

Agence Nationale de la Recherche

"Sécurité et Informatique"
(SETIN)

Appel à projets de recherche 2006

Ouverture de l'appel à projets : vendredi 28 Avril 2006

Clôture de l'appel à projets : Jeudi 15 Juin à 12h
(Date limite de soumission électronique)



La mise en oeuvre de l'appel à projets est réalisée par le CEA à qui l'ANR a confié la conduite opérationnelle de l'évaluation et de l'administration des dossiers de subvention.

Sommaire

1	Contexte et objectif de l'appel à projets	3
1.1	Introduction	3
1.2	Objectifs de l'appel à projets	4
1.3	Types de projets attendus.....	5
2	Domaines scientifiques et techniques de l'appel à projets (thèmes).....	6
2.1	Thème 1 : Sécurité des systèmes d'information	6
2.2	Thème 2 : Sûreté des systèmes informatisés	7
2.3	Thème 3 : Justification de la confiance	8
2.4	Thème 4 : Informatique sécuritaire et société	9
3	Éligibilité des projets et critères de sélection	11
3.1	Procédure de sélection	11
3.2	Critères d'éligibilité	11
3.3	Critères d'évaluation et de sélection	11
4	Règles de financement	14
4.1	Taux d'aide	14
4.2	Autres conditions	14
4.3	Dispositions relatives aux pôles de compétitivité	15
5	Suivi des projets et diffusion des résultats obtenus	16
6	Modalités de soumission	17
6.1	Management de projet	17
6.2	Dossier de soumission	17
6.3	Informations pratiques pour la soumission, date limite	18
7	Annexe 1 : Grille d'évaluation.....	20
8	Annexe 2 : Modèle à utiliser pour la description détaillée du projet	25
8	Annexe 3 : Modèle de lettre d'engagement.....	31

1 Contexte et objectif de l'appel à projets

1.1 Introduction

La sécurité a été depuis toujours une composante cruciale de l'activité humaine en concernant aussi bien la sécurité des personnes que celle des biens et des informations.

Notre histoire, ancienne ou récente, regorge de situations où les questions de sécurité de l'information ont joué un rôle fondamental. La sécurité des informations a donc été, est et restera un élément fondamental lié à toute activité humaine. 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 XIX^{ème} siècle. Des conséquences de cette évolution majeure concernent :

- l'urbanisation numérique globale et la quantité extraordinaire de données qui deviennent explicitement accessibles,
- notre dépendance de plus en plus importante envers les logiciels et matériels associés,
- l'accessibilité aux informations numériques et à 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 est omniprésente, depuis la combinaison classique entre matériel et logiciel, jusqu'à la mise en oeuvre 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 l'appel à projets Sécurité et Informatique (SETIN) financera des projets de recherche amont dans ce domaine.

Les questions posées par les questions de sécurité et de sûreté ont été évoquées dans de nombreux rapports, dont très récemment celui de Pierre Lasbordes¹. Tous soulignent l'importance de la maîtrise des éléments fondamentaux de la sécurité et leurs conséquences majeures tant au niveau économique, en particulier pour les PME, qu'au niveau des citoyens et de l'Etat. La Commission Européenne affiche également une priorité importante dans le prochain PCRD pour la recherche sur tous les aspects de la sécurité au sens large.

Dans un contexte scientifique et un cadre international très actif tant du point de vue académique qu'industriel, cet appel à projets sollicite donc des projets novateurs, se situant au meilleur niveau

¹ "La sécurité des systèmes d'information - Un enjeu majeur pour la France", Pierre LASBORDES, Député, Le 26 novembre 2005 (http://www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf).

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.

Cet appel encourage et considérera toute proposition originale sur le thème Sécurité et Informatique en soulignant qu'il concerne également les communautés scientifiques en automatique, droit, économie, électronique et composants, optique, science politique, traitement du signal.

Dans le prolongement des programmes de recherche amont SSIA (en 2005) et des ACI concernant la sécurité (de 1999 à 2004), cet appel à projets vise à développer une recherche fondamentale proposée par toute équipe de recherche, académique ou non. Il s'inscrit donc en complémentarité d'une part des appels à projets de l'ANR « Télécommunications », « Audiovisuel et Multimédia » et « Technologies logicielles », dont l'objectif est de développer les interactions entre recherche académique et entreprises, et d'autre part de l'appel à projets "Concepts, systèmes et outils pour la sécurité globale" de par sa spécificité en lien avec l'informatique et son caractère clairement « amont ».

*La mise en oeuvre de l'appel à projets est réalisée par le **CEA** à qui l'ANR a confié la conduite opérationnelle de l'évaluation et de l'administration des dossiers d'aide. La délégation de ce programme de l'ANR au CEA est mise en place dans le cadre des principes adoptés par le conseil d'administration de l'agence et explicitée sur le site web de l'ANR. Au CEA, l'ensemble des tâches liées à cette délégation est assurée par une unité rattachée à la Direction des Programmes appelée "**Délégation Calcul Intensif**".*

1.2 Objectifs de l'appel à projets

L'objectif de cet appel à projets est de fortement dynamiser la recherche fondamentale sur l'ensemble des aspects scientifique, juridique, politique et sociétale de la sécurité et de la sûreté des systèmes informatiques.

Il s'agit de développer l'expertise des équipes françaises sur ces thématiques pour faire significativement avancer le corpus de connaissance permettant de renforcer notre maîtrise scientifique et technique de ce domaine stratégique. 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 **validation communicable et vérifiable des propriétés de sécurité et de sûreté**. 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 juridiques, politiques, éthiques et sociaux** fondamentalement concernés par l'élaboration et la mise en place de solutions de sécurité et de sûreté. Il s'agit ici d'avoir une recherche pluri-thématique permettant d'élaborer des solutions cohérentes et communicables alliant les solutions techniques aux aspects sociétaux ainsi que d'élaborer les éléments d'une politique internationale en Sécurité et Informatique.

Compte tenu de ces objectifs et positionnements stratégiques, les thèmes de cet appel à projets sont les suivants, sans que l'ordre en soit significatif :

1. la sécurité des systèmes d'information,
2. la sûreté des systèmes informatisés,
3. la justification de la confiance,
4. l'informatique sécuritaire et la société.

1.3 Types de projets attendus

Les projets financés dans le cadre de cet appel sont de type "**recherche fondamentale**" en reprenant la terminologie du journal officiel de l'Union Européenne (JOCE 28/02/2004 L 63/23) : Recherche fondamentale : "activité visant à un élargissement des connaissances scientifiques et techniques non liées à des objectifs industriels et commerciaux".

Les projets attendus, d'une durée de **2, 3 ou 4 ans**, pourront être **structurés** :

- soit en **Projet de recherche sur un domaine commun** d'expertise clairement défini, basé sur la coopération active d'un nombre limité d'équipes,
- soit en **Projet de recherche aux interfaces** : basé sur la coopération active d'équipes de recherche relevant de **champs disciplinaires différents**. Le projet proposera un programme de recherche commun, pluridisciplinaire, basé sur la complémentarité des équipes participantes.
- soit en **Projet de recherche avec infrastructure** : Cet Appel à Projets peut être l'occasion de construire des projets de recherche nécessitant l'acquisition d'équipements hors de portée des financements classiques et pouvant contribuer à l'établissement de plate-formes de haute sécurité. De tels projets, s'appuyant sur un programme de recherche commun, devront être particulièrement argumentés. Le problème des moyens humains indispensables à l'utilisation et la maintenance des équipements devra être abordé, en explicitant les demandes faites dans le cadre de l'Appel à Projets et, le cas échéant, les autres apports.

Une attention particulière sera apportée aux projets susceptibles de fournir des solutions globales aux problèmes posés en favorisant les collaborations et les synergies entre chercheurs d'équipes ou de structures différentes.

2 Domaines scientifiques et techniques de l'appel à projets (thèmes)

S'agissant de projets de recherche fondamentale, les partenaires attendus seront principalement des laboratoires académiques. Toutefois la présence d'entreprises dans les projets n'est pas exclue.

Etant donné le caractère amont 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) ainsi que le domaine d'application dans le cas de projet multi-thématique. Dans tous les cas, un thème majeur devra être indiqué.

2.1 Thème 1 : Sécurité des systèmes d'information

Ce premier thème 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 négligents, défaillants ou perturbés (sans intention préalable) ou des acteurs 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. On pense bien entendu aux virus, ou aux cartes bancaires et au fait qu'elles doivent résister à des utilisations frauduleuses, éventuellement réalisées par des individus avertis. Dans ce contexte, les bases de données sont un enjeu fondamental puisqu'elles centralisent en particulier les connaissances et les compétences des entreprises. L'intégrité des données, l'authentification de leur accès et la traçabilité des opérations 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 électronique. 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.

L'informatisation globale concerne bien la sécurité de tous les types de réseaux et de leurs protocoles. Elle adresse également des systèmes d'armement. Leur informatisation, leur interopérabilité et leur mise en réseau posent des questions de sécurité spécifiques.

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.

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 (par exemple si de tels objets tombent entre les mains de l'attaquant). Les cartes à puce sont jusqu'à maintenant le cas le plus connu, mais il faut généraliser aux téléphones, terminaux divers et variés, consoles de jeux, baladeurs MP3. 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 "plate-formes de confiance", consistant en des 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 musique, films ou informations² 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.

La cryptologie est, bien sûr, une problématique importante et ses développements sont cruciaux en lien avec ses mises en oeuvre coopératives par exemple dans les protocoles et sur les réseaux.

2.2 Thème 2 : Sûreté des systèmes informatisés

Ce thème traite de toutes les questions de sûreté issues de l'urbanisation numérique ou pour lesquelles les modèles informatiques sont pertinents.

L'informatique a 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, plate-forme pétrolières), les véhicules et les infrastructures des systèmes de transport routiers et ferroviaires. En raison de la diffusion massive de capteurs de toutes natures, ces systèmes bénéficient à l'heure actuelle d'une instrumentation importante, 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 ou d'évolutions ou de déviations par rapport à un état ou un comportement de référence normal, souhaitable ou 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

² Information pris ici au sens chaîne de diffusion d'informations, e.g. France-info, Sky-news, etc.

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 aux besoins 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.

2.3 Thème 3 : Justification de la confiance

Méthodes de preuve, vérification, validation, évaluation, certification des thèmes 1 et 2, de façon à 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. La confiance que l'on accorde à de tels documents dépend donc d'une manière cruciale 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'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

Bien que cela pose de très nombreux problèmes 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 plate-forme 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.

D'une manière duale, la confiance est un élément essentiel à la mise en place de la sécurité. Elle joue par exemple un rôle important dans le processus d'identification de personnes ou de machines et dans l'utilisation de procédures et de systèmes sécuritaires.

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 l'élaboration des preuves et certificats jouent un rôle crucial dans l'établissement de la confiance démontrable.

Des adaptations des Critères Communs, ou des spécialisations pour des thèmes donnés comme ce qui est fait pour les cartes à puce, pourront être envisagées.

2.4 Thème 4 : Informatique sécuritaire et société

Ce thème insiste sur l'ensemble des aspects sociétaux soulevés en aval et en amont des questions de Sécurité et Informatique face aux problèmes de sécurité et sûreté.

Sécurité et informatique étendent et ravivent considérablement la problématique et la recherche des domaines scientifiques sous jacents : composants, cryptologie, logique et preuve, sûreté, fiabilité pour n'en citer à nouveau que quelques uns, car nous sommes dans une problématique profondément durable, alimentée par une évolution rapide et drastique des menaces sécuritaires.

De nouveaux croisements scientifiques deviennent par ailleurs essentiels et doivent prendre en compte les éléments suivants:

- Les aspects juridiques ont été déjà clairement identifiés et doivent être développés vigoureusement, éventuellement en tenant compte des aspects économiques sous-jacents.
- En quelques années, nous sommes passés du "hacking for fun" au "hacking for money". Les moyens mis en oeuvre sont différents, les réponses se doivent d'être adaptées. Des communautés malveillantes autrefois séparées unissent leurs forces (DDoS³, 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. 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.
- La construction d'une vision prospective ambitieuse et d'un positionnement réaliste et efficace au niveau mondial sont importants. Il est plus que jamais clair que les frontières numériques n'ont pas grand chose à voir avec les frontières géographiques. L'impact sur la sécurité comme sur la confiance qui en découle nécessite d'impulser des recherches dynamisant la créativité croisée en sciences politique et sécurité informatique permettant de comprendre et d'anticiper les problèmes pour maîtriser globalement leur mise en oeuvre industrielle, économique, juridique et politique sans négliger le fait que les questions de sécurité restent des questions d'ordre public et relèvent donc 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 de par l'accumulation et l'usage transparents et massifs de données personnelles.

Les projets pourront répondre sur l'un ou plusieurs des points de recherche mentionnés dans la description des thèmes ci-dessus. Ces points n'étant pas exhaustifs, les projets pourront en

³ Deni de service distribué.

développer, d'autres pourvu qu'ils rentrent clairement dans l'un des quatre thèmes. La soumission de projet devra rendre précis le(s) champs thématique(s) couvert(s) ainsi que le domaine d'application dans le cas de projet multi-thématique. Dans tous les cas, un thème majeur parmi les quatre ci-dessus devra être indiqué.

3 Eligibilité des projets et critères de sélection

3.1 Procédure de sélection

La procédure de sélection comprend les étapes suivantes :

- validation d'éligibilité des projets par le Comité d'évaluation et choix des experts,
- examen des projets par les experts⁴,
- examen et classement des projets par le Comité d'évaluation,
- sélection des projets par le Comité de deuxième niveau,
- décision de financement par l'ANR,
- finalisation du dossier administratif et financier pour les projets retenus.

La composition des Comités sera affichée sur le site Internet de l'ANR (<http://www.agence-nationale-recherche.fr>).

3.2 Critères d'éligibilité

- Le dossier doit tout d'abord être soumis dans les délais et au format demandé. **La description courte du projet devra être rédigée en français et en anglais. Il est fortement conseillé de rédiger la *description scientifique et technique détaillée* (annexe technique) en anglais, afin de faciliter l'évaluation qui peut faire appel à des experts étrangers.** Les dossiers devront être complets c'est à dire comprendre toutes les informations demandées.
- Une proposition doit s'inscrire dans le **champ** du présent appel à projets.
- La durée des projets sera de **deux, trois ou quatre ans**,
- **Les partenaires sont au minimum deux⁵.**
- Le partenariat devra être **raisonnablement équilibré** : pour chaque partenaire, l'effort envisagé dans le projet en termes d'hommes-mois ne pourra représenter plus de 70% de l'effort total.

3.3 Critères d'évaluation et de sélection

Les personnes déposant le dossier devront veiller à **donner les éléments utiles aux experts pour évaluer les projets selon les critères définis** ci-après. En particulier le dossier présenté devra

- s'appuyer sur un état de l'art au niveau international et démontrer l'intérêt du projet par rapport à celui-ci,

⁴ Il est possible aux partenaires publics ou privés désirant garder leurs projets confidentiels de signaler d'éventuelles restrictions quant au choix de ceux-ci.

⁵ Dans ce cadre, il faut comprendre deux équipes rattachées à des laboratoires différents.

- présenter les objectifs visés en précisant les résultats escomptés et en listant avec précision les "délivrables" du projet⁶,
- décrire l'organisation coopérative du projet en détaillant les compétences et le rôle des équipes partenaires impliquées dans le projet⁷.

Les projets seront évalués sur plusieurs aspects :

- 1. Pertinence de la proposition au regard de l'appel à projets**
- 2. Qualité scientifique et technique**
 - Excellence scientifique en terme de progrès des connaissances vis-à-vis de l'état de l'art au niveau international.
 - Caractère innovant du projet au regard de l'état de l'art au niveau international.
 - Cohérence avec les programmes nationaux et internationaux.
- 3. Impact du projet**
 - Impact attendu en particulier en terme de retombées pour la recherche.
 - Utilisation ou intégration des résultats du projet par la communauté scientifique ou éventuellement industrielle.
- 4. Méthodologie, qualité de la construction du projet et de la coordination**
 - Positionnement par rapport à l'état de l'art.
 - Structuration du projet, rigueur de définition des résultats finaux, identification de jalons.
 - Qualité du plan de coordination (expérience et gestion financière du projet).
 - Faisabilité scientifique du projet (choix des méthodes, équipements, gestion des risques).
 - Le cas échéant, stratégie de valorisation/diffusion et de protection des résultats du projet, gestion des questions de propriétés intellectuelle.
- 5. Qualité du consortium**
 - Niveau d'excellence scientifique ou d'expertise des équipes au regard de la proposition (compétences, nombre/qualité de publications, de brevets ou de réalisations, qualité des collaborations engagées).
 - Adéquation partenariat et objectifs scientifiques et techniques, complémentarité du partenariat.
 - Ouverture à de nouveaux acteurs.
 - Le cas échéant, rôle actif de PME.
- 6. Adéquation projet – moyens**
 - En particulier, la demande d'aide présentée sur la base des dépenses éligibles devra être justifiée au regard des enjeux du projet, le cas échéant grand poste par grand poste.
- 7. Critères spécifiques pour cet appel**

⁶ Etant donné l'aspect recherche amont du présent appel à projet, les "délivrables" pourront être revus en fonction de l'avancement de la recherche sur une base annuelle.

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.

- Quotité de participation des chercheurs des équipes impliquées et notamment du coordinateur et en regard des objectifs du projet
- Clarté de rédaction du projet, de sa justification, du programme de travail (définition des jalons, des résultats intermédiaires / finaux le cas échéant)

Chaque projet éligible est évalué, sur la base des critères énoncés ci-dessus, a minima par trois experts français ou étrangers indépendants et tenus à la confidentialité comme spécifié dans la charte de déontologie de l'ANR. La grille d'évaluation qu'ils utilisent est donnée en annexe 1.

4 Règles de financement

D'une manière générale, ce sont les dispositions du règlement financier de l'ANR qui sont applicables (<http://www.agence-nationale-recherche.fr/documents/reglementANR.pdf>).

4.1 Taux d'aide

Les financements par l'ANR, seront apportés sous forme d'aides non remboursables. Par ailleurs l'ANR n'attribuera pas d'aides d'un montant inférieur à 20000 € à un partenaire d'un projet⁸.

Pour les entreprises, le taux d'aide maximum est de 60% dans le cas de PME⁹ et de 40% pour les autres entreprises.

Pour les organismes publics et les fondations de recherche, l'aide finance le coût marginal du projet. Il y a une exception à cette règle : pour les laboratoires des établissements publics à caractère industriel et commercial (EPIC) impliqués dans des recherches partenariales¹⁰, l'ANR finance une partie du coût complet de l'opération.

Les dépenses sont calculées hors taxes, majorées le cas échéant pour les laboratoires publics de recherche de la TVA non récupérable.

4.2 Autres conditions

Les bénéficiaires pourront commander des travaux à des tiers extérieurs dans le respect des modalités fixées par le règlement financier de l'ANR

Les aides de l'ANR ne peuvent bénéficier qu'à des partenaires qui résident en France. Les projets peuvent inclure des partenaires qui résident hors de France mais, dans ce cas, ces partenaires doivent assurer leur propre financement.

L'objectif de l'ANR est que la majorité des projets reçoivent une **aide d'un montant compris entre 100 k€ et 500 k€**. Toutefois, l'ANR n'exclut pas d'accorder des aides d'un montant supérieur (notamment pour des projets impliquant des infrastructures) ou inférieur à cette fourchette.

⁸ Ainsi, à l'exception de partenaires avec des équipes associées au projet résident hors de France, ne pourront pas être présentés comme "partenaires" d'un projet les entités qui ne demandent aucune aide dans le cadre de leur participation au projet. Celles-ci pourront être mentionnées comme "associés" au projet, en particulier dans la description technique du projet avec éventuellement l'ajout au dossier de soumission d'un courrier confirmant l'intention de l'associé de participer au projet.

⁹ Une PME est une entreprise comprenant jusqu'à 249 salariés, avec un chiffre d'affaires inférieur à 50 M€ ou un total de bilan inférieur à 43 M€. Les filiales des grands groupes ne sont pas considérées comme des PME.

¹⁰ Par "recherche partenariale", il faut comprendre recherche impliquant au moins une entreprise.

Des CDD peuvent être financés par l'ANR dans la mesure où ceux-ci représentent un appoint pour la réalisation du projet. Dans le cas de CDD correspondant à des étudiants inscrits en thèse, il sera demandé au comité d'évaluation :

1. de vérifier que dans le projet le sujet de thèse et l'encadrement proposés sont satisfaisants,
2. en cas de demandes trop nombreuses, d'indiquer les projets à soutenir (la priorité sera donnée aux projets de thèse visant à former des étudiants dans le domaine de l'informatique).

Ce financement ne préjuge en rien de l'autorisation de l'école doctorale à laquelle l'étudiant en thèse devra s'inscrire.

4.3 Dispositions relatives aux pôles de compétitivité

Le porteur de projet pourra mentionner si le projet constitue tout ou partie d'un des projets labellisés (ou en cours de labellisation) par un pôle de compétitivité (ou par plusieurs, en cas de projet interpôle). Les partenaires d'un projet labellisé par un pôle de compétitivité et retenus par l'ANR dans le cadre de cet appel à projets pourront se voir attribuer un complément de financement par l'ANR.

Le porteur de projet devra fournir la(les) attestation(s) de labellisation signée(s) par un (des) représentant(s) habilité(s) de(des) structure(s) de gouvernance du(des) pôle(s) concerné(s) accompagnée(s) d'une fiche résumé du projet (contenant au minimum le résumé du projet, le nom des partenaires, le montant total du projet et les financements demandés) visée par un (des) représentant(s) habilité(s) de la(des) structure(s) de gouvernance du(des) pôle(s) concerné(s). Ces documents devront être transmis en exemplaire original par courrier et courrier électronique à la structure support au plus tard deux mois après la clôture de l'appel à l'adresse postale indiquée dans l'appel.

Faute de réception de ces documents dans les délais indiqués, aucun complément de financement ne sera accordé.

5 Suivi des projets et diffusion des résultats obtenus

Chaque projet donnant lieu à un financement fait l'objet d'un suivi régulier (qui conditionne le financement), suivant les jalons établis dans l'acte attributif de financement. Le suivi est effectué par la Délégation ANR Calcul Intensif (CEA) avec le cas échéant l'appui de membres du Comité d'Evaluation.

Le principe général de ce suivi est le suivant :

- Les partenaires du projet se réunissent régulièrement et au moins une fois par an à l'initiative du coordonnateur pour faire le point sur l'avancement du projet. Une première réunion (réunion de lancement) a lieu au moment du démarrage du projet. Un compte-rendu succinct de ces réunions est adressé à la Délégation ANR-Calcul Intensif, le responsable de cette délégation pouvant être invité à ces réunions si les participants le souhaitent.
- Des rapports d'avancement sont fournis tous les six mois. Les "livrables" du projet sont, le cas échéant, joints au rapport d'avancement qui suit leur production.
- Le coordonnateur du projet doit suivre l'avancement des travaux des différents partenaires et avertir la Délégation ANR-Calcul Intensif en cas de difficulté ou d'évènement majeur survenant dans le projet.
- Le rapport final d'exécution devra permettre d'évaluer l'impact pour les partenaires et la collectivité nationale du soutien apporté par l'ANR au projet, en particulier en ce qui concerne :
 - les publications,
 - les logiciels,
 - dans le cas de projet multi-thématiques, les relations établies entre équipes de recherche travaillant dans des domaines différents (informatique, automatique, physique, optique, mathématiques appliquées, juridique, domaines applicatifs, ...),
 - les actions de formation, notamment dans le cas de la présence de doctorants de leur devenir.

En outre, les résultats obtenus devront, sauf demande d'exception dûment motivée, faire l'objet d'une large diffusion au sein de la communauté de la recherche. Pour cela, ceux-ci devront être publiés régulièrement sur le site web du projet et fournis, dans le cas de documents de synthèse, pour publication sous une forme appropriée sur le site web du programme "Sécurité et Informatique". Ils feront par ailleurs l'objet de communications dans des séminaires qui pourront être organisés par le programme. La mention du support apporté par l'ANR au projet devra être portée sur les publications.

6 Modalités de soumission

6.1 Management de projet

Pour chaque projet, un partenaire coordonnateur unique est désigné. Il est responsable au niveau du projet de la mise en place et de la formalisation de la collaboration entre les partenaires, de la production des livrables, de la tenue des réunions d'avancement et de la communication des résultats intermédiaires et finaux obtenus par le moyen d'un site web pour le projet.

Chaque partenaire désigne un responsable scientifique et technique unique. Le responsable scientifique et technique du partenaire coordonnateur est en général le coordonnateur du projet dans son ensemble. Toutefois, notamment dans le cadre de projets importants, la coordination du projet peut être assurée par une tierce personne de la même entreprise ou du même laboratoire.

6.2 Dossier de soumission

Les projets doivent être soumis au travers du site web de l'appel à projets SETIN2006. Ce site web permet de saisir les **fiches administratives** et d'annexer la **description détaillée du projet**. Outre cette soumission en ligne, les projets doivent envoyer par courrier postal l'impression papier du dossier final soumis en ligne et imprimé en utilisant les commandes appropriées du site web.

Le dossier de soumission à l'appel à projets comporte 3 parties :

1. Un **formulaire regroupant les informations générales relatives au projet**. Ce formulaire se compose de **3 fiches administratives** :

- Fiche d'identité projet. Cette fiche précise en particulier le type du projet (tels que définis au paragraphe 1.3), le thème principal (tels que définis au chapitre 2) et le cas échéant le ou les thèmes secondaires auxquels le projet se rattache.
- Fiche partenaire (une par partenaire).
- Informations financières (une par partenaire) et Informations financières récapitulatives.

2. Une partie technique donnant en particulier une **description détaillée du projet**. La forme de ce document est indiquée en annexe 2. Il s'agit d'un document PDF en format libre qui doit être annexé sur le serveur de soumission. Il peut être rédigé en français ou en anglais. Dans le cadre de cet appel, il est fortement conseillé que la proposition soit écrite en anglais. Un résumé en français est obligatoire.

Le plan demandé 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)
- Organisation du projet - description des sous – projets (6 à 10 pages)
- Liste des "délivrables" (tableau)
- Résultats escomptés – perspectives (1 à 2 pages)
- Le cas échéant, propriété intellectuelle
- Justification scientifique des moyens demandés

3. Des **fiches d'engagement des organismes ou entreprises concernés**. Ces fiches doivent être fournies dans un délai d'un mois après la date limite de la clôture de l'appel. Les modèles sont présentés en annexe 3.

6.3 Informations pratiques pour la soumission, date limite

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

La **soumission électronique** des dossiers se fera jusqu'au **15 juin 2006 à 12h** sur le site web de l'action recherche amont SI : **<https://SETIN2006.loria.fr>**
La date fixée doit être impérativement respectée.

Afin d'organiser le processus d'évaluation des projets, il est **fortement souhaité** que les projets saisissent avant le **8 juin 2006 à 12h** : le **titre et le résumé du projet ainsi que la liste des partenaires**. Ces informations pourront néanmoins être mises à jour jusqu'à la date de fin de la soumission électronique.

Les **dossiers** doivent être envoyés par courrier pour confirmation (pli recommandé avec accusé de réception) au plus tard le **22 juin 2006 à minuit**, le cachet de la poste faisant foi, à l'adresse suivante :

DPg/ANR-CI – Appel à projets SETIN 2006
CEA/Saclay
Boîte 61 - Bât. 474
91191 Gif-sur-Yvette Cedex

Le dossier soumis sous forme papier devra comprendre les mêmes éléments que le dossier électronique du projet. Les **versions "papier", signées par le coordonnateur du projet**, devront être envoyées en 3 exemplaires agrafés ou reliés, dont l'original.

Les **lettres d'engagement** devront être fournies, en 3 exemplaires dont l'original, au plus tard le **24 juillet 2006 à minuit**, cachet de la poste faisant foi.

Récapitulatif du planning de soumission	
8 juin 2006 à 12h	Date limite (souhaitée) de saisie sur le serveur de soumission du titre, résumé et liste des partenaires du projet.
15 juin 2006 à 12h	Date limite de saisie sur le serveur de soumission du dossier du projet
22 juin 2006 à minuit	Date limite d'expédition (courrier A/R) du dossier papier du projet
24 juillet 2006 à minuit	Date limite d'expédition (courrier A/R) des fiches d'engagement des partenaires des projets
22 août 2006 à minuit	Date limite d'expédition (courrier A/R) des documents "pôle de compétitivité" (le cas échéant)

Pour tout renseignement concernant l'appel à projets, les questions sont à adresser, de préférence par courrier électronique, à

François ROBIN, Responsable de la Délégation ANR-CI au CEA,
 (+33)-1-69-08-53-34,
anr-ci@cea.fr

Pour les questions concernant la soumission en ligne

setintech@loria.fr

7 Annexe 1 : Grille d'évaluation

Projet	Expert
Acronyme du projet :	Nom : Prénom : Date de l'expertise :

Les notes doivent être accompagnées d'un commentaire. Les notes "globales" (pour un aspect de l'évaluation, pour l'ensemble du projet) 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 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.	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

	Note
2- Qualité scientifique et technique	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

	Note
3- Impact du projet	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

	Note
4- Méthodologie, qualité de la construction du projet et de la coordination	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

	Note
5- Qualité du consortium	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

	Note
6.1- Les moyens mis en oeuvre sont-ils bien adaptés à la conduite du projet?	Oui/Non
6.2- Le montant de l'aide demandée est-il justifié et raisonnable ?	Oui/Non
6.3- Les moyens en personnels demandés sont-ils raisonnables	Oui/Non
6.4- Le montant des investissements et achats d'équipements est-il raisonnable ?	Oui/Non
6.5- Les autres postes financiers (consommables, missions, sous-traitance, ...) sont-ils raisonnables ?	Oui/Non
6- Adéquation projet – moyens	X
<i>Commentaires justifiant l'évaluation (obligatoires). Expliquer en particulier les "Non"</i>	

	Note
7.1- Excellence de chaque partenaire dans le domaine proposé	X
7.2- Quotité de participation des chercheurs des équipes impliquées et notamment du coordinateur et en regard des objectifs du projet	X
7.3- Clarté de rédaction du projet, de sa justification, du programme de travail (définition des jalons, des résultats intermédiaires / finaux le cas échéant)	X
7- Critères spécifiques pour cet appel	X
<i>Commentaires justifiant l'évaluation (obligatoires).</i>	

Questions diverses	Note
8.1- 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
<i>Expliquer, le cas échéant, les "Non" (obligatoires)</i>	

Commentaire général et avis	Note
1- Pertinence de la proposition au regard des orientations de l'appel à projets.	X
2- Qualité scientifique et technique	X
3- Impact du projet	X
4- Méthodologie, qualité de la construction du projet et de la coordination	X
5- Qualité du consortium	X
6- Adéquation projet – moyens	X
7- Critères spécifiques pour cet appel	X
Avis général sur le projet	X
<p>Points forts du projet :</p> <p>Points faibles du projet :</p>	
Décision recommandée par l'expert concernant le projet	
A retenir en priorité / A retenir si possible / A ne pas retenir.	
<p>Motivations principales de cette décision :</p> <p>Le projet pourrait-il être amélioré en faisant l'objet de modifications ou d'adaptation ? Le cas échéant lesquelles ?</p>	

<p>Je déclare que, autant que je sache, je n'ai aucun conflit d'intérêt, dans l'évaluation de cette proposition</p> <p><i>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"</i></p>	<p>Nom :</p> <p>Date :</p> <p>Signature :</p>
---	---

8 Annexe 2 : Modèle à utiliser pour la description détaillée du projet

Texte libre à fournir au format PDF

A- Description courte du projet (maximum 2 pages)

Cette partie doit comprendre une version française et une version anglaise.

On précisera, en particulier, les motivations du projet, sa pertinence, les enjeux scientifiques et éventuellement techniques/économiques associés, les objectifs fixés, le caractère novateur du projet, les verrous scientifiques et/ou technologiques à lever, la méthodologie mise en œuvre, les résultats attendus et les perspectives ouvertes sur le plan scientifique et/ou en termes d'applications.

Identification du projet

Acronyme du projet :

Thème de l'appel à projets principal auquel le projet se rattache :

Thème(s) de l'appel à projets secondaire(s) auxquels le projet se rattache (le cas échéant) :

Type de projet :

A.1- Contexte et motivation du projet

A.2- Retombées scientifiques et techniques attendues

A.3- Retombées industrielles et économiques escomptées (le cas échéant)

B- Description scientifique et technique détaillée du projet

Cette partie peut être rédigée en langue française ou anglaise mais il est fortement recommandé d'utiliser la langue anglaise.

B.1- But du projet (2 pages maximum)

On décrira les objectifs du projet en montrant comment celui-ci contribue aux objectifs du programme. On décrira de manière succincte les principaux travaux qui vont être menés dans le cadre du projet.

B.2- Contexte et état de l'art (2 page maximum)

On précisera, en particulier, la position du projet par rapport à la concurrence nationale et internationale, en donnant les références nécessaires. On décrira aussi les compétences et savoir-faire des équipes impliquées vis-à-vis de l'état l'art au niveau national et international, capacités attestées par la qualité de leur production scientifique antérieure en termes de publications.

B.3- Organisation du projet - description des sous-projets (6 à 10 pages)

On décrira le programme de travail prévu en identifiant pour chaque étape, les objectifs poursuivis, les moyens scientifiques et techniques mis en œuvre, en explicitant le rôle de chaque partenaire. La valeur ajoutée des coopérations entre les différentes équipes sera argumentée. Le mode de pilotage du projet sera décrit en tenant compte des aléas susceptibles d'être rencontrés. Les moyens demandés dont la justification sera présentée au §3 devront être en adéquation avec les objectifs du projet et son déroulement prévu.

Si des doctorants sont présents dans le projet, on explicitera leur sujet de thèse et les conditions de leur encadrement

On listera les membres permanents des laboratoires impliqués dans le projet avec pour chacun d'eux la quotité de temps consacrée au projet en moyenne sur sa durée. On joindra en annexe un mini-CV de ceux-ci (1/2 page incluant une liste de 3 publications récentes en rapport avec le projet).

B.4- Principaux "délivrables"

Etant donné l'aspect recherche amont du présent appel à projet, les "délivrables" pourront être revus en fonction de l'avancement de la recherche sur une base annuelle. Le tableau mis à jour des "délivrables" établi d'un commun accord entre le coordonnateur du projet et la Délégation ANR Calcul Intensif au CEA.

	Libellé	Type ¹¹	Partenaire pilote	Partenaires participants	Date ¹²
1					
2					
3					
4					
5					
6					
...					

¹¹ Article écrit en vue de publication, film, logiciel ou maquette de logiciel, publication de logiciel ou de maquette de logiciel en open-source, proceedings, ...

¹² T0+x mois où T0 désigne la date de lancement du projet.

Il est souhaitable de rappeler dans ce tableau, les "délivrables" suivants :

1. *Comptes rendus intermédiaires semestriels (courts / longs) et compte rendu final.*
2. *Mise en place d'une page web propre au projet (rapidement après le démarrage du projet) et tenue à jour au minimum semestrielle de celle-ci.*

B.5- Résultats escomptés – perspectives (1 à 2 pages)

On résumera les objectifs du projet et les résultats escomptés, en proposant des critères de réussite et d'évaluation. On décrira également les perspectives scientifiques et éventuellement technologiques ouvertes au-delà de la durée du projet.

B.6- Propriété intellectuelle (le cas échéant)

On présentera une analyse des problèmes de propriété intellectuelle et industrielle identifiés ou susceptibles de se poser, en termes de brevets existants, de licences à obtenir, etc. Les principes de l'accord de propriété intellectuelle qui sera mis en œuvre entre les partenaires du consortium doivent être explicités, y compris pour les projets amont menés par des partenaires académiques. Les partenaires d'un consortium impliquant un industriel doivent s'engager à signer un accord dans les 6 mois qui suivent la notification de financement du projet.

Il est rappelé que le règlement relatif à l'attribution des aides de l'ANR prévoit que : "A la demande du chef de projet, la confidentialité des résultats est de droit. La propriété de ces résultats appartient aux bénéficiaires de l'aide, qui en disposent selon les modalités convenues à leur niveau et sous réserve des droits à intéressement des inventeurs. Sous réserve de la nécessité de prévoir une période de confidentialité, dans les cas où des résultats sont à protéger, le bénéficiaire doit s'assurer par toute mesure appropriée de la diffusion publique des comptes rendus scientifiques ou de leurs résumés."

C- Justification scientifique des moyens demandés

C.1- Moyens financiers demandés au GIP ANR dans le cadre du présent AAP

On présentera ici brièvement une justification scientifique des moyens demandés pour chacune des équipes impliquées dans le projet, en distinguant les demandes en équipement, fonctionnement, personnels (hors doctorant(e)s). Pour les demandes d'équipement, préciser si les achats envisagés doivent être complétés par d'autres sources de crédits, le montant et l'origine des crédits complémentaires qui seront utilisés. Les moyens demandés et l'évaluation du montant total du projet en coûts complets sont récapitulés pour chaque équipe partenaire dans le dossier saisi sur le serveur de soumission. **Note : sauf exception qui doit être clairement expliquée et motivée, l'AAP "Sécurité et Informatique" n'a pas pour objet de financer des équipements informatiques lourds.**

C.2- Autres demandes ou sources de financement de l'ANR concernant le projet

Une partie de ce projet a t-elle été soumise à un autre appel de l'agence ?	
Si oui :	
• Lequel ?	
• Explications sur la complémentarité des soumissions.	

C.3- Autres soutiens financiers apportés au projet (hors ANR)

Le GIP ANR a vocation à soutenir des projets de façon importante et décisive. Il est néanmoins demandé ici de présenter le budget global du projet hors financement des personnels titulaires et des coûts d'infrastructures en veillant à indiquer toutes les sources de financement du projet hors ANR (types de crédits et montants, nom et nature du programme,...), en précisant si le financement est obtenu ou s'il fait l'objet d'une demande en cours d'évaluation.

C.4- Autres actions contractuelles dans lesquelles les partenaires sont engagés

On mentionnera ici de façon exhaustive, pour chacune des équipes participant au projet présenté, son implication dans d'autres projets et leur degré d'avancement.
En particulier, on précisera pour chacune des équipes participantes si elle est impliquée dans des projets européens ou dans d'autres types de projets nationaux ou internationaux. Si tel est le cas, on veillera à préciser le positionnement relatif de chacun de ces projets.
Les indications fournies serviront notamment à apprécier le dynamisme des équipes impliquées dans le projet.

C.5- Relation avec les pôles de compétitivité

Ce projet fait-il partie d'un ou de projet(s) labellisé(s) (ou en cours de labellisation) par un (des) pôle(s) de compétitivité ? ¹³ Si oui :	
<ul style="list-style-type: none"> • Quel(s) pôle(s) ? 	
<ul style="list-style-type: none"> • Quel(s) projet(s) du(des) pôle(s) ? 	

¹³ Cette information n'est pas prise en compte par les experts et les comités d'évaluation. Pour les projets académiques elle n'intervient pas dans le processus d'évaluation.

8 Annexe 3 : Modèle 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. Etablir la fiche d'engagement sur papier à entête. Supprimer le modèle non utilisé.

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 du GIP 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 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)

Signature du chef de laboratoire :
(*Prénom et NOM* du responsable du laboratoire) atteste avoir pris connaissance de ce projet.

Date et 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 du GIP 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 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)