



GOVERNEMENT

Liberté  
Égalité  
Fraternité



**bpi**france



Financé par  
l'Union européenne  
NextGenerationEU

**Stratégie Nationale Quantique**  
« Développer l'offre de  
cryptographie post-quantique »

**Stratégie Nationale Cyber**  
« Développement de technologies  
cyber innovantes critiques »

## Cryptographie post-quantique

### Cahier des charges de l'appel à projets

<https://www.bpifrance.fr/nos-appels-a-projets-concours/appel-a-projets-cryptographie-post-quantique>

Le numérique est aujourd'hui présent dans tous les pans de la vie des Français. Support de nombreuses innovations qui bénéficient à chacun, il induit aussi des risques en matière de sécurité et de souveraineté. En outre, le développement du télétravail durant la crise sanitaire a contribué à rendre plus ténue la frontière entre les outils informatiques professionnels et personnels, augmentant d'autant la vulnérabilité des systèmes. Dans ce cadre, le Gouvernement a souhaité, *via* la Stratégie Nationale Cyber, accompagner le développement de la filière française de la cybersécurité. À ce titre, cette stratégie visera à faire émerger des champions français de la cybersécurité, tant pour accompagner le développement d'une filière au potentiel économique important, que pour garantir à notre pays la maîtrise des technologies essentielles à la garantie de sa souveraineté.

S'il est peu probable à court terme, le risque de voir, post 2030, un ordinateur quantique capable de déchiffrer, éventuellement rétroactivement, des données protégées par des algorithmes à clé publique actuels, est pris très au sérieux par les autorités de sécurité de plusieurs pays. Pour faire face à ce risque et garder l'avance de l'industrie de sécurité française, le Gouvernement a souhaité, *via* la Stratégie Nationale Quantique, accompagner le développement de l'offre de cryptographie post-quantique. Cette stratégie vise à enrichir et affirmer la capacité de la France sur le plan scientifique et technologique et placer le pays dans le premier cercle des pays maîtrisant les chaînes de valeur industrielles permettant de garantir et pérenniser notre indépendance dans ce domaine technologique qui façonnera le futur.

À l'horizon 2025, l'objectif assigné à la stratégie cyber est l'atteinte d'un chiffre d'affaires de 25 Md€ pour la filière (soit un triplement du chiffre d'affaires actuel), le doublement des emplois dans le secteur en passant de 37 000 à 75 000 emplois et l'émergence de trois licornes françaises en cybersécurité. Pour cela, elle s'articule autour de 5 axes :

1. Développer des solutions souveraines et innovantes de cybersécurité ;
2. Renforcer les liens et synergies entre les acteurs de la filière ;
3. Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales ;
4. Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
5. Soutenir le développement des entreprises via des investissements en fonds propres.

A l'horizon 2030, l'objectif de la stratégie quantique est de faire contribuer la filière quantique à 2% des exportations françaises, créer 16 000 emplois directs et indirects, et faire émerger 3 licornes françaises. Pour cela elle s'articule autour de 6 axes :

1. Développer et diffuser l'usage des simulateurs et accélérateurs NISQ ;
2. Développer l'Ordinateur Quantique universel Passant à l'Echelle ;
3. Développer les technologies et applications des Capteurs Quantiques ;
4. Développer l'offre de Cryptographie Post-Quantique ;
5. Développer les systèmes de communication quantique ;
6. Développer une offre de technologies habilitantes compétitive.

Cet appel à projets s'inscrit dans l'axe 5 de la stratégie quantique et les axe 1 et 2 de la stratégie cyber. Il vise à soutenir le développement de briques technologiques innovantes et critiques en cybersécurité, capables de résister aux attaques des ordinateurs quantiques. Il participe également à renforcer les liens et synergies entre les acteurs des filières cyber et quantique en interne et entre eux.

## Calendrier

- **Une première relève des dossiers complets sera effectuée le 4 mars 2022 à 12h00 (midi heure de Paris) ;**
- Pour cette première relève, les auditions se tiendront la semaine du 25 avril 2022 (dates indicatives) ;
- Pour les projets aux enveloppes totales supérieures à 6M€, des compléments de dossiers pourront être demandés suite aux retours éventuels reçus lors des auditions et seront à fournir avant le 30 mai 2022 à 12h00 (midi heure de Paris).
  
- **Une seconde et dernière relève des dossiers complets sera effectuée le 4 mai à 12h00 (midi heure de Paris).**
- Pour cette relève finale, les auditions se tiendront la semaine du 6 juin 2022 (dates indicatives).
- Pour les projets aux enveloppes totales supérieures à 6M€, des compléments de dossiers pourront être demandés suite aux retours éventuels reçus lors des auditions et seront à fournir avant le 8 juillet 2022 à 12h00 (midi heure de Paris).

## 1. Contexte et objectifs de l'appel à projets

### 1.1. Axe « Développement de l'offre de Cryptographie Post-Quantique » de la Stratégie Nationale quantique

Le **chiffrement asymétrique** et l'échange de clé permettent **une gestion décentralisée des identités adaptée au contexte d'internet**. Les mécanismes asymétriques employés aujourd'hui, seront, en cohérence avec l'avancée des processeurs quantiques par ailleurs promue dans la stratégie nationale, menacés par un algorithme qui peut être mis en œuvre sur un éventuel ordinateur quantique universel suffisamment puissant, l'algorithme de Shor.

Face à cette menace, il est nécessaire de mettre en œuvre de nouvelles modalités de sécurisation des communications. Ces modalités devront satisfaire des exigences de robustesse de plusieurs niveaux comme :

- La résistance aux attaques par ordinateurs quantiques, de sorte à ce qu'un futur ordinateur quantique suffisamment puissant ne puisse pas remonter en temps utile à une clé de chiffrement ;
- La protection des communications passées ou « *perfect forward secrecy* », de façon à ce que la compromission d'un moyen de chiffrement, si elle menace les communications futures, n'ouvre pas en outre les portes des communications passées.

C'est le domaine de recherche de la cryptographie post-quantique. Une compétition internationale organisée sous l'égide du NIST américain vise à sélectionner les meilleurs candidats pour de tels mécanismes en 2022. Remplacer les mécanismes actuels par de nouveaux mécanismes résistants à l'ordinateur quantique permet de **conserver inchangée l'infrastructure actuelle de communications**.

S'agissant des mécanismes de **chiffrement symétriques**, utilisés pour sécuriser les informations très sensibles, **rien ne permet d'affirmer, à l'heure actuelle, qu'ils seraient sérieusement menacés par les ordinateurs quantiques**. Si nous disposions d'un ordinateur quantique suffisamment puissant pour attaquer par force brute sur le mécanisme de chiffrement symétrique de 128 bits, en exploitant l'algorithme de Grover, 30 ans environ seraient nécessaires pour trouver la clé de chiffrement. Ainsi, dans un avenir prévisible, les attaques par Grover ne semblent pas représenter une menace tangible. Elles peuvent, en tout cas, être déjouées à très faible coût en passant à un niveau de sécurité plus élevé, en multipliant par deux la taille de la clé de chiffrement (256).

Il sera important en revanche d'**ajuster à la hausse les exigences relatives aux sources de nombres aléatoires**. Les **générateurs quantiques de nombres aléatoires** pourront, ainsi, jouer un rôle important dans le renforcement du chiffrement symétrique.

## 1.2. Action globale « Développement de technologies innovantes critiques » de la Stratégie Nationale Cyber

L'offre française en cybersécurité comporte des lacunes en ce qui concerne la maîtrise de certaines technologies clés, comme en font état plusieurs initiatives (action « technologies clés » de la revue stratégique de cyberdéfense, feuille de route de l'ANSSI<sup>1</sup>, feuille de route du projet « cybersécurité et sécurité de l'IoT » du Comité Stratégique de Filière « Industries de sécurité » par exemple).

Les technologies ainsi identifiées sont critiques du fait de leur sensibilité en termes de sécurité et appellent autant que possible des solutions souveraines. En outre, elles représentent un marché potentiel de taille pour les acteurs français.

Le développement de solutions innovantes de confiance et souveraines sur ces briques doit donc être une priorité de la stratégie d'accélération. C'est ce que vise à permettre cet appel à projets (AAP) en cofinçant des projets de recherche et développement portant sur des briques technologiques innovantes et critiques en cybersécurité. Pour ce faire, une liste de thématiques de travail a été constituée (voir annexe 1). Au terme du présent AAP, la liste des thématiques sera amendée et une nouvelle phase de soumission de projets sera lancée.

Les thématiques proposées s'articuleront autour de 4 axes :

1. la protection des infrastructures critiques à l'heure des nouveaux usages (OIV/OSE notamment) ;
2. la protection des collectivités locales, startups/PME et télétravailleurs ;
3. la sécurité de l'IoT ;
4. les briques technologiques critiques spécifiques à certains secteurs clés.

## 1.3. Nature des projets attendus

Les projets visant au développement de technologies innovantes critiques sont des projets de R&D en cybersécurité adressant les thématiques détaillées dans l'annexe 1 du présent cahier des charges.

Les projets peuvent être conduits par (au choix) :

- Une entreprise, porteur unique ;
- un consortium qui rassemble des partenaires industriels dont des PME / ETI ;
- un consortium qui rassemble des partenaires industriels dont des PME / ETI et des partenaires de recherche<sup>2</sup>.

Ils correspondent à des assiettes de travaux d'un montant supérieur à **1 million d'euros**. Cette limite inférieure **pourra être abaissée à 500 000 € dans le cas d'un projet porté par une jeune pousse** au sens de la définition adoptée pour le régime exempté relatif aux aides en faveur des PME (SA.100189).

<sup>1</sup> liée notamment à la qualification de produits et services.

<sup>2</sup>Dont les IRT (Instituts de recherche technologiques), ITE (Instituts de pour la transition énergétique). Des projets financés dans le cadre de ces structures pourront ainsi être cofinancés.

Sont notamment éligibles les dépenses de personnels affectés au projet, identifiés et appartenant aux catégories suivantes : chercheurs, ingénieurs et techniciens, les amortissements d'équipements et de matériels de recherche et les travaux sous-traités à des laboratoires publics ou privés<sup>3</sup>.

Les travaux de R&D représentant moins de 10 % de l'assiette de dépenses du projet ou, dans le cas d'un consortium, ayant une contribution faible à son caractère collaboratif ont vocation à être pris en charge soit directement par les entreprises, soit en sous-traitance.

Les établissements de recherche ne peuvent être chefs de file des projets.

## **2. Critères d'éligibilité**

Pour être éligible, le projet déposé à cet AAP doit satisfaire simultanément aux critères suivants :

### **Dossier**

1. être soumis, dans les délais, sur [l'extranet des Projets Innovants Collaboratifs](#) de Bpifrance ;
2. compléter un dossier de candidature complet, au format imposé ;

### **Projet**

3. respecter l'objet de l'AAP et s'inscrire dans l'un des domaines d'application identifiés dans l'annexe 1 ;
4. présenter un total de dépenses éligibles supérieur à 1M€ (500K€ pour les jeunes pousses);
5. présenter une durée minimale de 12 mois et maximale de 36 mois ;
6. porter sur des travaux fortement innovants de recherche et développement en cybersécurité réalisés en France et non commencés (*i.e.* seul les coûts postérieurs à la demande seront éligibles à une aide) avant le dépôt de la demande d'aide ;

### **Porteur**

7. être déposé par (au choix) :
  - a. une entreprise, porteuse unique ;
  - b. un consortium, dont le chef de file est un industriel, pouvant impliquer d'autres industriels et/ou des acteurs de la recherche (dans le respect d'au moins 20% des travaux réalisés par des PME ou ETI et qu'aucun membre du consortium ne soit destinataire de moins de 10% du coût total du projet) ;
8. être porté par une société immatriculée en France au registre du commerce et des sociétés (RCS) à la date de dépôt du dossier ;
9. être porté par une entreprise à jour de ses obligations fiscales et sociales. Si l'entreprise est « entreprise en difficulté » selon le droit européen, son projet ne sera considéré comme éligible et donc instruit que si elle présente lors du dépôt de son dossier des éléments probants et jugés satisfaisants par Bpifrance justifiant sa sortie du statut d'« entreprise en difficulté » avant la décision sur le financement potentiel.

<sup>3</sup> Liste non exhaustive.

Sont exclus les projets qui causeraient un préjudice important du point de vue de l'environnement (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie.

Les projets ne respectant pas l'un des critères d'éligibilité sont écartés du processus de sélection, sans recours possible.

### **3. Organisation et financement des projets**

#### **3.1. Organisation du consortium (le cas échéant)**

Un accord de consortium portant sur tous les aspects liés à la réalisation du projet et notamment les règles applicables en matière de propriété intellectuelle, devra être préparé le plus tôt possible. La présentation d'un accord de consortium signé est indispensable au premier versement de l'aide.

Est appelé « partenaire du projet » toute entité signataire de l'accord de consortium. Il est rappelé qu'un partenaire du projet n'est pas forcément bénéficiaire direct d'aide : soit parce qu'il est financé en tant que sous-traitant, soit parce que ses dépenses ne sont pas éligibles ou retenues, soit parce qu'il n'a pas demandé de financement. Dans ces cas, il s'agit d'un partenaire non-bénéficiaire.

Chaque bénéficiaire d'une aide sera signataire d'une convention bilatérale avec Bpifrance. Les partenaires non-bénéficiaires n'auront pas de convention, mais en tant que membres du consortium, ils pourront être associés aux actions de communication du projet.

Le consortium doit être constitué de manière à ce que les conditions suivantes soient respectées (toute demande de dérogation devra être dûment justifiée) :

- Au moins 20% des coûts éligibles correspondent à des travaux réalisés par des PME ou des ETI ;
- Aucun bénéficiaire ne doit être concerné par moins de 10% du coût total du projet.

#### **3.2. Financement octroyé**

##### **3.2.1. Coûts éligibles à cet AAP**

Les dépenses liées au projet sont à présenter hors taxe et selon la ventilation requise dans l'annexe financière du projet en annexe 2 du dossier de candidature

Les coûts éligibles correspondent entre autres aux :

- **Salaires de personnel interne ;**
- **Frais connexes forfaitaires<sup>4</sup> ;**

<sup>4</sup> Les frais connexes sont les dépenses qui concourent à la réalisation du projet sans toutefois pouvoir être directement attribués à celui-ci et s'appliquent uniquement sur les dépenses de RDI. Le montant forfaitaire de ces dépenses est égal à 20 % des salaires de personnel internes.

- **Coûts communs :**
  - Études de faisabilité ou d'intégration des traitements sur les données hétérogènes,
  - Études permettant d'élaborer les méthodes d'évaluation et de recueil des données et sur les enjeux de sécurité,
  - Études permettant d'élaborer un modèle économique sur les données,
  - Collecte, validation, stockage, partage, exploitation des données recueillies,
  - Synthèse des résultats et leur communication,
  - Animation et coordination du projet,
  - Transfert des résultats aux autorités publiques.
- **Infrastructures :**
  - Équipements rendus nécessaires sur l'infrastructure,
  - Surcoûts d'exploitation rendus nécessaires par l'intégration du service ou de la captation des données.
- **Coûts de sous-traitance (maximum 30% des dépenses présentées)**
- **Contribution aux amortissements, frais de mission directement liés au projet, autres coûts (achats, consommables, etc.)**

Les dépenses seront éligibles à l'AAP uniquement si elles ne sont pas déjà financées par un ou des acteurs publics (Métropoles, Régions, EPCI, Europe notamment).

Les dépenses ne peuvent être prises en compte qu'à compter de la date de relève du dossier (cf. processus de sélection), étant entendu que les dépenses engagées avant la notification des conventions d'aide par Bpifrance le sont au risque des bénéficiaires.

L'ensemble des coûts relatifs au projet doit être détaillé dans le dossier de demande d'aide. L'instruction permet notamment de déterminer les coûts éligibles et retenus pour le financement par le Programme d'Investissements d'Avenir (PIA).

Par ailleurs, le quatrième programme d'investissements d'avenir participe au plan « France relance » de 100 Md€ pour la période 2021-2022, ayant vocation à être financé à hauteur de 40 % par l'Union européenne. Le présent AAP s'inscrit pleinement dans le cadre des mesures éligibles à cette part européenne, qui sont présentées dans le plan national de relance et de résilience (PNRR) de la France<sup>5</sup> et qui seront financées in fine via son outil, la « Facilité pour la reprise et la résilience » (FRR)<sup>6</sup>. Le soutien apporté au titre de cette facilité interviendra sous forme de remboursement à l'Etat des financements octroyés et non d'un financement direct auprès des bénéficiaires. En vertu de l'article 9 du règlement précité, **ce soutien est toutefois conditionné par l'interdiction de bénéficier d'un autre soutien au titre d'autres programmes et instruments de l'Union couvrant les mêmes coûts**. Dans ce contexte, le candidat pourra être amené à fournir des informations sur les autres sources de financement d'origine européenne mobilisées ou demandées pour son projet dans son dossier de candidature.

<sup>5</sup> Plus d'informations sur : <https://www.economie.gouv.fr/plan-national-de-relance-et-de-resilience-pnrr#>.

<sup>6</sup> Règlement (UE) 2021/241 du Parlement européen et du Conseil du 12 février 2021 établissant la facilité pour la reprise et la résilience.

### 3.2.2. Taux d'aide pour les bénéficiaires soumis au secteur concurrentiel

Dans le cas général, le régime d'aide retenu dans le cadre du PIA est le régime cadre exempté d'aides à la recherche, au développement et à l'innovation N° SA.58995<sup>7</sup>, pris sur la base du règlement général d'exemption par catégorie n° 651/2014 adopté par la Commission européenne le 17 juin 2014 publié au JOUE du 26 juin 2014, tel que modifié par les Règlements (UE) 2017/1084 de la Commission du 14 juin 2017 publié au JOUE du 20 juin 2017, 2020/972 du 2 juillet 2020 publié au JOUE du 7 juillet 2020 et 2021/1237 du 23 juillet 2021 publié au JOUE du 29 juillet 2021.

La somme des financements publics doit respecter le taux d'aide maximal fixé par ce régime d'aide.

Sur la base de la classification des dépenses éligibles, Bpifrance détermine une aide pouvant aller jusqu'au maximum du taux permis par le régime d'aide selon le tableau suivant :

	Petite entreprise	Moyenne entreprise	Grande entreprise
Recherche industrielle	70%	60%	50%
Dans le cadre d'une collaboration effective <sup>8</sup> et/ou en cas d'une large diffusion des résultats du projet <sup>9</sup>	80%	75%	65%
Développement expérimental	45%	35%	25%
Dans le cadre d'une collaboration effective (1) et/ou en cas d'une large diffusion des résultats du projet (2)	60%	50%	40%

<sup>7</sup> Ce régime s'applique, par dérogation, aux entreprises qui n'étaient pas en difficulté au 31 décembre 2019, mais qui sont devenues des entreprises en difficulté au cours de la période comprise entre le 1er janvier 2020 et le 30 juin 2021.

<sup>8</sup> une collaboration effective existe :

- entre des entreprises parmi lesquelles figure au moins une PME, ou est menée dans au moins deux Etats membres, ou dans un Etat membre et une partie contractante à l'accord EEE, et aucune entreprise unique ne supporte seule plus de 70 % des coûts admissibles ;

ou

- entre une entreprise et un ou plusieurs organismes de recherche et de diffusion des connaissances, et ce ou ces derniers supportent au moins 10 % des coûts admissibles et ont le droit de publier les résultats de leurs propres recherches.

<sup>9</sup> les résultats du projet peuvent être largement diffusés au moyen de conférences, de publications, de dépôts en libre accès ou de logiciels gratuits ou libres.



### 3.2.3. Taux d'aide pour les autres bénéficiaires

Pour les établissements publics et assimilés et les organismes de recherche et assimilés, **l'aide se fait sous forme de subvention.**

Pour les établissements de recherche, quel que soit leur statut, et remplissant une mission d'intérêt général en consacrant une part prépondérante de leur activité à la R&D, les aides sont accordées sous forme de subvention dans la limite de 100% des coûts marginaux. Tout organisme de ce type peut néanmoins, s'il en fait la demande, être pris en charge à 50% des coûts complets. Le responsable légal de l'organisme doit préalablement attester sur l'honneur qu'il possède une comptabilité analytique lui permettant de justifier des coûts présentés dans l'assiette de dépenses. Cette demande est définitive pour l'ensemble des appels à projets de soutien public à la RDI. De ce fait, tout établissement de recherche ayant déjà bénéficié, pour un projet antérieur de la prise en charge de coûts complets au taux de 50% se verra obligatoirement appliquer cette modalité pour l'AAP.

### 3.2.4. Modalités d'aides et retours à l'Etat

Une fois le taux d'aide déterminé, l'aide apportée aux activités économiques sera constituée d'une part de subvention et d'une part remboursable. Dans le cas général, la part de subvention sera de :

- 75% pour les projets majoritairement « recherche industrielle » ;
- 60% pour les projets majoritairement « développement expérimental ».

**L'attention des porteurs est attirée sur le fait qu'il s'agit de 75% ou 60% de l'aide d'Etat qui sera sous forme de subvention et non 75% ou 60% de l'assiette totale du projet (cf. paragraphe 3.2.2).**

Les dépenses qualifiées de « recherche industrielle » doivent faire l'objet d'une justification étayée de la part du demandeur<sup>10</sup>. A défaut, ces dépenses pourront être requalifiées en « développement expérimental » et soutenues selon les modalités correspondantes.

Le remboursement de la part remboursable prend en général la forme d'un échancier forfaitaire, sur trois à cinq annuités, déclenché par le succès technique et/ou commercial du projet.

Le montant des échéances de remboursements tient compte des prévisions d'activité du bénéficiaire et d'un taux d'actualisation, basé sur le taux de référence et d'actualisation fixé par la Commission européenne à la date de la décision d'octroi des aides, lequel est majoré de 100 points de base. Ce taux d'actualisation peut être ajusté à la hausse en cas d'évolution des modalités de remboursement.

Lorsque le comité interministériel en charge du suivi du dispositif, constate en fin de projet une création effective et satisfaisante d'emplois sur le territoire dans le secteur cyber, **il peut être décidé de renoncer à tout ou partie du remboursement.**

<sup>10</sup> Cette justification devant permettant à l'opérateur de s'assurer du respect de l'encadrement européen.

Les modalités plus précises concernant le remboursement de la part remboursable seront précisées dans les conventions prévues entre Bpifrance et les bénéficiaires des aides.

### 3.2.5. Date d'acceptation des coûts et début des projets

La date de début des projets et d'acceptabilité des coûts correspond à la date de relèvement du dossier (cf. calendrier) sous réserve de la sélection définitive. Aucun coût antérieur ne pourra être accepté.

### 3.2.6. Mise en œuvre, suivi des projets et allocation des fonds

Chaque bénéficiaire signe une convention avec Bpifrance. Cette convention précise notamment l'utilisation des crédits, le contenu du projet, le calendrier de réalisation, les modalités de pilotage du projet, le montant des tranches et les critères de déclenchement des tranches successives, les prévisions de cofinancement des projets, les conditions de retour financier pour l'état, les modalités de restitution des données nécessaires au suivi et à l'évaluation des investissements, et les modalités de communication.

La convention d'aide est signée en principe dans un délai de 4 mois à compter de la date de signature de la décision du Premier ministre, sous peine de caducité de la décision d'aide.

Le bénéficiaire met en place un tableau de bord comportant des indicateurs de suivi de l'avancement des projets et des résultats obtenus. Il le transmet régulièrement à Bpifrance selon les modalités prévues par la convention. Pour chaque projet soutenu, une réunion d'avancement est prévue, au moins annuellement. Organisée par Bpifrance le cas échéant, elle associe le Secrétariat général pour l'investissement (SGPI) et l'ensemble des ministères concernés. Cette réunion a pour objet de suivre la mise en œuvre du projet et notamment le niveau d'exécution budgétaire, l'avancement des opérations financées et le respect du planning.

Une fois le projet sélectionné, chaque bénéficiaire soutenu par le PIA est tenu de mentionner ce soutien dans ses actions de communication, ou la publication des résultats du projet, avec la mention unique : « Ce projet a été soutenu par le Programme d'Investissements d'Avenir et le Plan de Relance. », accompagnée des logos du Programme d'Investissements d'Avenir<sup>11</sup> et de France Relance<sup>12</sup>. L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires. Toute autre communication est soumise à l'accord préalable du bénéficiaire.

Le bénéficiaire est tenu de communiquer régulièrement à Bpifrance et à l'État les éléments d'informations nécessaires à l'évaluation de l'avancement du projet (performance commerciale, emplois créés, brevets déposés, effets environnementaux et énergétiques), ainsi qu'à l'évaluation *ex post* donc après réalisation du projet. Ces éléments, et leurs évolutions, sont précisés dans conditions générales de la convention d'aide entre Bpifrance et le bénéficiaire.



## **4. Critères de sélection et fixation du niveau de financement**

Les dossiers retenus pour instruction seront **évalués selon les critères ci-dessous**.

### **4.1. Pertinence du projet**

- Pertinence de la taille du projet et du dimensionnement des étapes conduisant à une exploitation commerciale future. Le projet mené présente une envergure appropriée pour obtenir des résultats en quantité suffisante pour être représentatifs et exploitables ;
- Pertinence des choix technologiques ;
- Caractère généralisable, à un coût global raisonnable, de la solution innovante développée dans le cadre du projet soumis et existence d'un marché pour ce type de solution rendant possible un fort impact économique ;
- Adéquation du projet avec les objectifs de la stratégie d'accélération cyber, notamment la capacité du projet à accroître l'autonomie nationale ou européenne en particulier au regard des enjeux de sécurité et de souveraineté dans le cyber espace.

### **4.2. Impact économique et social du projet**

- Pertinence des objectifs commerciaux en exploitation, notamment sur l'adéquation du niveau d'équipement des infrastructures avec un déploiement massif futur ;
- Argumentation du modèle économique au regard d'un déploiement futur, qu'il s'agisse du modèle économique de l'entreprise commercialisant la solution ou de la viabilité économique pour les partenaires supportant une expérimentation ;
- Capacité de valorisation des travaux du projet notamment en termes de propriété intellectuelle (notamment brevets et licences) ;
- Capacité à faire progresser les connaissances sur les usages, les domaines de pertinence et l'acceptabilité des systèmes et des services ; Le projet doit présenter à cet égard des expérimentations menées avec de vrais usagers/clients.
- Impact sociétal

### **4.3. Critères de performance environnementale et impact sociétal**

L'AAP sélectionne des projets démontrant une réelle prise en compte de la transition énergétique et écologique. Les effets positifs attendus et démontrés du projet, du point de vue écologique et énergétique, de même que les risques d'impacts négatifs, sont utilisés pour sélectionner les meilleurs projets parmi ceux présentés, ou pour moduler le niveau d'intervention publique accordé au projet.

Chaque projet doit expliciter sa contribution au développement durable, en présentant les effets, quantifiés autant que faire se peut, directs ou indirects, positifs ou négatifs, estimés pour les axes ci-dessous (cf. Annexe 2) :

- atténuation au changement climatique ;
- adaptation au changement climatique ;
- utilisation durable et protection des ressources aquatiques et marines ;
- transition vers une économie circulaire ;

- prévention et réduction de la pollution ;
- protection et restauration de la biodiversité et des écosystèmes ;

Compte-tenu de la nature des projets attendus, une attention particulière sera portée aux performances visées par les projets en matière d'utilisation durable des ressources et de sobriété énergétique.

#### **4.4. Qualité de l'organisation du projet**

- Pertinence et complémentarité du partenariat (adéquation du nombre de partenaires aux enjeux du projet, synergie et valeur ajoutée de tous les partenaires) ;
- Gouvernance, gestion et maîtrise des risques inhérents au projet, par exemple, avancement du projet d'accord de consortium ;
- Adéquation du programme de travail et du budget avec les objectifs du projet (définition des jalons, des résultats intermédiaires et des livrables) ;
- Solidité du plan de financement du projet et robustesse financière des partenaires, notamment capacité financière à mener le projet ;
- Qualité des informations transmises : celles-ci apportent suffisamment de précision dans les références et les arguments pour permettre d'évaluer sérieusement les aspects techniques et scientifiques, la justification des coûts du plan de travail ainsi que les perspectives industrielles et commerciales.

#### **4.5. Impact de l'intervention publique**

- Caractère incitatif de l'intervention ;
- Effet de levier de l'intervention publique.

### **5. Composition des dossiers**

Le dossier de candidature complet est constitué de plusieurs annexes disponibles sur le site internet de l'appel à projets.

Les modèles de dossier de candidature et de base de données des coûts du projet, présentant notamment la liste exhaustive des documents à fournir, sont disponibles en téléchargement sur le site internet Bpifrance de l'appel à projets : <https://www.bpifrance.fr/nos-appels-a-projets-concours/appel-a-projets-cryptographie-post-quantique>

Les projets incomplets ou ne respectant pas les formats de soumission ne sont pas recevables.

### **6. Processus de sélection**

Afin de retenir les meilleurs projets respectant l'ambition du PIA, **la procédure de sélection est menée par un comité d'expert** qui conduit une première analyse des dossiers reçus en termes d'éligibilité et d'opportunité. Cette analyse peut conduire à une audition des porteurs de projets.

**L’instruction est conduite par Bpifrance, qui s’appuie sur les experts des ministères.** À l’issue de cette phase d’instruction, **la décision d’octroi de l’aide est prise par le Premier Ministre, sur proposition du Comité exécutif et après avis du Secrétariat général pour l’investissement.**

## **7. Données**

Le partage de données entre les acteurs d’une filière est un élément essentiel à sa structuration, axe fort de la Stratégie Nationale cyber. **Dans le plein respect du droit de propriété des producteurs des données**, cet appel à projets introduit certaines exigences qui doivent faciliter leur partage. Ces exigences seront valables pour tous les projets recevant des financements étatiques dans le cadre de la Stratégie Nationale Cyber.

### **7.1. Protection et respect de la réglementation**

Il est essentiel que les données produites ou manipulées dans le cadre des projets financés par la Stratégie Nationale, que ce soit lors de la phase de développement, d’expérimentation ou ultérieurement en production, soient protégées au bon niveau en fonction de leur sensibilité. Les objectifs sont à la fois de veiller à la protection de la propriété intellectuelle, d’éviter l’appauvrissement informationnel (typiquement contractuel) et de prévenir au mieux les fuites massives de données.

Dans cette optique un travail d’analyse préalable est demandé au(x) porteur(s) pour déterminer le niveau de sensibilité des différentes catégories de données du projet. Les mesures de sécurité qui en découleront (et qui devront être implémentées dans le cadre du projet) pourront faire intervenir la protection des communications de bout en bout (i.e. cryptographie) lors du transfert des données, un stockage sécurisé (i.e. chiffré et sauvegardé), un contrôle d’accès adéquat ainsi que des mesures juridiques ou contractuelles appropriées. Le cas échéant, le respect de la réglementation applicable (RGPD par exemple) sera bien sûr le point de départ de cette analyse et de ces travaux.

### **7.2. Production, stockage et valorisation de données d’intérêt cyber**

Dans le cadre des projets candidats, il est également demandé au(x) porteur(s) de capitaliser sur les opportunités de production de données d’intérêt cyber (de toutes natures). Cela implique de mettre en place les mécanismes ad-hoc de captation, de prétraitement (typiquement de labélisation ou de normalisation) et de stockage de ces données même s’il s’agit de données annexes non essentielles au projet.

Les réflexions sur un modèle économique autour de ces données sont fortement encouragées.

Dans le cas d’une abondance trop importante de données ou de contraintes spécifiques, une priorisation sur les données à stocker pourra être effectuée en discussion avec le comité de suivi du projet. De même, la durée de stockage est à déterminer en fonction de la typologie des données concernées.

Le non-respect de cet aspect impactera négativement le dossier lors du processus de sélection et pourra in fine aboutir à une réduction du taux d’aide.

### **7.3. Accès aux données d'expérimentation**

Les données générées dans le cadre du paragraphe précédent restent la propriété de leur producteur. Néanmoins, il est demandé au(x) porteur(s) bénéficiant d'aide d'Etat dans le cadre de la Stratégie Nationale de cybersécurité de s'engager à mettre à disposition ces données gracieusement de manière ponctuelle dans le cadre d'expérimentations techniques non commerciales sous réserve de la compatibilité avec la réglementation et avec la non-concurrence des acteurs. Dans les deux cas d'exception, les données pourront éventuellement être mise à disposition si des traitements permettent de s'affranchir de ces contraintes (par exemple par de la cryptographie homomorphe, de l'anonymisation, de l'échantillonnage, etc.).

## **8. Confidentialité**

Bpifrance s'assure que les documents transmis dans le cadre de l'AAP sont soumis à la plus stricte confidentialité et ne sont communiqués que dans le cadre de l'expertise et de la gouvernance du PIA, de la Stratégie Nationale de cybersécurité et du Grand Défi cybersécurité. L'ensemble des personnes ayant accès aux dossiers de candidatures est tenu à la plus stricte confidentialité.

Une fois le dossier sélectionné, les bénéficiaires sont tenus de mentionner le soutien apporté par le Programme d'investissements d'avenir dans leurs actions de communication et la publication de leurs résultats avec la mention unique « ce projet a été financé par le Gouvernement dans le cadre du plan de relance et du programme d'investissement d'avenir » et les logos de France Relance, du PIA et de Bpifrance.

Toute opération de communication doit être concertée entre le porteur et Bpifrance, afin de vérifier notamment le caractère diffusable des informations et la conformité des références au plan de relance, au PIA et à Bpifrance.

L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires.

Enfin, les bénéficiaires sont tenus à une obligation de transparence et de *reporting* vis-à-vis de l'État et de Bpifrance, nécessaire à l'évaluation *ex post* des projets ou du plan de relance.

## **9. Soumission des projets**

Les projets peuvent être soumis pendant toute la période d'ouverture et dans la limite du budget alloué sur la plateforme de Bpifrance : <https://extranet.bpifrance.fr/projets-innovants-collaboratifs/>

Pour toutes questions relatives au dépôt du dossier sur la plateforme, Bpifrance peut être contacté directement : [strategies-acceleration@bpifrance.fr](mailto:strategies-acceleration@bpifrance.fr)

Pour toutes questions relatives à l'appel à projets, le Directeur de programme peut être contacté directement : [aap-technos-cyber.dge@finances.gouv.fr](mailto:aap-technos-cyber.dge@finances.gouv.fr)

Pour toutes questions relatives à la Stratégie Nationale cyber ou dépassant le cadre de cet appel à projets, le coordinateur de la Stratégie peut être contacté directement : [strategie.cyber@pm.gouv.fr](mailto:strategie.cyber@pm.gouv.fr)

Pour toutes questions relatives à la Stratégie Nationale quantique ou dépassant le cadre de cet appel à projets, le coordinateur de la Stratégie peut être contacté directement :  
[quantique.info@pm.gouv.fr](mailto:quantique.info@pm.gouv.fr)

## Annexe 1 : Implémentation des standards de chiffrement post-quantique

### Mise en œuvre d’algorithmes résistants au calcul quantique

L’émergence de l’informatique quantique fait peser un risque sur les algorithmes cryptographiques asymétriques actuellement employés. La mise à jour d’un grand nombre de schémas de chiffrement et d’authentification vers des algorithmes résistants à l’informatique quantique (dit PQC – Post Quantum Cryptography) est indispensable à courte échéance, afin de protéger les systèmes de communication et d’authentification utilisés aujourd’hui de manière généralisée, par tous et tous les jours.

À travers cet appel à projet, les stratégies quantique et cyber souhaitent donc soutenir des projets visant à mettre en œuvre de manière opérationnelle des algorithmes PQC standardisés et faisant consensus dans la communauté (typiquement ceux qui seront sélectionnés par le NIST<sup>13</sup>, ces derniers ayant vocation à être les seuls acceptés une fois publiés). L’évaluation valorisera également les projets intégrant la possibilité de remplacer l’algorithme retenu par un autre sans pour autant revoir l’architecture du produit dans son ensemble.

Les déposants devront proposer des projets d’implémentations PQC adaptées à au moins l’une des contraintes suivantes :

1. Composants hardware destinés à des utilisations dans des systèmes embarqués ;
2. Langages de programmation ou méthodes de développement permettant une sécurité renforcée.

Par ailleurs, il est demandé aux déposants de respecter les consignes suivantes :

- Prendre en compte les recommandations du référentiel général de sécurité de l’ANSSI<sup>14</sup>, en particulier les annexes B1<sup>15</sup>, B2<sup>16</sup> et B3<sup>17</sup> pour les algorithmes crypto. Les recommandations ne prennent pas en compte les algorithmes post-quantiques mais les niveaux de sécurité sont transposables et les bonnes pratiques d’implémentation ne changent pas.
- Réaliser un audit de sécurité complet avec un CESTI en fonction de la cible de sécurité choisie par le projet dans le respect de l’état de l’art afin de garantir le respect du modèle de sécurité choisi. Selon le contexte d’emploi prévu, le modèle de sécurité devra être adapté, mais l’implémentation devra prendre en compte dès le départ les contraintes de cet environnement. Une attention particulière devra être apportée à la protection contre les attaques par canaux auxiliaires.

<sup>13</sup> <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>

<sup>14</sup> <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>

<sup>15</sup> RGS B1 – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques :  
[https://www.ssi.gouv.fr/uploads/2014/11/RGS\\_v-2-0\\_B1.pdf](https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf)

<sup>16</sup> RGS B2 – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques :  
[https://www.ssi.gouv.fr/uploads/2014/11/RGS\\_v-2-0\\_B2.pdf](https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf)

<sup>17</sup> RGS B3 – Règles et recommandations concernant les mécanismes d’authentification, version 1.0 et version 2.0  
[https://www.ssi.gouv.fr/uploads/2014/11/RGS\\_v-2-0\\_B3.pdf](https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf)



- Favoriser de manière générale les approches open-source, à l'exception des implémentations optimisées au-delà de l'état de l'art connu, dont on pourra choisir de valoriser la propriété intellectuelle dans un produit fini ou via cession de licence.

### **Projets hardware**

Pour les projets hardware, l'objectif principal relève de l'implémentation des algorithmes PQC dans des schémas cryptographiques avec contraintes d'embarquabilité. Cela peut aller du téléphone portable à la carte à puce en passant par les nombreux systèmes dit « IoT » (capteurs, microcontrôleurs...).

Une attention particulière à la consommation énergétique et à la consommation mémoire est attendue dans la plupart des contextes. L'implémentation pourra être logicielle uniquement sur un matériel adapté (par exemple SoC embarqué), en co-design logiciel-matériel (par exemple microprocesseur + FPGA ou microcontrôleur + module hardware ASIC), voire uniquement matérielle, en fonction des besoins en espace mémoire, en vitesse et en consommation du projet.

Pour l'implémentation d'un schéma cryptographique complet, l'utilisation d'un générateur de nombres aléatoires (RNG) en complément des algorithmes PQC est en général nécessaire. Les générateurs proposés devront disposer d'une analyse de leur source d'entropie utilisable dans le cadre d'une certification selon le référentiel AIS31 publié par le BSI<sup>18</sup>. Une telle analyse est en principe plus aisée pour un générateur aléatoire reposant sur un phénomène quantique (QRNG) que pour les générateurs aléatoires électroniques habituels dont les sources de bruit ne sont pas toujours bien caractérisées. Bien que le QRNG ne soit pas le sujet principal de cet appel à projet, l'intégration conjointe d'un algorithme de PQC et d'un QRNG pour un schéma cryptographique est valorisée dans le processus d'évaluation.

### **Projets logiciels**

S'agissant des implémentations logicielles, l'utilisation d'un langage et/ou un cycle de développement apportant une résistance renforcée par conception à certaines attaques (e.g. Langage Rust, méthodes formelles, *etc.*) est encouragé. De plus, la partie logicielle devra minimiser les dépendances externes. Dans le cadre du développement d'implémentations efficaces, la protection du point de la propriété intellectuelle est fortement encouragée.

Dans un objectif de performances, la possibilité de remplacer à la compilation certaines sous-fonctions par des dépendances externes (OpenSSL, ...) est également encouragée.

<sup>18</sup> Cf "A proposal for: Functionality classes for random number generators" available at [https://www.bsi.bund.de/EN/Topics/Cryptography/RandomNumberGenerators/random\\_number\\_generators.html](https://www.bsi.bund.de/EN/Topics/Cryptography/RandomNumberGenerators/random_number_generators.html)

## **Annexe 2 : Critères de performance environnementale**

Les projets causant un préjudice important du point de vue de l'environnement seront exclus (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie<sup>19</sup>.

En créant un langage commun et une définition claire de ce qui est « durable », la taxonomie est destinée à limiter les risques d'écoblanchiment (ou "greenwashing") et de distorsion de concurrence, et à faciliter la transformation de l'économie vers une durabilité environnementale accrue. Ainsi, la taxonomie définit la durabilité au regard des **six objectifs environnementaux** suivants :

- l'atténuation du changement climatique ;
- l'adaptation au changement climatique ;
- l'utilisation durable et la protection des ressources aquatiques et marines ;
- la transition vers une économie circulaire ;
- la prévention et la réduction de la pollution ;
- la protection et la restauration de la biodiversité et des écosystèmes.

Compte-tenu de la nature des projets attendus, une attention particulière sera portée aux performances visées par les projets en matière d'utilisation durable des ressources et de sobriété énergétique.

Pour l'évaluation technique de l'impact du projet vis-à-vis de chaque objectif environnemental, **le déposant doit renseigner le document dédié disponible sur le site de l'appel à projets (dossier de candidature) et le joindre au dossier de candidature.**

Il s'agira d'autoévaluer les impacts prévisibles de la solution proposée (faisant l'objet de l'aide) par rapport à une solution de référence explicitée et argumentée. Cette analyse tient compte du cycle de vie des process et du ou des produits ou livrables du projet, suivant les usages qui en sont faits. En tant que de besoin, ces estimations pourront être étayées par des analyses en cycle de vie plus complètes.

<sup>19</sup> Règlement (UE) 2020/852 sur l'établissement d'un cadre visant à favoriser les investissements durables, en mettant en place un système de classification (ou « taxonomie ») pour les activités économiques durables sur le plan environnemental, publié au journal officiel de l'UE le 22 juin 2020.