

## ANNEXE CCTP PHOTOVOLTAÏQUE

- **clause relative à la performance des modules photovoltaïques et à la durée de garantie ;**

« Le titulaire du marché doit assurer la fourniture et la pose de modules photovoltaïques de haute performance, de technologie de type silicium monocristallin.

Les modules avec leurs cellules photovoltaïques doivent satisfaire aux conditions décrites ci-après :

Rendement du module STC minimal : 19%

Garantie du produit : 20 ans minimum\* ;

Garantie de performance : 85 % à l'année 25 ;

L'ensemble des modules constituant le générateur photovoltaïque doivent avoir des caractéristiques identiques avec une tolérance de +/- 5%/0% sur la valeur de la puissance crête. »

- **clause attestant de l'absence d'éléments perturbateurs du recyclage ;**

« Afin d'optimiser la recyclabilité des modules, le titulaire est tenu de fournir des modules garantis sans éléments perturbateurs du recyclage.

Pour être conforme à cette exigence, les modules doivent respecter, selon leur composition, pour la face avant et la face arrière les exigences suivantes :

- si composite : la résine doit être hors « époxy » et les couches polymères sans fluor ;

- si polymères : le polymère doit être sans fluor ».

- **clause de traçabilité du verre et d'absence de la présence d'antimoine ;**

« Afin d'optimiser la recyclabilité des modules, le Titulaire est tenu de faire apposer sur le verre composant ses modules un marquage précisant l'identité du fournisseur et la présence, ou non, d'antimoine dans le verre ».

- **clause limitant la présence de substances dangereuses ;**

« Afin de réduire l'impact environnemental des modules pendant les phases de fabrication, d'élimination et de recyclage, le titulaire est tenu de fournir des modules présentant un niveau de substances dangereuses aussi faible que possible.

A ce titre, :

- la teneur en plomb des modules ne peut excéder 0,1% ;

- la teneur en cadmium des modules ne peut excéder 0,01% ».

- **clause relative à la cybersécurité.**

Contrôles et audits :

Durant la préparation ou la réalisation du marché, l'acheteur peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants.

Dans tous les cas, des audits légitimés par la sélection ou le suivi de titulaires de marchés peuvent être réalisés sans accord préalable dès lors que les tests et sondes respectent les conventions techniques d'usage permettant de les identifier (par exemple, User-Agent référençant une URL d'explication, reverse-DNS permettant de donner une origine claire à une adresse IP, etc.).

Documentation :

Le Titulaire est tenu de fournir à première demande la documentation nécessaire à la sécurisation de ses fournitures.

En particulier, sa documentation explicite tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc.), et les dispositifs de contrôle d'accès et de maintien en condition de sécurité.

Si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre Sécurité du mode d'emploi (par exemple, la procédure de changement des mots de passe par défaut ou des interfaces exposées, de mise à jour de composants logiciels...).

Etat de l'art :

La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient à chaque titulaire de marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition.

A première demande, le titulaire fournit tous les éléments démontrant la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

Concernant plus spécifiquement les appareils connectés, le titulaire met en place :

- un dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
- un dispositif de mise à jour sécurisé.
- une limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connexions non chiffrées TELNET, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

#### Signalements de sécurité :

Pour les prestations, produits et services qu'il fournit dans le cadre du marché, le titulaire met à disposition des fils publics par abonnement (flux RSS, liste de diffusion par courriel) ou autre dispositif d'information dédié à la sécurité informatique. Ces fils, identifiés dans le chapitre Sécurité des modes d'emploi, permettent aux bénéficiaires d'être tenu informés en continu des événements et changements impactant la sécurité, par exemple annonce de correctif, attaque en cours, nouvelle configuration à appliquer, violation de données à caractère personnel, etc.

Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing. Les fils peuvent être multiples dans le cas de fournitures en plusieurs composants mais sans laisser de vide d'information.

Réciproquement, les outils numériques mis à disposition permettent aux bénéficiaires et leurs experts en cybersécurité de signaler directement aux équipes appropriées du titulaire de possibles failles ou détournements de dispositifs de sécurité.

Afin que ces signalements soient effectifs et efficaces, les conventions d'usage en cybersécurité sont respectées (security.txt, abuse@). Dans tous les cas, il faut moins d'une minute pour trouver le point d'entrée approprié du signalement.

Après analyse partagée et vérification, le titulaire a obligation d'enregistrer les failles auprès des autorités compétentes (CERT nationaux pour les éditeurs, registres RGPD et CNIL ou équivalent pour la divulgation de données personnelles, ANSSI pour les opérateurs d'importance vitale ou de services essentiels, etc.) en suivant les réglementations établies. L'emploi d'un système de cotation connu (par exemple CVSS) permet de hiérarchiser l'urgence pour tous les acteurs en aval. A défaut d'action sous 3 mois, l'acheteur a la possibilité de se substituer aux titulaires dans les actions précédentes ou de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques).