composants, de l'optique, du traitement du signal.*

### *2.1.2 Axe 2 : " Sûreté des systèmes informatisés "*

*Cet axe thématique traite de toutes les questions de sûreté issues de l'urbanisation numérique ou pour lesquelles les modèles informatiques sont pertinents.*

L'informatique joue un rôle crucial dans la sûreté de fonctionnement des systèmes technologiques critiques et/ou complexes, tels que les centrales nucléaires, les avions et engins spatiaux, les systèmes industriels de production continue (électricité, pétrole, chimie, métallurgie, sidérurgie), les grands ouvrages de génie civil (barrages, ponts, plates-formes pétrolières), les véhicules et les infrastructures des systèmes de transport routiers et ferroviaires. En raison de la diffusion massive

[4] Information pris ici au sens chaîne de diffusion d'informations, *e.g.* France-info, Sky-news, *etc*.

de capteurs de toutes natures, ces systèmes bénéficient à l'heure actuelle d'une instrumentation conséquente, et leur sûreté de fonctionnement passe par la conception d'algorithmes de traitement in-situ des données numériques ainsi disponibles. Sur la base des informations et connaissances disponibles (instrumentation, modèles), il s'agit alors en particulier d'opérer une véritable perception (détection, localisation, diagnostic) et réaction (correction, tolérance, maintenance) par rapport aux événements imprévus, évolutions ou déviations par rapport à un état ou un comportement de référence nominal. Les événements et déviations en question concernent aussi bien le système proprement dit que son environnement humain et technique, en particulier les infrastructures informatiques.

Les liens entre les aspects sécurité (*i.e*. résistant à des actions délibérées) et les aspects sûreté (*i.e*. dont le fonctionnement nominal est validé en particulier face à des fautes induites de manière non délibérée comme l'effet de particules ionisantes ou d'autres perturbations liées à l'environnement opérationnel) sont extrêmement imbriqués. Cette interdépendance pourra être exploitée dans les deux directions.

Par ailleurs, les systèmes informatiques et matériels sur lesquels reposent de plus en plus nos activités deviennent extrêmement complexes tant dans leur conception que dans leur réalisation et leur maintenance. Il faut accroître la maîtrise globale de ces développements de systèmes, combinant au besoin matériels et logiciels pour assurer leur sûreté et, le cas échéant, leur sécurité. Typiquement, des erreurs de programmes sont exploitées pour créer des failles de sécurité, de la même manière qu'une erreur dans la conception informatique d'un système de freinage pourra entraîner des conséquences dramatiques sur la sécurité physique des passagers d'un véhicule.

La sûreté des systèmes informatisés en présence de fautes physiques (« pannes »), de fautes de conception résiduelles (« bogues »), de maladresses ou de malveillances des opérateurs ou des utilisateurs, nécessite la définition et la conception d'architectures résilientes, capables de s'autogérer, de s'auto-protéger et de s'auto-guérir. De telles architectures doivent faire appel à la redondance (existante ou additionnelle, à l'identique ou au contraire, diversifiée) pour masquer les anomalies ou pour récupérer un fonctionnement acceptable après la détection, le diagnostic et l'isolation des anomalies. La détermination des concepts adéquats, la définition et la validation d'algorithmes de résilience et le développement de moyens de mise en œuvre performants posent entre autres défis de rendre résilientes les architectures comportant un nombre potentiellement très grand de processeurs : nano-architectures, architectures de grilles, architectures orientées services ; de faire face au dynamisme (défaillances, mobilité, ...) et à l'hétérogénéité potentielle des systèmes informatiques diffus (réseaux ad hoc, systèmes d'information spontanés, réseaux de capteurs, ...) ; de mettre en place des défenses autogérées (architectures autonomiques) et de prévoir quelles défenses mettre en place pour des systèmes qui s'autogèrent (systèmes autonomes).

Les problèmes induits par les très fortes densités d'intégration et les faibles niveaux d'énergie mis en jeu se traduisent en pratique par des tracas réels quant à l'obtention d'un rendement de production suffisant, voire à de sérieuses difficultés en opération. Il est donc essentiel et maintenant acquis de prévoir des techniques de tolérance aux fautes, destinées à être appliquées, soit en phase de développement, soit en phase opérationnelle, afin d'assurer un niveau de résilience compatible avec un certain nombre d'applications critiques. Ces techniques doivent cependant tenir compte d'un autre risque : le détournement à des fins malveillantes des fonctionnalités offertes ou des dispositifs redondants mis en place pour faciliter le traitement des fautes (par exemple, circuits facilement testables). Il peut s'agir de l'exploitation de droits d'accès privilégiés offerts par un noyau de système d'exploitation ou bien de canaux cachés mis en place à partir de configurations spécifiques de test d'un circuit intégré ou d'une carte complexe. Le souci de prendre en compte simultanément et de façon cohérente les risques induits par les fautes

accidentelles et les malveillances est ainsi une nécessité et un défi à relever pour les années à venir. Les travaux à mener couvrent à la fois les aspects architecture matérielle, le développement des logiciels de base et la validation (par analyse et par expérimentation) des moyens de protection proposés.

Nous assistons à l'émergence de nouvelles techniques de développement d'architectures logicielles dynamiques. Qu'elles soient à base de composants, d'aspects ou de services, leur motivation principale est de rendre ces systèmes adaptables aux évolutions des besoins fonctionnels mais aussi à la configuration du système et aux ressources disponibles, une caractéristique nécessaire pour le déploiement de « l'informatique omniprésente » et « mobile ». Un premier axe d'étude concerne l'utilisation de ces techniques pour l'adaptation des mécanismes de sûreté (de tolérance aux fautes, en particulier) au contexte courant (configuration, ressources, hypothèses et contraintes opérationnelles). Un second axe vise la conception de mécanismes spécifiques aux systèmes dynamiques et à la nature même de leurs architectures. Ces deux axes doivent en outre prendre en considération les techniques de vérification adaptées aux technologies à composants dynamiques.

*Les communautés scientifiques concernées par ces thèmes sont en particulier celles de l'informatique, des mathématiques, de l'automatique, des statistiques et de l'apprentissage, de l'électronique et des composants, du traitement du signal.*

### *2.1.3 Axe 3 : " Justification de la confiance "*

*Cet axe thématique traite de méthodes de preuve, de vérification, de validation, d'évaluation et de certification de la sûreté ou de la sécurité, de façon à définir, évaluer, justifier voire normaliser la confiance.*

La sécurité joue un rôle essentiel dans l'établissement de la confiance. Jusqu'à récemment, les archives d'une entreprise ou les photographies familiales étaient conservées dans un coffre-fort, au fond d'une armoire ou chez un notaire. Il peut en aller tout autrement dans notre société numérique puisque ces archives digitales, outre la question de leur persistance temporelle, ne doivent pas pouvoir être accédées, modifiées ou transmises sans autorisation. Il est fondamental de préserver les notions d'intégrité et d'authentification de ces documents et la confiance qui leur est accordée dépend crucialement de la qualité de la sécurité qui entoure leur accès et leur utilisation. Elle dépend aussi de la transparence des solutions mises en jeu. Cette confiance peut varier dans le temps, en particulier du fait des progrès technologiques. Par exemple, la réalisation de machines basées sur le calcul quantique remettrait complètement en cause la plupart des fondements actuels de la cryptographie et par conséquent notre confiance dans son utilisation.

L'absence de mesure de la confiance d'un système numérique est l'un des obstacles majeurs pour le maintien de réseaux et d'infrastructures de télécommunications dans un état maîtrisé et contrôlé, tant pour leur sécurité que leur sûreté de fonctionnement. Le manque de confiance dans les infrastructures des TIC se manifeste dans toutes les étapes du cycle de vie de celles-ci : à l'exploitation, puisque ces systèmes doivent affronter des attaques intentionnelles ou faire face à des pannes accidentelles, et à la conception de ces systèmes puisque la sécurité ou la robustesse n'ont souvent pas été incluses dès la spécification du système. Les infrastructures et systèmes de communications impliquent des milliers, voire des millions de dispositifs nomades et des mises en œuvre de constructions virtuelles (réseaux virtuels, réseaux de recouvrement) qui fonctionnent à la fois sur le matériel et le logiciel, et sur le réseau et les serveurs.

Les projets pourront aborder toutes les facettes de la problématique de la confiance qui soulève des questions à la fois théoriques et pratiques d'ingénierie. La définition de la confiance :

confiance totale, partielle, déléguée ; les protocoles pour instiller la confiance ; l'étude de la compatibilité et de la modularité des modèles de confiance (basée sur la réputation, la fréquentation ou la surveillance, sur des mécanismes de sécurité ou de redondance) vis-à-vis d'un système, d'un service, d'un réseau, d'un composant matériel ou logiciel, d'une architecture ; les mesures de la confiance en temps réel dans un système ; l'estimation de la confiance par un utilisateur, un exploitant.

L'évaluation et la certification indépendante par une tierce partie de confiance fait partie intégrante de la sécurité et surtout de la garantie et la confiance que peut avoir un utilisateur final (intégrateur, industriel mais aussi citoyen) dans un système de sécurité. Ce volet évaluation/certification est aujourd'hui normalisé (Critères Communs), avec des accords permettant une reconnaissance mondiale des certificats émis. Les applications les plus critiques (bancaire, santé, certains services à péage, *etc*.) utilisent quotidiennement ces schémas. Des adaptations des Critères Communs, ou des spécialisations pour des thèmes donnés comme ce qui est fait pour les cartes à puce, peuvent être envisagées.

La généralisation d'une évaluation/certification indépendante et notamment l'ouverture de ce mécanisme aux PME et startups requièrent des développements en validation de dispositifs tant matériels que logiciels, et ce dans des environnements contrôlés. L'adaptation des méthodes mises au point dans le domaine de la sûreté et de la fiabilité est un axe porteur. La mise au point de systèmes logiques aptes à permettre la mise au point des preuves et certificats joue un rôle crucial dans l'établissement de la confiance démontrable.

Bien que cela pose des questions importantes tant déontologiques et techniques que juridiques et politiques, il ne peut exister de recherche en défense sans une recherche efficace en anticipation des faiblesses potentielles. Ce volet fait partie intégrante de l'évaluation indépendante des systèmes de sécurité. Les projets de plateforme allant dans ce sens et prenant en compte de façon objective et explicite l'ensemble des éléments nécessaires à leur mise en place pourront être proposés.

*Les communautés scientifiques concernées par ces thèmes sont en particulier celles de l'informatique, des statistiques, de l'électronique et des composants, du droit, de l'économie, des sciences politique et géostratégique, de la sociologie et de la psychologie.*

### *2.1.4 Axe 4: " Aspects sociétaux de l'informatique sécuritaire "*

*Cet axe thématique insiste sur l'ensemble des aspects sociétaux soulevés en aval et en amont des questions de sécurité et de sûreté des systèmes d'information.*

Sécurité et informatique étendent et ravivent considérablement les questions de recherche et de nouveaux croisements scientifiques deviennent essentiels.

Les aspects juridiques ont été déjà clairement identifiés et doivent être développés vigoureusement. Il faut également prendre en compte les aspects économiques sous-jacents.

En quelques années, nous sommes passés du "hacking for fun" au "hacking for money". Les moyens mis en œuvre sont différents, les réponses se doivent d'être adaptées. Des communautés malveillantes autrefois séparées unissent leurs forces (ddos[5], phishing, fraude, extorsion d'argent, spam, pédophilie, blanchiment d'argent, *etc*.). Peu d'efforts sont actuellement consacrés à l'évaluation, la modélisation et la quantification de ces menaces. Les chercheurs n'ont souvent que

[5] *distributed denial of service*

des rumeurs ou des grandes phrases de consultants pour comprendre ce qu'il se passe. Une démarche pluridisciplinaire à la fois sociologique et informatique doit être envisagée. De même que tout travail en sûreté de fonctionnement présuppose l'existence de modèles de fautes afin de travailler sur des hypothèses réalistes, il faut disposer d'éléments similaires pour baser les recherches en sécurité et valider les solutions.

Il faut également construire une vision prospective ambitieuse et un positionnement réaliste et efficace au niveau mondial. Il est plus que jamais clair que les frontières numériques n'ont pas grand chose à voir avec les frontières géographiques. Les impacts sur la sécurité comme sur la confiance qui en découlent nécessitent d'impulser des recherches dynamisant la créativité croisée entre sciences politiques et sécurité permettant de comprendre et d'anticiper les problèmes pour maîtriser globalement leur mise en œuvre industrielle, économique, juridique et politique sans négliger que les questions de sécurité restent des questions d'ordre public et relèvent des prérogatives nationales.

L'émergence de l'intelligence ambiante, depuis les "smart objects", calculateurs portables, téléphones, réseaux de capteurs, dans leurs versions macro, micro et maintenant nano, induit des questions sécuritaires à tous les niveaux, en particulier sur la vie privée par l'accumulation et l'usage transparents et massifs de données personnelles. Il faut donc prendre en compte cet aspect dès la conception de nouvelles applications et bien avant leur déploiement, de façon à y intégrer efficacement des technologies de protection de la vie privée (PETs, pour "Privacy-Enhancing Technologies"). Ceci est particulièrement vrai pour l'informatique diffuse (RFID, services basés sur la localisation, réseaux de capteurs, etc.), de par la multiplication des équipements personnels ou portants des informations personnelles sensibles. Il convient en particulier de soutenir le développement de PETs génériques (par exemple, pour permettre aux individus de garder le contrôle de leurs informations personnelles) ou spécifiques d'applications particulières (par exemple, pour minimiser la divulgation d'informations personnelles). Il est important aussi de soutenir des actions pluridisciplinaires sur les aspects légaux et techniques, entre autres sur la façon dont les dépositaires d'informations personnelles peuvent et doivent en protéger la confidentialité et contrôler leur transmission éventuelle aux autorités judiciaires ou gouvernementales.

*En coopération avec les disciplines traitant traditionnellement des questions de sécurité et sûreté, les communautés concernées par ces thèmes sont celles du droit, de l'économie, des sciences politique et géostratégique, de la sociologie, la philosophie et de la psychologie.*

## 2.2 Caractéristiques des projets attendus

### *2.2.1 Caractéristiques nécessaires*

Cet appel soutient des projets de type recherche fondamentale* ou de type recherche industrielle* dont l'objectif est de renforcer l'expertise des équipes françaises dans ces thématiques mais aussi d'associer des spécialistes des STIC et des experts de domaines applicatifs. Les projets devront viser la mise en place d'équipes capables de pérenniser le savoir-faire obtenu, seules ou en coopération. Les projets doivent favoriser le transfert et la mise en œuvre des connaissances, outils et méthodes, au bénéfice d'applications et de communautés susceptibles d'en assurer la diffusion. Lorsque la pérennisation doit se faire au sein d'une communauté s'appuyant sur des "logiciels libres", il convient de préciser la réalité et l'engagement de cette communauté vis-à-vis des résultats visés par le projet. Lorsque la pérennisation repose sur l'utilisation des résultats par des entreprises, il convient d'expliquer le contexte de cette utilisation.

Le personnel intervenant dans le projet peut être du personnel permanent (déjà présent dans l'organisme ou dans l'entreprise) ou non permanent (recruté spécifiquement pour le projet). En ce qui concerne le personnel permanent, seules les personnes intervenant à plus de 20% de leur temps dans un projet peuvent être comptabilisées dans les calculs d'hommes x ans*, les personnes intervenant à moins de 20% du temps ne sont considérées que comme des experts apportant une aide ponctuelle au projet.

### *2.2.2 Autres caractéristiques*

Cet appel concerne également, outre la discipline informatique, les communautés scientifiques en automatique, droit, économie, électronique et composants, mathématiques, optique, science politique et géostratégique, statistique et apprentissage, traitement du signal, sociologie, philosophie, psychologie. Ces aspects pluridisciplinaires seront rappelés dans les axes thématiques détaillés ci-dessus.

Pour les projets de recherche fondamentale*, les partenaires sont en général des organismes de recherche, bien que la présence d'entreprises dans le projet ne soit pas exclue.

Une attention spécifique sera portée par les comités d'évaluation et de pilotage, sur les projets traitant des points suivants :

- Analyse des faiblesses potentielles de sécurité ;
- Couches basse des systèmes et informatique de confiance, i.e. "trusted computing" ;
- Ergonomie de la sécurité ;
- Protection de la vie privée ;
- Méthodes formelles et certification ;
- Réseaux et services de communication ;
- Supervision.

# 3 Critères d'éligibilité et de sélection des projets

Sont décrits ci-après les critères d'éligibilité et d'évaluation utilisés au cours de la procédure de sélection décrite en annexe.

## 3.1 Critères d'éligibilité

Pour être éligible, le projet doit satisfaire les conditions suivantes :

- Le coordinateur du projet ne doit pas être membre du comité d'évaluation du programme.
- Les dossiers sous forme électronique et sous forme papier (les deux documents doivent être identiques) ainsi que les lettres d'engagement doivent être soumis dans les délais, au format demandé et être complets.
- Le projet doit entrer dans le champ de l'appel à projets.
- La durée du projet doit être comprise entre 2 ans et 4 ans.
- Les projets doivent réunir au moins deux partenaires.
- Le partenariat devra être équilibré :
  - Pour tous les projets :
    - Pour aucun partenaire, le total de l'effort envisagé (en hommes x ans*) ne pourra représenter plus de 75 % de l'effort total envisagé pour le projet. Pour un organisme de recherche, des équipes d'un même laboratoire seront considérées comme un partenaire unique.
    - La part de l'aide demandée par un partenaire ne pourra dépasser 70% de l'aide totale demandée.
  - Pour les projets de type recherche industrielle* uniquement :
    - Les projets devront être des projets partenariaux organisme de recherche / entreprise*.
    - Le total de l'effort envisagé (en hommes x ans* pour le personnel permanent et non-permanent) pour chaque catégorie de partenaire ne pourra représenter moins de à 20% de l'effort total envisagé pour le projet, sauf exception dûment justifiée.

**Important : Les dossiers ne satisfaisant pas aux critères d'éligibilité ne seront pas soumis à avis d'expert extérieur et ne pourront en aucun cas faire l'objet d'un financement de l'ANR.**

## 3.2 Critères d'évaluation et de sélection

Les projets seront évalués selon les critères suivants, l'ordre des critères ne préjugeant pas de leur importance relative :

1. Pertinence de la proposition au regard des orientations de l'appel à projets. En particulier :
   - adéquation aux axes thématiques de l'appel à projets (cf. § 2.1),
   - adéquation aux caractéristiques « recommandées » des projets (cf. § 2.2).

2. Qualité scientifique et technique. En particulier :
   - excellence scientifique en termes de progrès des connaissances vis-à-vis de l'état de l'art,
   - caractère innovant, en termes d'innovation technologique ou de perspectives d'innovation par rapport à l'existant,
   - levée de verrous technologiques,
   - cohérence avec les programmes nationaux et internationaux.

3. Impact global du projet pour la recherche et/ou pour l'industrie. En particulier :
   - utilisation ou intégration des résultats du projet par la communauté scientifique ou industrielle, et impact du projet en termes d'acquisition de savoir faire,
   - modalités prévues pour l'exploitation et la dissémination des résultats,
   - pérennité des développements effectués et/ou des équipes constituées.

4. Méthodologie, qualité de la construction du projet et de la coordination. En particulier :
   - faisabilité scientifique et technique du projet (notamment : choix des méthodes),
   - structuration du projet, rigueur de définition des résultats finaux (livrables), identification de jalons,
   - qualité du plan de coordination (expérience, gestion financière et juridique du projet),
   - stratégie de valorisation/diffusion et de protection des résultats du projet, gestion des questions de propriétés intellectuelle.

5. Qualité du consortium[6]. En particulier :
   - niveau d'excellence scientifique ou d'expertise des équipes[7],
   - adéquation entre partenariat et objectifs scientifiques et techniques,
   - complémentarité du partenariat,
   - ouverture à de nouveaux acteurs,
   - rôle actif de PME (pour les projets de recherche industrielle).

6. Adéquation projet-moyens et faisabilité du projet. En particulier :
   - calendrier (y compris des livrables)
   - justification de l'aide demandée (y compris coût de la coordination).

7. Encadrement des doctorants
   - caractère formateur du sujet
   - conditions d'encadrement[8]

En outre, la clarté de la rédaction du dossier, de sa justification, du programme de travail (définition des jalons, des résultats intermédiaires / finaux) sera prise en considération dans l'évaluation.

Les personnes déposant le dossier devront veiller à donner les éléments utiles aux experts et aux membres des Comités pour évaluer les projets selon les critères définis ci-avant[9].

---

*[6] Pour un projet partenarial organisme de recherche/entreprise, la labellisation du projet par un pôle de compétitivité est considérée comme un indicateur de qualité. Cet indicateur sera pris en compte dans le cadre de l'examen par le comité de pilotage. Il est rappelé qu'il n'est pas nécessaire que tous les partenaires d'un projet soient membres du pôle ou localisés dans sa région pour que ce projet puisse bénéficier du label de "projet de pôle".*

*[7] La liste des personnels permanents affectés au projet devra être fournie explicitement, accompagnée de la quotité de temps qu'ils consacreront au projet et d'un "mini-CV" de ces personnels.*

*[8] A ce titre, le dossier de soumission du projet devra comprendre le sujet détaillé de la thèse ainsi que le nom des personnes pressenties pour encadrer cette thèse.*

*[9] Les erreurs suivantes sont à éviter : le manque de justificatifs clairs pour les demandes d'équipements, le manque de démonstration de l'originalité du projet, le manque de démonstration de la pérennité des résultats obtenus, le manque de liste précise des "livrables" du projet, le manque de précision sur le personnel impliqué (quotité, nom pour le personnel permanent ou déjà en place…), les taux de main d'œuvre non conformes à la demande de l'ANR d'afficher uniquement les salaires + charges salariales et patronales.*

## 4 Modalités de financement des projets

Le financement attribué par l'ANR à chaque partenaire sera apporté sous forme d'une aide non remboursable, selon les dispositions du "Règlement relatif aux modalités d'attribution des aides de l'ANR" disponible sur le site internet[10] de l'ANR.

Seuls pourront être bénéficiaires des aides de l'ANR les partenaires résidant en France, les laboratoires associés internationaux des organismes de recherche et des établissements d'enseignement supérieur et de recherche français ou les institutions françaises implantées à l'étranger. La participation de d'organismes de recherche ou d'entreprises étrangers est néanmoins possible dans la mesure où chaque partenaire étranger assure son propre financement dans le projet.

L'objectif est que la majorité des projets reçoivent une aide totale d'un montant compris entre 200 k€ et 1000 k€. Toutefois, il n'est pas exclu d'accorder des aides d'un montant supérieur ou inférieur à cette fourchette.

Important : L'ANR n'attribuera pas d'aides de montant inférieur à 15 000 € à un organisme de recherche* ou à une entreprise*[11].

Pour les entreprises* les taux d'aides maximum sont :

| Dénomination | Taux maximum d'aide pour les PME* | Taux maximum d'aide pour les entreprises autres que PME* |
|---|---|---|
| Recherche fondamentale* | 60% | 50% |
| Recherche industrielle* | 60% | 40% |

Dispositions relatives au financement des personnels temporaires

Des personnes avec des statuts non permanents pourront être recrutées pour mener à bien des travaux liés au projet (stagiaires, CDD, intérim, …). Sauf cas particulier, l'effort correspondant (en hommes x ans*) donnant lieu à un financement ANR ne devra pas être supérieur à celui de la main d'œuvre permanente engagée sur le projet. Le financement de doctorants par l'ANR ne préjuge en rien de l'accord de l'école doctorale.

Suivi :

Les projets financés par l'ANR feront l'objet d'un suivi dont les modalités, ainsi que celles de diffusion des résultats obtenus, sont définies en annexe (§7.4).

[10] *http://www.agence-nationale-recherche.fr/documents/reglementANR.pdf*

[11] *Ainsi, ne sont pas considérés comme "partenaires" d'un projet les entités (organismes de recherche ou entreprises) qui ne demandent aucune aide dans le cadre de leur participation au projet. Celles-ci seront considérées comme des "associés" du projet, en particulier dans la description technique du projet avec l'ajout au dossier de soumission d'un courrier confirmant l'intention de l'associé de participer au projet.*

## 5 Modalités relatives aux pôles de compétitivité

Les partenaires du projet pourront mentionner si le projet fait partie des projets labellisés, ou en cours de labellisation, par un pôle de compétitivité (ou plusieurs, en cas de projet interpôles).

Les partenaires d'un projet labellisé par un (des) pôle(s) de compétitivité et retenu par l'ANR dans le cadre de cet appel à projets pourront se voir attribuer un complément de financement par l'ANR.

Le partenaire coordinateur ou le(s) partenaire(s) concerné(s) devront transmettre à l'ANR et à l'unité support (CEA), pour chaque pôle de compétitivité concerné, un formulaire d'attestation de labellisation dûment rempli et signé par un représentant de la structure de gouvernance du pôle, dans un délai de deux mois maximum après la date limite d'envoi des projets sous forme électronique. La procédure à suivre est décrite en annexe (§7.2).

# 6 Modalités de soumission

## 6.1 Dossier de soumission

Le dossier de soumission à l'appel à projets devra comporter l'ensemble des éléments nécessaires à l'évaluation scientifique et technique du projet.

Ce dossier comprend trois parties à rédiger selon des modèles qui seront disponibles sur le site web de l'ANR sur la page consacrée au présent appel à projets au plus tard le 01-02-07.

### *6.1.1 Informations générales relatives au projet (fiches A, C et D)*

Les informations générales relatives au projet font l'objet de trois fiches "modèle" à compléter :
- **[Fichier modèle : SESUR-07-Fiche-A-C.xls] Fiche d'identité projet (fiche A)** (une pour le projet à rédiger par le coordonnateur) et **fiche partenaire (fiche C)** (une par partenaire)
- **[Fichier modèle : SESUR-07-Fiche-D.xls**] **Informations financières (fiche D)** (une par partenaire)

### *6.1.2 Description technique détaillée du projet (fiche B)*

**[Fichier modèle : SESUR-07-Fiche-B.doc]** Ce document devra être rédigé de préférence en anglais sauf pour les projets pour lesquels l'usage du français s'impose. Au cas où :
- La description scientifique et technique est rédigée en anglais, une traduction en français de la description courte du projet devra être fournie.
- La description scientifique et technique est rédigée en français, le coordinateur du projet concerné devra fournir une traduction en anglais à l'ANR, dans un délai de dix jours, si le comité d'évaluation désigne un ou des experts externes étrangers non francophones pour les expertises.

Le plan demandé[12] est le suivant :

- Description courte du projet (2 pages maximum)
- But du projet (2 pages maximum)
- Contexte et état de l'art (2 pages maximum)
- Partenaires (3 pages maximum)
- Organisation et management du projet (2 pages maximum)
- Structure du projet - description des sous-projets (10 pages maximum)
- Liste des livrables (tableau)
- Résultats escomptés – perspectives (2 pages maximum)
- Propriété intellectuelle
- Justification techniques des moyens demandés

On se reportera à la fiche "modèle" B pour le plan détaillé demandé ainsi que les informations attendues dans ce document.

[12] *Des annexes peuvent être ajoutées si nécessaire.*

### *6.1.3 Lettres d'engagement*

**[Modèle en annexe]** Des lettres d'engagement des organismes ou entreprises concernés (une par partenaire) sont à fournir dans un délai d'un mois après la date limite d'envoi des projets sous forme électronique. Des modèles sont présentés en annexe.

## 6.2 Informations pratiques pour la soumission, dates limites

Chaque projet devra choisir un acronyme comportant au maximum 6 caractères[13]. Les projets seront identifiés par leur acronyme.

Le dossier soumis sous forme électronique devra être composé des fichiers suivants (aaaaaa désigne l'acronyme du projet, xx le numéro du partenaire sachant que le coordonnateur est par convention le partenaire 01) :

- un fichier nommé "aaaaaa-fiche-a-c.xls" (fichier excel) : fiche d'identité projet (A) et fiche partenaire (C) (une par partenaire), ce fichier doit comporter un onglet par partenaire.
- un fichier nommé "aaaaaa-fiche-b.doc" ou ".rtf" (fichier word) : description technique détaillée du projet (B). Les textes explicatifs (arial9) sont à supprimer, les textes ajoutés doivent être en arial11 (style : "normal").
- un fichier nommé "aaaaaa-fiche-d.xls" (fichier excel) : informations financières (D), ce fichier doit comporter un onglet par partenaire.
- un fichier nommé "aaaaaa-dossier.pdf" (fichier acrobat) : dossier complet projet en format PDF comportant dans l'ordre la fiche d'identité du projet, la description technique détaillée du projet, l'ensemble des fiches partenaires, le tableau de synthèse financier (construit automatiquement à partir des fiches financières des partenaires), l'ensemble des fiches financières des partenaires.

Il est indispensable de suivre les consignes qui sont présentes dans les fichiers modèles et en particulier de **ne pas modifier la structure des fichiers Excel** (ne pas ajouter ou supprimer d'onglets, ne pas ajouter ou supprimer de lignes ou colonnes, …), ceux-ci étant exploités par des procédures automatiques.

Le dossier soumis sous forme papier devra comprendre les mêmes éléments que dossier complet électronique du projet, des différences dans le contenu des deux dossiers pourront conduire à déclarer le projet inéligible. Les **versions "papier"**, signées, devront être envoyées en 2 exemplaires agrafés ou reliés, dont l'original. Les lettres d'engagement devront être fournies, en 2 exemplaires dont l'original, au plus tard un mois après la date limite de soumission électronique des dossiers.

Le **dossier sous forme électronique** devra impérativement être envoyé avant le **Mardi 27 Mars (12h)** à l'adresse suivante : anr-sesur@cea.fr. La réception des dossiers électroniques sera confirmée par message électronique envoyé par l'unité support (CEA) au coordonnateur du projet dans un délai maximum de 6 jours ouvrables. Il appartient au coordonnateur du projet de prendre contact d'urgence avec l'unité support (CEA, à l'adresse électronique : anr-sesur@cea.fr) s'il ne reçoit pas le message électronique de confirmation dans les délais indiqués.

[13] *En cas de dépassement, l'acronyme fourni par le projet sera tronqué à 6 caractères.*

Le **dossier sous forme papier** devra être **posté** (pli recommandé avec accusé de réception) au plus tard le **Mardi 3 Avril à minuit** (cachet de la poste faisant foi) à l'adresse suivante :

DPg/ANR-CI – Appel à projets SESUR 2007
CEA/Saclay
Boîte 61 - Bât. 474
91191 Gif-sur-Yvette Cedex

La **lettre d'engagement** devra être **postée** (pli recommandé avec accusé de réception) au plus tard le **Vendredi 27 Avril à minuit** (cachet de la poste faisant foi) à la même adresse.

| **Récapitulatif du planning de soumission** | |
|---|---|
| 27 mars 2007 à 12h | Date limite d'envoi du dossier sous forme électronique (par courrier électronique |
| 3 avril 2007 à minuit | Date limite d'expédition (courrier recommandé A/R) du dossier papier du projet (2 exemplaires) |
| 27 avril 2007 à minuit | Date limite d'expédition (courrier recommandé A/R) des fiches d'engagement des partenaires des projets (2 exemplaires) |
| 27 mai 2007 à minuit | Date limite d'expédition des documents "pôle de compétitivité" (le cas échéant) |

Pour tout renseignement, les personnes à contacter, de préférence par courrier électronique, sont les suivantes

- pour toute information concernant l'appel à projets (AAP) :
  - Françoise ANGRAND,anr-sesur@cea.fr, 01-69-08-73-81
  - Valérie BELLE, valerie.belle@cea.fr, 01-69-08-96-35
- pour toute information de nature administrative et financière :
  - Pascal PAVEL, pascal.pavel@cea.fr, 01-69-08-53-41

# 7 Annexes

## 7.1 Procédure de sélection

Les principales étapes de la procédure de sélection sont les suivantes :

- Examen de l'éligibilité des projets par le comité d'évaluation et désignation des experts extérieurs
- Evaluation des projets par le comité d'évaluation après réception des avis des experts extérieurs
- Examen des projets par le comité de pilotage et proposition d'une liste des projets à financer par l'ANR (liste principale et éventuellement liste complémentaire)
- Etablissement de la liste des projets sélectionnés par l'ANR (liste principale et éventuellement liste complémentaire) et publication de la liste
- Envoi aux coordinateurs des projets non sélectionnés d'un avis synthétisé des comités
- Finalisation des dossiers administratif et financier pour les projets retenus et publication de la liste des projets retenus pour financement

Les rôles respectifs des principaux acteurs de la procédure de sélection sont :

- Le comité d'évaluation, composé de membres des communautés de recherche concernées, français ou étrangers, issus de la sphère publique ou privée, a pour mission d'évaluer les projets et de les répartir dans trois catégories : A (recommandés), B (acceptables), et C (rejetés).
- Les experts extérieurs[14], français ou étrangers, désignés par le comité d'évaluation, donnent un avis écrit sur les projets. Au moins deux experts sont désignés pour chaque projet.
- Le comité de pilotage composé de personnalités qualifiées et de représentants institutionnels a pour mission de proposer à partir des travaux du comité d'évaluation, une liste de projets à financer par l'ANR.

Les dispositions de la charte de déontologie doivent être respectées par les personnes intervenant dans la sélection des projets, notamment les dispositions liées à la confidentialité et aux conflits d'intérêt. La charte de déontologie de l'ANR est disponible sur son site internet (www.agence-nationale-recherche.fr).

Les modalités de fonctionnement et d'organisation des comités d'évaluation et de pilotage sont décrites dans des documents disponibles sur le site internet de l'ANR. La composition des comités du programme est affichée sur le site internet de l'ANR (www.agence-nationale-recherche.fr)

[14] *Il est possible aux partenaires publics ou privés désirant garder leurs projets confidentiels de signaler d'éventuelles restrictions quant au choix de ceux-ci.*

## 7.2 Modalités relatives aux pôles de compétitivité

Le formulaire d'attestation de labellisation d'un projet par un pôle de compétitivité se trouve avec l'ensemble des documents téléchargeables constituant le dossier de soumission.

Le partenaire coordinateur ou le(s) partenaire(s) concerné(s) devront :

- transmettre le formulaire renseigné sous forme électronique à la structure de gouvernance de chaque pôle de compétitivité concerné (un projet interpôles peut faire l'objet d'une labellisation par chacun des pôles concernés) ,
- réceptionner une version papier dûment signée de l'attestation de labellisation, en cas d'accord du pôle pour la labellisation, pour chaque pôle concerné,
- transmettre :
    - o à l'ANR la(les) attestation(s) de labellisation dûment signée(s) par courrier ou par fax (coordonnées indiquées sur le formulaire),
    - o à l'unité support une copie de la(les) attestation(s) de labellisation dûment signée(s) de préférence par télécopie (01-69-08-90-34) ou par courrier[15].

Les attestations dûment signées devront être transmises à l'ANR et à l'unité support dans un délai de **deux mois maximum après la date limite d'envoi des projets sous forme électronique**.

[15] *A la même adresse que celle à utiliser pour l'envoi des dossiers papier.*

## 7.3 Définitions

### *7.3.1 Définitions relatives aux différents types de recherche*

**Recherche fondamentale** : Par ce terme, la Commission Européenne entend « une activité visant un élargissement des connaissances scientifiques et techniques non liées a priori à des objectifs précis industriels ou commerciaux » (JOCE 28/02/2004 L 63/23).

**Recherche industrielle** : Par ce terme, la Commission Européenne entend « la recherche planifiée ou des enquêtes critiques visant à acquérir de nouvelles connaissances, l'objectif étant que ces connaissances puissent être utiles pour mettre au point de nouveaux produits, procédés ou services ou entraîner une amélioration notable des produits, procédés ou services existants » (JOCE 28/02/2004 L 63/23).

**Développement pré-concurrentiel** : Par ce terme, la Commission Européenne entend « la concrétisation des résultats de la recherche industrielle dans un plan, un schéma, ou un dessin pour des produits, procédés ou services nouveaux, modifiés ou améliorés, qu'ils soient destinés à être vendus ou utilisés, y compris la création d'un premier prototype qui ne pourra pas être utilisé commercialement. Elle peut en outre comprendre la formulation conceptuelle et le dessin d'autres produits, procédés ou services ainsi que des projets pilotes, à condition que ces projets ne puissent pas être convertis ou utilisés pour des applications industrielles ou une exploitation commerciale. Elle ne comprend pas les modifications de routine, procédés de fabrication, services existants et autres opérations en cours, même si ces modifications peuvent représenter des améliorations » (JOCE 28/02/2004 L 63/23).

### *7.3.2 Définitions relatives à l'organisation des projets*

Pour chaque projet, un **partenaire coordinateur** unique est désigné et chacun des autres **partenaires** désigne un **responsable scientifique et technique**.

**Partenaire coordinateur** : Organisme de recherche ou entreprise d'appartenance du coordinateur.

**Coordinateur** : Il est le responsable de la coordination scientifique et technique du projet, de la mise en place et de la formalisation de la collaboration entre les partenaires, de la production des livrables du projet, de la tenue des réunions d'avancement et de la communication des résultats. L'organisme auquel appartient le coordinateur est appelé partenaire coordinateur.

**Partenaire** : unité d'un organisme de recherche ou entreprise.

**Responsable scientifique et technique** : Il est l'interlocuteur privilégié du coordinateur et est responsable de la production des livrables du partenaire. Pour l'organisme assurant la coordination générale du projet, le responsable scientifique et technique du projet est en général le coordinateur du projet dans son ensemble. Toutefois, notamment dans le cadre de projets de grande taille, la coordination du projet peut être assurée par une tierce personne de la même entreprise ou du même laboratoire.

**Projet partenarial organisme de recherche / entreprise** : projet de recherche pour lequel au moins un des partenaires est une entreprise, et au moins un des partenaires appartient à un organisme de recherche (cf. définitions au § 3.3 de la présente annexe).

### *7.3.3 Définitions relatives aux structures*

**Organisme de recherche** : Est considéré comme organisme de recherche, une entité, telle qu'une université ou institut de recherche , quel que soit son statut légal (organisme de droit public ou privé) ou son mode de financement , dont le but premier est d'exercer les activités de recherche fondamentale ou de recherche industrielle ou de développement expérimental et de diffuser leur résultats par l'enseignement, la publication ou le transfert de technologie ; les profits sont intégralement réinvestis dans ces activités, dans la diffusion de leurs résultats ou dans l'enseignement ; les entreprises qui peuvent exercer une influence sur une telle entité, par exemple en leur qualité d'actionnaire ou de membre, ne bénéficient d'aucun accès privilégié à ses capacités de recherche ou aux résultats qu'elle produit (Document adopté le 22/11/06 par la Commission Européenne[16]).

**Entreprise** : Est considérée comme entreprise, toute entité, indépendamment de sa forme juridique, exerçant une activité économique. Sont notamment considérées comme telles, les entités exerçant une activité artisanale, ou d'autres activités à titre individuel ou familial, les sociétés de personnes ou les associations qui exercent régulièrement une activité économique (Recommandation 2003/361/CE de la Commission Européenne du 6 mai 2003 concernant la définition des petites et moyennes entreprises[17]).

**Petite et Moyenne Entreprise (PME)** : La définition d'une PME est celle de la Commission Européenne, figurant dans la Recommandation 2003/361/CE de la Commission Européenne du 6 mai 2003[18]). Notamment, est une PME une entreprise autonome comprenant jusqu'à 249 salariés, avec un chiffre d'affaires inférieur à 50 M€ ou un total de bilan inférieur à 43 M€.

### *7.3.4 Autres définitions*

**homme x an** (**h*an**) : quantité de travail fournie par une personne en un an à temps plein. A titre d'exemple, c'est également la quantité de travail fournie par 2 personnes en 6 mois ou par une personne à mi-temps en 2 ans.

[16] *Encadrement communautaire des aides d'État à la recherche, au développement et à l'innovation - http://ec.europa.eu/comm/competition/state_aid/reform/rdi_fr.pdf*
[17] *JO L du 20.5.2003, p. L 124/39*
[18] *JO L du 20.5.2003, p. L 124/39*

## 7.4 Suivi des projets et diffusion des résultats obtenus

### *7.4.1 Suivi des projets*

Chaque projet fait l'objet d'un suivi effectué par l'unité support pour le compte de l'ANR suivant les modalités définies dans les actes attributifs.

Les moyens mis en œuvre pour ce suivi sont en particulier :
- Des comptes rendus intermédiaires semestriels d'avancement
- Un compte rendu final permettant notamment de mesurer l'impact du projet.
- Des visites sur site de l'unité support,
- La participation des proposants à des colloques de suivi organisés par l'unité support.

### *7.4.2 Diffusion des résultats obtenus*

D'une manière générale[19] les projets doivent favoriser une large diffusion des résultats obtenus au sein de la communauté de recherche suivant les modalités définies dans les actes attributifs.

Cette communication peut s'appuyer notamment sur :
- Un site web pour le projet assurant une publication régulière des résultats obtenus.
- Des communications dans des séminaires ou colloques qui pourront être organisés, co-organisés ou soutenus par l'ANR ou l'unité support.

En outre, la mention du support apporté par l'ANR au projet devra être portée sur les publications avec la référence du numéro ANR du projet.

[19] *Sauf nécessité particulière liée notamment la confidentialité des résultats.*

## 7.5 Modèles de lettre d'engagement

*Utiliser l'un des 2 modèles d'engagement donnés plus bas pour les laboratoires publics ou les entreprises et entités de droit privé. Chaque partenaire doit établir un fiche d'engagement sur papier à entête.*

**Modèle à utiliser pour les laboratoires publics**

Après avoir pris connaissance du dossier ci-dessus et du règlement relatif aux modalités d'attribution des aides de l'Agence nationale de la recherche, M……., ayant pouvoir d'engager juridiquement *(…dénomination de l'établissement…)* en qualité de……., déclare :

Je, soussigné, donne mon accord pour la participation du laboratoire au projet (… *nom du projet*) soumis dans le cadre de l'appel à projet ANR-07-SESUR dans les conditions décrites de répartition des tâches et de financement demandé, et garantis les informations données par le coordonnateur du projet nommé ci-dessus.

Fait à…….. le …….

M. (*Prénom et NOM)* de la personne habilitée à engager l'établissement

Signature *(Cachet de l'établissement)*

Visa du Directeur du Laboratoire concerné

M. (*Prénom et NOM)*

Signature

**Modèle à utiliser pour les entreprises/associations ou entités de droit privé**

Après avoir pris connaissance du dossier ci-dessus et du règlement relatif aux modalités d'attribution des aides de l'Agence nationale de la recherche, M……, ayant pouvoir d'engager juridiquement *(…statut et dénomination…)* en qualité de ……, déclare :

Je, soussigné, donne mon accord pour participer au projet (… *nom du projet*) soumis dans le cadre de l'appel à projet ANR-07-SESUR dans les conditions décrites de répartition des tâches et de financement demandé, et garantis les informations données par le coordonnateur du projet nommé ci-dessus. J'atteste sur l'honneur de la régularité de la situation de la (…*statut et dénomination*…) au regard de ses obligations fiscales et sociales.

Fait à…….. le …….

M. *(Prénom et NOM)* de la personne habilitée à engager l'entreprise ou l'entité partenaire

Signature (Cachet de l'entreprise)

Visa du Directeur du Laboratoire concerné

M. (Prénom et NOM)

Signature

## 7.6 Grille d'expertise[20]

| Projet | Expert |
|---|---|
| Acronyme du projet : | Nom :<br>Prénom :<br>Date de l'expertise : |

*Les notes doivent être accompagnées d'un commentaire. Elles seront utilisées avec un poids différent en fonction de la nature du projet : (fondamental, industriel, pré-concurrentiel, plate-forme). Les notes à la rubrique 8 reflètent l'avis général de l'expert. Elles ne résultent pas obligatoirement d'une moyenne pondérée des notes précédentes même si elle doit être en cohérence avec l'impression d'ensemble qui s'en dégage. Le commentaire est susceptible d'être transmis au coordinateur du projet soumis.*

*Le barème est : 5 = excellent, 4 = très bon, 3 = bon, 2 = juste, 1 = médiocre, 0 = éliminatoire ou non éligible.*

| | **Note** |
|---|---|
| **1- Pertinence de la proposition au regard des orientations de l'appel à projets.** | **de 0 à 5** |
| *Justification de la note - commentaires.* | |

| | **Note** |
|---|---|
| **2- Qualité scientifique et technique.** | **de 0 à 5** |
| *Justification de la note - commentaires.* | |

| | **Note** |
|---|---|
| **3- Impact global du projet.** | **de 0 à 5** |
| *Justification de la note - commentaires.* | |

| | **Note** |
|---|---|
| **4- Méthodologie, qualité de la construction du projet et de la coordination.** | **de 0 à 5** |
| *Justification de la note - commentaires.* | |

| | **Note** |
|---|---|
| **5- Qualité du consortium – Niveau d'excellence ou d'expertise des équipes au regard de la proposition.** | **de 0 à 5** |
| *Justification de la note - commentaires.* | |

[20] *La taille des cases réservées aux justifications et commentaires des experts a été réduite pour les besoins de l'intégration de ce formulaire dans le présent document.*

| **6- Adéquation projet – moyens** | |
|---|---|
| 6.1- Les moyens mis en oeuvre sont-ils bien adaptés à la conduite du projet? | **Oui/Non/ Ne sait pas** |
| 6.2- Le montant de l'aide demandée est-il justifié et raisonnable ? | **Oui/Non/ Ne sait pas** |
| 6.3- Les moyens en personnels demandés sont-ils justifiés | **Oui/Non/ Ne sait pas** |
| 6.4- Le montant des investissements et achats d'équipements est-il raisonnable ? | **Oui/Non/ Ne sait pas** |
| 6.5- Les autres postes financiers (consommables, missions, sous-traitance, …) sont-ils raisonnables ? | **Oui/Non/ Ne sait pas** |
| *Justification de vos réponses – commentaires sur le coût du projet* | |

| **7- Questions diverses** | |
|---|---|
| 7.1- La nature du projet (fondamental, industriel, pré-concurrentiel, plate-forme) telle que annoncée est elle conforme ? | Oui/Non/ Ne sait pas |
| 7.2- Si le projet contient le financement d'un doctorant, les conditions requises en terme de caractère formateur du sujet et d'encadrement sont elles remplies ? | Oui/Non/ Ne sait pas |
| *Justification de vos réponses* | |

| **8 - Commentaire général et avis** | **Note** |
|---|---|
| **Avis général sur le projet** | **de 0 à 5** |
| **Recommandation de l'expert concernant le projet** | **à retenir en priorité**<br>**à retenir si possible**<br>**à ne pas retenir** |
| *Commentaires généraux, points forts, points faibles, recommandations, le projet pourrait-il être amélioré en faisant l'objet de modifications ou d'adaptation ? Le cas échéant lesquelles ? (5-20 lignes)*<br>*Ces commentaires sont susceptibles d'être transmis au coordinateur du projet soumis.* | |

| | |
|---|---|
| Je déclare avoir pris connaissance de la charte de déontologie de l'ANR, de l'avoir acceptée et que, autant que je sache, je n'ai aucun conflit d'intérêt, dans l'évaluation de cette proposition<br><br>*Extrait de la charte de déontologie de l'ANR : "Par conflit d'intérêt on entend toute situation où un individu est amené 1) à porter un jugement, 2) à participer à une prise de décision, dont lui-même pourrait tirer un bénéfice direct ou indirect dans le cadre de ses activités de scientifique ou de responsable scientifique"* | Nom :<br><br>Date :<br><br>Signature : |