

Systèmes Embarqués et Grandes Infrastructures

Défi sécurité Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute

SEC&SI

Appel à Projets 2008

Date limite de dépôt des projets de recherche
03/04/2008 à 12h00

La mise en œuvre de l'appel à projets est réalisée par l'ANR pour assurer la conduite opérationnelle de l'évaluation et l'administration des dossiers d'aide.

MOTS CLES

Système d'exploitation sécurisé. Cryptographie. Modélisation des politiques de sécurité. Cloisonnement. Authentification distante. Preuve d'origine. Infrastructure de gestion de clés. Signature électronique. Mise à jour sécurisée. Sûreté de fonctionnement. Ergonomie de la sécurité.

CLOTURE DE L'APPEL A PROJETS

DATE LIMITE DE DEPOT DES PROJETS

SOUS FORME ELECTRONIQUE (DOCUMENTS DE SOUMISSION A ET B)

03/04/2008 impérativement avant 12h00 (heure de Paris)

sur le site de soumission électronique accessible au plus tard le 22 février 2008.

ET

DATE LIMITE D'ENVOI DU DOCUMENT DE SOUMISSION A

SOUS FORME PAPIER, SIGNE PAR TOUS LES PARTENAIRES

18/04/2008 cachet de la poste faisant foi, à l'adresse :

Programme Systèmes Embarqués et Grandes Infrastructures – Défi Sécurité
Agence Nationale de la Recherche
212 rue de Bercy
75012 Paris

CONTACTS

Chargé de Mission
Vincent BRUNIE
secsi@agencerecherche.fr
01 78 09 80 18
Assistante Emilie DELAET – 01 78 09 80 47

RESPONSABLE DE PROGRAMME ANR

Bertrand BRAUNSCHWEIG - 01 78 09 80 16

RECOMMANDATIONS

- Lire attentivement l'ensemble du présent document, **et en particulier le § 3.1 relatif aux critères d'éligibilité**, ainsi que le règlement relatif aux modalités d'attribution des aides de l'ANR, avant de déposer un projet de recherche ;
- Ne pas attendre la date limite d'envoi des projets pour la soumission de leur projet par voie électronique (attention : le respect de l'heure limite de soumission est impératif) ;
- Consulter régulièrement la rubrique consacrée à cet appel à projets sur le site internet de l'ANR <http://www.agence-nationale-recherche.fr> et le forum de discussion.
- Contacter, si besoin, l'ANR, par courrier électronique, à l'adresse mentionnée plus haut.

SOMMAIRE

1. CONTEXTE ET OBJECTIFS DE L'APPEL A PROJETS	4
2. CHAMP DE L'APPEL A PROJETS	4
2.1. AXE THEMATIQUE	4
2.2. CARACTERISTIQUES GENERALES DES PROJETS CARACTERISTIQUES NECESSAIRES	5
3. CRITERES D'ELIGIBILITE ET D'EVALUATION	7
3.1. CRITERES D'ELIGIBILITE	7
3.2. CRITERES D'EVALUATION	7
4. DISPOSITIONS RELATIVES AU FINANCEMENT	8
5. POLES DE COMPETITIVITE	9
6. MODALITES DE SOUMISSION	10
ANNEXE	
1. PROCEDURE DE SELECTION	11
2. DEFINITIONS	12
3. ACCORDS DE <i>CONSORTIUM</i> POUR LES PROJETS PARTENARIAUX ORGANISME DE RECHERCHE/ENTREPRISE	14
4. PRINCIPES DU DEFI	15
5. MODELE POUR LE DOCUMENT DE SOUMISSION B	18

1. CONTEXTE ET OBJECTIFS DE L'APPEL A PROJETS

CONTEXTE ET OBJECTIFS DU PROGRAMME

Le contexte et les objectifs du programme « Systèmes Embarqués et Grandes Infrastructures » sont décrits dans l'appel à projets général de l'édition 2008 de ce programme.

OBJECTIFS DE L'APPEL A PROJET

Dans le cadre de l'axe 5 du programme « Systèmes Embarqués et Grandes Infrastructures », le présent appel à projets « Défi sécurité Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute » a pour objectif l'intégration des résultats de recherche en matière de sécurité des systèmes d'information dans un cas concret permettant de favoriser l'utilisation par le grand public de moyens sécurisés.

Les « équipes » (voir définition ci-dessous) retenues dans le cadre du présent appel à projets, d'une part, proposeront chacune une solution et, d'autre part, chercheront à mettre en évidence les vulnérabilités des solutions proposées par les autres équipes.

Le défi se déroulera sur deux ans. Chaque équipe commencera par proposer une version de sa solution. La période qui suivra sera l'occasion, pour chaque équipe, d'évaluer les solutions concurrentes au plan des différents critères ci-dessous. La mise en évidence de vulnérabilités sur les solutions concurrentes pourra faire l'objet de publication (voir § 2.2). Les solutions seront comparées entre elles et feront l'objet d'un classement par un jury.

Le fonctionnement détaillé du suivi du défi est présenté en annexe § 4.

2. CHAMP DE L'APPEL A PROJETS

2.1. AXE THEMATIQUE

DEFI SYSTEME D'EXPLOITATION CLOISONNE ET SECURISE POUR L'INTERNAUTE

Il est proposé comme objectif de concevoir à destination du grand public un système d'exploitation sécurisé permettant d'accéder depuis un ordinateur aux services de banque en ligne, d'e-administration et à un service d'envoi de messages au minimum signés.

Le défi consistera à proposer une solution :

- ergonomique : l'utilisateur doit pouvoir continuer à utiliser son ordinateur sans changement, même si c'est cet ordinateur qui est utilisé pour l'usage des fonctions sécurisées ;
- fonctionnelle : la solution proposée devra être compatible avec des services en ligne couramment utilisés et l'utilisateur devra pouvoir stocker des éléments justificatifs

- éventuels ;
- tolérante aux agressions : les vulnérabilités sur l'ordinateur et sur les applications utilisés ne doivent pas avoir un impact immédiat sur l'ensemble des applications sécurisées ;
- adaptable : la prise en compte des évolutions fonctionnelles et de sécurité nécessitera de pouvoir mettre à jour la solution, et ce de façon sécurisée.

L'idée du défi est de s'adresser à la population des internautes qui est habituée à des fonctionnalités accessibles par des interfaces utilisateur intuitives. Les solutions proposées devront donc disposer d'une interface graphique.

Les fonctionnalités qui devront être disponibles sont au minimum les suivantes :

- .1 L'internaute dispose généralement d'un service de messagerie SMTP proposé par son fournisseur d'accès. La solution devra permettre d'utiliser ce service pour fournir un complément sécuritaire par la signature électronique des messages. Cette signature nécessitera de mettre en place dans la solution une ou plusieurs clés privées dont la sécurité devra bien entendu être assurée.
- .2 La télé-déclaration des impôts sur Internet est un processus désormais largement employé qui utilise une clé privée, des applications java et une possibilité d'accès sécurisé par https. La solution proposée devra permettre d'exploiter le service correspondant et de protéger les secrets nécessaires.
- .3 L'internaute est également de plus en plus enclin à accéder à des services en ligne sécurisés proposés par les banques, le commerce, les associations, les fournisseurs, les assurances, etc. Le standard de fait en matière de sécurité, observé pour ces services est l'usage de SSL ou TLS, couplé à des services d'information non sécurisés basés sur http. La solution devra permettre d'utiliser ces services.
- .4 L'utilisation de ces différents services nécessite le plus souvent de pouvoir conserver des informations (récépissé de paiement, de déclaration, messages envoyés et reçus, etc.). La solution devra permettre une telle conservation en assurant la sécurité des données.
- .5 Tout système d'information, spécialement lorsqu'il est sécurisé, doit être en mesure de s'adapter à des évolutions matérielles, fonctionnelles ou à l'émergence de nouvelles menaces ou vulnérabilités. Ces évolutions doivent elles-mêmes être sécurisées pour garantir l'intégrité du système. Les solutions proposées devront intégrer ce besoin.

L'enjeu du défi est de garantir la sécurité de l'ensemble de ces fonctionnalités dans une approche système, tout en simplifiant l'emploi de ces technologies pour les rendre accessibles à des utilisateurs non avertis.

Des détails supplémentaires sont présentés en annexe § 4.

2.2. CARACTERISTIQUES GENERALES DES PROJETS

2.2.1. CARACTERISTIQUES NECESSAIRES

Cet appel à projets est ouvert à des propositions d'équipes :

- non collaboratives, constituées d'un seul partenaire appartenant nécessairement à un organisme de recherche¹), ou

¹ Cf. définition en annexe § 2.

- collaboratives, constituées de plusieurs partenaires (organismes de recherche^{ou} entreprises) dont l'un, au moins, appartient à un organisme de recherche²).

La durée du projet sera de deux ans

Les recherches menées seront uniquement des travaux de recherche industrielle (voir définition en annexe §2)

Le projet aura deux lots :

- Développement d'une solution originale conformément à l'axe thématique 2.1
- Evaluation des solutions concurrentes au plan des différents critères ci-dessous. La mise en évidence de vulnérabilités sur les solutions concurrentes pourra faire l'objet de publication (voir ci-dessous)

Le déroulement du défi apparaît donc comme une compétition, chaque projet développant sa solution et étant attaqué par les autres projets. Cette compétition sera régie à travers un suivi spécifique détaillé en annexe 4.

Proposition de solution

La plate-forme matérielle visée ne doit pas être contrainte. Il s'agit donc d'une architecture matérielle de type PC i386 disposant d'une MMU sur laquelle on peut imaginer que l'internaute fait tourner de façon habituelle un système d'exploitation quelconque (Dos, Windows 95, XP, Vista, Linux, BSD, etc.). L'idée est que la majorité des internautes doivent pouvoir utiliser les solutions proposées, donc on ne devra pas faire d'hypothèse réductrice sur les fonctionnalités de sécurité matérielles disponibles (par exemple extensions matérielles pour la virtualisation, IOMMU, TPM, etc.). La présence de telles fonctions pourra par contre être utilisée pour renforcer la sécurité de la solution dans ce cas ; Les équipes qui s'inscriront devront proposer une solution basée sur un système d'exploitation Linux utilisant un noyau 2.6. Cette règle est destinée à faciliter la comparaison des solutions et à rendre plus facile l'évaluation croisée des solutions par les équipes. Elle vise aussi à pouvoir proposer des solutions s'adaptant à la diversité des plates-formes matérielles existantes.

Les équipes sont libres de modifier le noyau, d'appliquer des patches, de choisir leur distribution de base dans le respect des licences applicables.

La solution ne devra s'appuyer que sur du logiciel libre et, si nécessaire, sur des outils non libres mais utilisables et diffusables librement pour un usage non commercial à des fins de recherche dans le cadre du défi.

Règles de publication

Les équipes devront proposer leur solution et son code source pour que chacun puisse procéder à son analyse. La conception de la solution devra être documentée et présentée lors des séminaires organisés à cet effet.

Les publications d'attaque sur une solution seront possibles **sous réserve que** :

- l'équipe concurrente soit pré-alertée ;
- le ou les responsables des développements éventuellement impactés soient pré-alertés ;

² Cf. définitions en annexe § 2.

- le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques de la DCSSI (CERTA) soit informé en même temps de ces vulnérabilités, puis dans un second temps des résultats des procédures ci-dessus.

3. CRITERES D'ELIGIBILITE ET D'EVALUATION

Sont décrits ci-après les critères d'éligibilité et d'évaluation utilisés au cours de la procédure de sélection décrite en annexe §1.

3.1. CRITERES D'ELIGIBILITE

- Le coordinateur du projet ne doit pas être membre du comité d'évaluation du programme
- Les dossiers sous forme électronique (documents de soumission A et B) et sous forme papier (document de soumission A uniquement) doivent être soumis dans les délais, au format demandé et être complets ; les contenus des versions électronique et papier du document de soumission A doivent être identiques.
- Le projet doit entrer dans le champ de l'appel à projets.
- Le projet doit être un projet de recherche industrielle (cf. définition en annexe §2.1).
- La durée du projet doit être de 2 ans.
- Nature du partenariat (cf. § 2.2.1). Les partenaires doivent appartenir à l'une des catégories suivantes³ :
 - Organisme de recherche (université, EPST, EPIC,...).
 - Entreprise.

Le projet doit compter au moins un partenaire appartenant à la catégorie « organisme de recherche ».

IMPORTANT

- Les dossiers ne satisfaisant pas aux critères d'éligibilité ne seront pas soumis à avis d'experts extérieurs et ne pourront en aucun cas faire l'objet d'un financement de l'ANR.
- Les dossiers transmis après les échéances indiquées seront déclarés non recevables.

3.2. CRITERES D'EVALUATION

Le nombre maximal d'équipes sélectionnées sera de 15.

Les propositions seront examinées selon les critères suivants :

- Qualité scientifique et technique
- Méthodologie, qualité de la construction du projet et de la coordination
- Qualité du consortium⁴

³ Cf. définition des organismes de recherche et des entreprises en annexe § 2.3.

⁴ Pour un projet partenarial organisme de recherche/entreprise, la labellisation du projet par un pôle de compétitivité

- Adéquation projet – moyens / Faisabilité du projet

4. DISPOSITIONS RELATIVES AU FINANCEMENT

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 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 partenaires étrangers est néanmoins possible dans la mesure où chaque partenaire étranger assure son propre financement dans le projet.

IMPORTANT

L'ANR n'attribuera pas d'aide d'un montant inférieur à 15 000 € à un partenaire d'un projet.

Pour les entreprises⁵, le **taux maximum** d'aide de l'ANR est le suivant :

Dénomination	Taux maximum d'aide pour les PME ⁶	Taux maximum d'aide pour les entreprises autres que PME
Recherche industrielle ¹	75 *% des dépenses éligibles	40 % des dépenses éligibles

(*) Pour les projets ne faisant pas appel à une coopération effective entre une entreprise et un organisme de recherche, le taux maximum pour toutes les entreprises est de **40 %**.

Il y a collaboration effective entre une entreprise et un organisme de recherche lorsque l'organisme de recherche supporte au moins 10 % des coûts entrant dans l'assiette de l'aide et qu'il a le droit de publier les résultats des projets de recherche, dans la mesure où ces résultats sont issus de recherches qu'il a lui-même effectuées.

IMPORTANT

en application des nouvelles dispositions communautaires sur les aides d'État :

- L'effet d'incitation⁷ d'une aide de l'ANR à une entreprise autre que PME devra être établi. En conséquence, les entreprises autres que PME sélectionnées dans le cadre du présent appel à projets seront sollicitées, pendant la phase de finalisation des dossiers

(cf. § 5) 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".

⁵ On entend par « entreprise » toute entité exerçant une activité économique, indépendamment de sa forme juridique (cf. définition en annexe § 3.3).

⁶ En particulier, 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€ (cf. annexe § 3.3).

⁷ La définition de l'effet d'incitation figure en annexe § 1.

administratifs et financiers (cf. annexe § 1), pour fournir les éléments d'appréciation nécessaires.

- Les bénéficiaires de l'aide de l'ANR sur des projets partenariaux organisme de recherche/entreprise devront fournir, dans un délai maximum de douze mois après la date d'entrée en vigueur des actes attributifs d'aide les concernant, une copie de leur accord de *consortium* ainsi qu'une attestation signée par eux de sa compatibilité avec les dispositions de l'encadrement communautaire des aides à la recherche, au développement et à l'innovation (cf. annexe § 3).

Montant d'aide par équipe

Dans le cadre du présent appel à projets, chaque projet se verra attribuer un montant maximal d'aide de 120 k€.

5. POLES DE COMPETITIVITE

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.

La procédure à suivre est décrite ci-après.

Le formulaire d'attestation de labellisation d'un projet par un pôle de compétitivité téléchargeable au format Word (*.doc) est disponible avec les documents téléchargeables constituant le dossier de soumission sur le site internet de l'ANR.

Le partenaire coordinateur devra transmettre le formulaire d'attestation de labellisation, **avec le volet 1 dûment renseigné**, sous forme électronique à la structure de gouvernance de chaque pôle de compétitivité sollicité.

En cas de labellisation, la structure de gouvernance du pôle de compétitivité sollicité devra transmettre à l'ANR le formulaire d'attestation de labellisation **avec le volet 2 dûment renseigné, en deux versions** : une version sous forme papier **signée** envoyée par courrier et une version sous forme électronique au format Word (*.doc) (adresses postale et électronique figurant sur le formulaire).

Le formulaire d'attestation de labellisation sous forme papier **signé** devra être transmis à l'ANR dans un délai de **deux mois maximum** après la date limite de dépôt des projets sur le site de soumission.

6. MODALITES 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.

Les éléments du dossier de soumission seront mis en ligne sur le site internet de l'ANR, au plus tard le 22/02/2008. Le modèle de document B est donné à l'annexe § 5 de l'appel à projets.

Il est recommandé de produire une description scientifique et technique du projet en anglais, sauf pour les projets pour lesquels l'usage du français s'impose. Au cas où la description scientifique et technique serait rédigée en français, une traduction en anglais pourra être demandée dans un délai compatible avec les échéances du processus d'évaluation.

**LES DOCUMENTS DU DOSSIER DE SOUMISSION DEVRONT IMPERATIVEMENT ETRE TRANSMIS
PAR LE PARTENAIRE COORDINATEUR**

SOUS FORME ELECTRONIQUE

**(documents de soumission A et B) au plus tard le 03/04/2008
impérativement avant 12h (heure de Paris) sur le site de soumission.**

ET

SOUS FORME PAPIER

(uniquement document de soumission A, signé par tous les partenaires)
par voie postale au plus tard le **18/04/2008 à 24 h**, en un exemplaire,
le cachet de la poste faisant foi, à l'adresse suivante :

Programme Systèmes Embarqués et Grandes Infrastructures – Défi Sécurité
Agence Nationale de la Recherche
212 rue de Bercy
75012 Paris

**UN ACCUSE DE RECEPTION SOUS FORME ELECTRONIQUE
sera envoyé au coordinateur par l'ANR**

Les contenus des documents de soumission A sous forme électronique et sous forme papier devront être identiques.

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

Vincent BRUNIE
secsi@agencerecherche.fr
01 78 09 80 18

Bertrand BRAUNSCHWEIG
secsi@agencerecherche.fr
01 78 09 80 16

ANNEXE

1. PROCEDURE DE SELECTION

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 entreprises autres que PME sélectionnées seront sollicitées pour fournir les éléments d'appréciation nécessaires pour établir l'effet d'incitation⁸ de l'aide de l'ANR.

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** 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 de l'ANR 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 (<http://www.agence-nationale-recherche.fr/DocumentsAgence>).

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 (<http://www.agence-nationale-recherche.fr/DocumentsAgence>).

La composition des comités du programme est affichée sur le site internet de l'ANR (<http://www.agence-nationale-recherche.fr/Comites>).

⁸ *Avoir un effet d'incitation signifie, aux termes des dispositions communautaires, que l'aide doit déclencher, chez son bénéficiaire, un changement de comportement l'amenant à intensifier ses activités de R & D : elle doit avoir comme incidence d'accroître la taille, la portée, le budget ou le rythme des activités de R & D. L'analyse de l'effet d'incitation reposera sur une comparaison de la situation avec et sans octroi d'aide, à partir des réponses à un questionnaire qui sera transmis à l'entreprise. Divers indicateurs pourront, à cet égard, être utilisés : coût total du projet, effectifs de R & D affectés au projet, ampleur du projet, degré de risque, augmentation du risque des travaux, augmentation des dépenses de R & D dans l'entreprise, ...*

2. DEFINITIONS

2.1. DEFINITIONS RELATIVES AUX DIFFERENTES CATEGORIES DE RECHERCHE

Ces définitions figurent dans l'encadrement communautaire des aides d'État à la recherche, au développement et à l'innovation⁹. On entend par :

- **recherche fondamentale**, « des travaux expérimentaux ou théoriques entrepris essentiellement en vue d'acquérir de nouvelles connaissances sur les fondements de phénomènes ou de faits observables, sans qu'aucune application ou utilisation pratiques ne soient directement prévues ».
- **recherche industrielle**, « la recherche planifiée ou des enquêtes critiques visant à acquérir de nouvelles connaissances et aptitudes en vue de mettre au point de nouveaux produits, procédés ou services, ou d'entraîner une amélioration notable des produits, procédés ou services existants. Elle comprend la création de composants de systèmes complexes, nécessaire à la recherche industrielle, notamment pour la validation de technologies génériques, à l'exclusion des prototypes visés [dans la définition du développement expérimental] [...] ci-après ».
- **développement expérimental**, « l'acquisition, l'association, la mise en forme et l'utilisation de connaissances et de techniques scientifiques, technologiques, commerciales et autres existantes en vue de produire des projets, des dispositifs ou des dessins pour la conception de produits, de procédés ou de services nouveaux, modifiés ou améliorés. Il peut s'agir notamment d'autres activités visant la définition théorique et la planification de produits, de procédés et de services nouveaux, ainsi que la consignation des informations qui s'y rapportent. Ces activités peuvent porter sur la production d'ébauches, de dessins, de plans et d'autres documents, à condition qu'ils ne soient pas destinés à un usage commercial.

La création de prototypes et de projets pilotes commercialement exploitables relève du développement expérimental lorsque le prototype est nécessairement le produit fini commercial et lorsqu'il est trop onéreux à produire pour être utilisé uniquement à des fins de démonstration et de validation. En cas d'usage commercial ultérieur de projets de démonstration ou de projets pilotes, toute recette provenant d'un tel usage doit être déduite des coûts admissibles.

La production expérimentale et les essais de produits, de procédés et de services peuvent également bénéficier d'une aide, à condition qu'ils ne puissent être utilisés ou transformés en vue d'une utilisation dans des applications industrielles ou commerciales.

Le développement expérimental ne comprend pas les modifications de routine ou périodiques apportés à des produits, lignes de production, procédés de fabrication, services existants et autres opérations en cours, même si ces modifications peuvent représenter des améliorations ».

2.2. DEFINITIONS RELATIVES A 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.

⁹ Cf. JOUE 30/12/2006 C323/9-10 (<http://www.agence-nationale-recherche.fr/documents/uploaded/2007/encadrement.pdf>)

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).

2.3. DEFINITIONS RELATIVES AUX STRUCTURES

On entend par :

- **organisme de recherche**, « une entité, telle qu'une **université** ou un **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 leurs 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 »⁹.

Les centres techniques, sauf exception dûment motivée, sont considérés comme des organismes de recherche.

- **entreprise**, toute entité, indépendamment de sa forme juridique, exerçant une activité économique. On entend par activité économique toute activité consistant à **offrir des biens et/ou des services sur un marché donné**¹⁰. 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 économique¹¹.

- **micro, petite et moyenne entreprise (PME)**, une entreprise répondant à la définition d'une PME de la Commission Européenne¹². 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€.

- **microentreprise**, une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros¹¹.

¹⁰ Cf. Encadrement communautaire des aides d'État à la recherche, au développement et à l'innovation, JOUE 30/12/2006 C323/11 (<http://www.agence-nationale-recherche.fr/documents/uploaded/2007/encadrement.pdf>).

¹¹ Cf. Recommandation de la Commission Européenne du 6 mai 2003 concernant la définition des petites et moyennes entreprises, JOUE 20/5/2003 L 124/39.

¹² Ibid.

3. ACCORDS DE CONSORTIUM POUR LES PROJETS PARTENARIAUX ORGANISME DE RECHERCHE/ENTREPRISE

Pour les projets partenariaux organisme de recherche/entreprise, les partenaires devront conclure, sous l'égide du coordinateur du projet, un accord précisant :

- la répartition des tâches, des moyens humains et financiers et des livrables ;
- le partage des droits de propriété intellectuelle des résultats obtenus dans le cadre du projet ;
- le régime de publication / diffusion des résultats ;
- la valorisation des résultats du projet.

Ces accords permettront également de déterminer l'existence éventuelle d'une aide indirecte entrant dans le calcul du taux d'aide maximum autorisé par l'encadrement communautaire des aides à la recherche, au développement et à l'innovation (ci après appelé « l'encadrement »).

L'absence d'aide indirecte est présumée si l'une au moins des conditions suivantes est remplie :

- le bénéficiaire soumis à l'encadrement supporte l'intégralité des coûts du projet ;
- dans le cas de résultats non protégeables par un titre de propriété intellectuelle, l'organisme de recherche bénéficiaire peut diffuser largement ses résultats ;
- dans le cas d'un résultat protégeable par un titre de propriété intellectuelle, l'organisme de recherche bénéficiaire en conserve la propriété ;
- le bénéficiaire soumis à l'encadrement qui exploite un résultat développé par un organisme de recherche bénéficiaire verse à cet organisme une rémunération équivalente aux conditions du marché.

Le coordinateur du projet transmettra une copie de cet accord ainsi qu'une attestation signée des partenaires attestant de sa compatibilité avec les dispositions de l'encadrement ainsi qu'avec la(les) convention(s) définissant les modalités d'exécution et de financement du projet. Cette transmission interviendra dans le délai de douze mois à compter de la date d'entrée en vigueur des actes attributifs d'aide.

L'attestation devra donc certifier soit que l'accord remplit l'une des conditions énumérées ci-dessus, soit que tous les droits de propriété intellectuelle sur les résultats, ainsi que les droits d'accès à ces résultats sont attribués aux différents partenaires et reflètent adéquatement leurs intérêts respectifs, l'importance de la participation aux travaux et leurs contributions financières et autres au projet. A défaut, l'accord pourra être considéré comme constituant une forme d'aide indirecte, conduisant à minorer le taux d'aide directe attribuée par l'ANR.

4. PRINCIPES DU DEFI

Planning

Les travaux des deux lots seront séquencés en six phases suivant le planning suivant :

- les six premiers mois seront alloués aux équipes pour développer leur solution. Un séminaire sera dédié, à l'issue de cette période, à la présentation de la solution et des choix de conception effectués.
- À l'issue de ce séminaire s'ouvrira une nouvelle période de six mois pendant laquelle les équipes seront libres d'attaquer les autres propositions. Les équipes pourront également continuer d'améliorer leur solution pour prendre en compte les attaques théoriques ou pratiques mises en évidence pendant cette phase. Pendant cette période, un classement mensuel des solutions sera maintenu. Un premier classement sera établi à la fin de cette période. Suivra une nouvelle période de trois mois de conception d'une deuxième version de la solution pour chaque équipe. Un nouveau séminaire permettra à la fin de cette période de présenter les évolutions réalisées.
- Les trois derniers mois, feront l'objet d'un dernier challenge offensif, à la suite desquels un nouveau classement sera établi.

Une dernière période de trois mois de conception suivie de trois mois d'attaque résultera en un dernier classement qui permettra de désigner le vainqueur.

	Semestre 1	Semestre 2	Semestre 3		Semestre 4	
Lot 1	Développement	Améliorations	Dév.	Amél.	Dév.	Amél.
Lot 2		Attaques		Att.		Att.

Règles de comparaison des solutions

Règles sur les attaques

Seront seules prises en compte pour le classement les attaques logiques sur les solutions proposées. Les attaques physiques sur le PC de l'utilisateur, de même que l'espionnage de ses actions par un dispositif extérieur ne seront pas prises en compte. Sont **interdites** les attaques sur les services qui ne sont pas élaborés au titre de l'appel à projet mais qui font partie du périmètre utilisé par l'internaute (banque en ligne, commerce en ligne, télé-déclaration des impôts, etc.). Par contre, une proposition qui utiliserait un service en ligne particulier pour assurer des fonctions de sécurité (par exemple un serveur de mise à jour), pourra être attaquée au niveau de ce service.

Il ne sera fait aucune hypothèse restrictive sur les capacités d'un attaquant réel. Celui-ci peut disposer d'un serveur malveillant sur l'internet, de capacités d'usurpation d'adresse IP, d'un réseau botnet, etc.

Principes du classement

Un jury établira le classement des équipes pendant les phases d'attaque. Ce jury jugera souverainement et sans recours des litiges éventuels dans la constatation de la réalité d'une attaque ou de la vraisemblance de ses hypothèses. Il prendra également en compte l'ergonomie de la solution. Le règlement détaillé pour l'établissement du classement sera transmis aux équipes avant le démarrage effectif des projets.

Biens à protéger

Pour permettre une comparaison la plus objective possible des solutions, seules les attaques sur les biens listés dans le tableau ci-dessous seront comptabilisées. En d'autres termes, une attaque sera considérée comme réussie si une atteinte à la confidentialité (C), à l'intégrité (I) ou à la disponibilité (D) de l'un de ces biens est observée ou déduite des hypothèses réalistes annoncées de l'attaque.

Le tableau ci-dessous précise également un coefficient d'importance de l'attaque, c'est-à-dire une estimation de l'impact de celle-ci. Si une attaque concerne plusieurs biens, les mesures d'impact s'additionnent. Ces coefficients correspondent au pourcentage mis en jeu du score de la solution attaquée.

Bien concerné	Exemple de scénario possible	Mesure de l'impact			Commentaire
		I	C	D	
PC utilisateur	Utiliser une vulnérabilité de la solution proposée pour accéder à des données de l'utilisateur ou altérer son système natif ou l'empêcher d'utiliser la solution proposée.	4	2	1	La solution doit évidemment être fonctionnelle (D), mais elle doit de façon encore plus importante ne pas induire de vulnérabilité sur la configuration de l'utilisateur. La lecture d'informations pourrait ainsi compromettre des données personnelles de l'utilisateur et une atteinte à l'intégrité du système natif serait encore davantage dommageable.
Biens utilisateur sur PC	Récupérer ou altérer des données sensibles que l'utilisateur a obtenues ou élaborées lors de l'usage de ses services en ligne (récépissé de télé-déclaration, message envoyé, etc.)	4	2	1	Ceci vise la fonctionnalité demandée de conservation sécurisée des données. Là encore, l'altération des données à l'insu de l'utilisateur est la menace ayant le plus d'impact.
Clés utilisateur sur PC	Récupérer ou altérer les éléments secrets cryptographiques dont l'utilisateur dispose pour accéder à ses services ou signer ses messages.	1	4	1	Ici l'altération de l'intégrité de la clé revient à la rendre indisponible puisqu'elle n'est plus utilisable pour l'accès au service. Par contre, si une clé privée est compromise, l'attaquant va pouvoir usurper l'identité de l'utilisateur et accéder en ligne et en différé à l'intégralité des données protégées par cette clé.

Biens utilisateur sur service	Profiter de la connexion de l'utilisateur pour accéder aux données qu'il manipule ou modifier le logiciel pour qu'il mémorise ces données ou profiter d'erreurs d'effacement pour retrouver des informations de sessions antérieures, etc.	4	2	1	L'intégrité des données présentes sur le site est évidemment la propriété la plus recherchée. Une destruction sur le site de données préalablement enregistrées par l'utilisateur serait d'ailleurs également considérée comme une atteinte en intégrité. Une attaque empêchant l'utilisateur d'accéder à ces informations mais sans que ces dernières soient altérées sur le site serait considérée comme une atteinte en disponibilité.
Mises à jour sécurisées	Introduire des mises à jour erronées dans le système.	2	0	1	La disponibilité des mises à jour est importante mais peut être empêchée au niveau réseau. L'introduction de mises à jour erronées n'a un impact important que si cela permet de monter une attaque sur les autres biens qui sera alors comptabilisée, d'où un coefficient d'impact relativement faible.

Gravité de l'attaque

L'impact d'une attaque sera en outre multiplié par un coefficient d'aggravation :

Type d'attaque	Coeff .	Commentaire
ciblée	1	L'attaque doit viser un internaute particulier. Elle nécessite, par exemple, que son matériel soit vulnérable à une attaque particulière. Dans ce cas il n'y a pas d'aggravation.
générique	2	L'attaque peut être appliquée à tout internaute qui utiliserait cette solution. Par exemple, une vulnérabilité logicielle de la solution est exploitable par un virus. Dans ce cas l'impact est doublé.
systématique	4	L'attaque a un impact immédiat sur tous les internautes utilisant la solution. Par exemple, le système de mise à jour est percé ou une clé de sécurisation du système est compromise.
théorique	¼	Une attaque peut être démontrée moyennant des hypothèses de capacités d'attaque réalistes mais difficiles à mettre en œuvre (disponibilité d'un botnet, de capacité mémoire importante, etc.) ou de vulnérabilité réalistes sur certains composants du système : <ul style="list-style-type: none"> - le navigateur web ; - le client de messagerie ; - une librairie partagée ; - etc. Dans ce cas, un coefficient réducteur est appliqué. Le fait que ce coefficient ne soit pas nul encourage à publier toute vulnérabilité structurelle et à corriger ces faiblesses avant qu'elles ne deviennent exploitables.

Si une solution propose une version destinée aux architectures 64 bits, toute attaque sur cette version sera considérée comme ciblée. Inversement, une attaque générique sur la

version i386 se verra attribuée le coefficient d'aggravation 2, même si elle n'est pas applicable aux architectures 64 bits. Ceci vise à ne pas trop pénaliser une proposition qui chercherait à étendre le spectre des configurations matérielles utilisables, tout en privilégiant la sécurité de la configuration majoritairement rencontrée.

5. MODELE POUR LE DOCUMENT DE SOUMISSION B

Acronyme	
Titre du projet (en français)	
Titre du projet (en anglais)	

Les pages seront numérotées et le nom de l'équipe devra figurer sur toutes les pages du document en pied de page.
Un sommaire du document est bienvenu

1. QUALIFICATION DE L'EQUIPE (1/2 A 1 PAGE MAXIMUM)

- 1) Fournir ici les éléments permettant d'apprécier la **qualification de l'équipe** pour sa participation au défi : biographie des principaux intervenants, bibliographie, acquis et savoir-faire de l'équipe, ...
- 2) Pour les équipes collaboratives, montrer la **complémentarité et la valeur ajoutée des coopérations entre les partenaires**.

2. PROGRAMME SCIENTIFIQUE ET TECHNIQUE (1/2 PAGE MAXIMUM)

Décrire brièvement le **programme de travail** : approches retenues, acquis, nouveaux développements envisagés,...

3. RETOMBÉES ATTENDUES (1/2 PAGE MAXIMUM)

Présenter les **retombées attendues** de la participation de l'équipe au défi en précisant selon les cas :

- les retombées scientifiques, techniques, industrielles, économiques...
- la valorisation des résultats attendus, connaissances à protéger ou à diffuser, ...
- la place du projet dans la stratégie industrielle de l'entreprise (ou du groupe)
- les échéances et la nature des retombées technico-économiques attendues
- l'incidence éventuelle sur l'emploi, la création d'activités nouvelles, ...

4. MOYENS MIS EN ŒUVRE (1/2 PAGE MAXIMUM)

On présentera ici la **description des moyens mis en œuvre** par l'équipe pour sa participation au défi.