

Agence nationale de la sécurité des  
systèmes d'information

**Le Directeur général**

**15 DEC. 2023**

Paris, le  
N° *2171* /ANSSI/SDE

**DECISION DE QUALIFICATION D'UN PRODUIT**  
**AU NIVEAU STANDARD**

**CRYHOD**  
**VERSION Q2021.X AVEC X≥3**

**PRIM'X TECHNOLOGIES**

**RCS 448 603 985**

**18 rue du Général Mouton-Duvernet**  
**69003 Lyon Cedex**  
**France**

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1<sup>er</sup> ;

Vu le décret du 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;

Vu le processus de qualification d'un produit, version en vigueur ;

Vu le rapport de certification, ANSSI-CC-2022/35, 27/06/2022 ;

Vu le dossier de demande de qualification déposé par PRIM'X,

Décide :

- Art. 1<sup>er</sup> – Le produit fourni par la société PRIM'X TECHNOLOGIES portant le nom « CRYHOD » en version Q2021.X avec X $\geq$ 3 respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 et est qualifié au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.
- Art. 2 – Le produit fourni par la société PRIM'X portant le nom « CRYHOD » en version Q2021.X avec X $\geq$ 3 est agréé pour la protection d'informations marquées Diffusion Restreinte ou classifiées Diffusion Restreinte OTAN/NATO *Restricted* ou Restreint UE/UE *Restricted* sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.
- Art. 3 – La présente décision est valable jusqu'au 17 octobre 2025.

Vincent STRUBEL  
Directeur général de l'Agence nationale  
de la sécurité des systèmes d'information



## Annexe

Conditions et limites de la qualification.
--

### Références

- [1]. Rapport de certification, ANSSI-CC-2022/35, 27/06/2022.
- [GUIDE\_INSTALL]. Cryhod Q.2021 Guide d'installation, référence PX20A1406r1, version 1.1 ;
- [GUIDE\_ADMIN]. Cryhod Q2021, Mise en œuvre de la signature des politiques, référence PX13C133r4r2, version 1.4 ;
- [GUIDE\_UTIL]. Cryhod Q.2021, Guide d'utilisation, référence PX20A1404r4 ;

### Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

- C0. Elle emploie la version qualifiée du produit la plus à jour.
- C1. Les objectifs de sécurité sur l'environnement définis dans la cible de sécurité référencée dans le rapport [1] doivent être respectés.
- C2. Les restrictions d'usage figurant dans le rapport [1] doivent être respectées.
- C3. Les restrictions d'usage figurant au chapitre 2.6 du rapport [1] doivent être respectées ; l'utilisateur du produit devra en particulier s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS] à savoir :
  - sensibiliser l'utilisateur au fait qu'il ne doit pas laisser son PC sans surveillance une fois que le système d'exploitation a été lancé ;
  - lorsque la TOE est installée sur un poste, protéger la partition système par la TOE ;
  - désactiver l'utilisation des périphériques DMA dans les paramètres de configuration du BIOS de la station de travail ;
  - désactiver la fonctionnalité de production d'une image mémoire en cas de défaillance du système si elle n'est pas nécessaire ;
  - générer, conformément aux règles et recommandations de l'ANSSI, les clés RSA générées à l'extérieur du produit puis embarquées dans des fichiers de clés ou des objets physiques (pour être utilisées en tant que clés d'accès) ;
  - configurer les accès obligatoires et l'accès de recouvrement de l'administrateur (politique P131) ;
  - fixer le seuil d'acceptation des mots de passe à 100% (politique P710) et leur longueur à 12 caractères au minimum (politique P712) ;

- utiliser la politique P258 avec sa valeur par défaut soit « Imposer le transchiffrement de la partition » ;
  - désactiver la politique P382 qui fait réaliser les calculs AES par le processeur plutôt que par le logiciel fourni par Prim'X ;
  - utiliser la version 2.2 de RSA PKCS#1 avec SHA-256 (politique P383) ;
  - configurer la politique P386 avec le mécanisme de signature « PKCS#1 v2.2 PSS » ;
  - configurer la politique P387 avec le mécanisme de dérivation de mot de passe « SHA256-PBKDF2 » ou « SHA512-PBKDF2 » ;
  - configurer la politique P885 à « Non installé » (valeur par défaut) pour ne pas autoriser l'installation du module de démarrage automatique ;
  - configurer à « oui » la politique P303 afin d'activer les événements pour toutes les opérations d'administration ;
  - configurer la politique P339 à « 0 » pour permettre la collecte d'information pour le support technique ;
  - renseigner le mot NONE dans le nom de la valeur de la politique P137 ;
  - pour le mode alternatif, configurer la politique P070 en indiquant le chemin du fichier de configuration alternative des politiques.
- C2. Les guides d'installation [GUIDE\_INSTALL], d'administration [GUIDE\_ADMIN] et d'utilisation [GUIDE\_UTIL] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout au long de son cycle de vie.
- C3. Dans le cas d'un usage pour la protection d'informations *Diffusion Restreinte*, *Restreint OTAN* ou *Restreint UE/UE Restricted*, le système d'information support doit également être homologué pour ce même niveau.

### Limite

- L1. Seules les fonctions identifiées dans le rapport [1] sont couvertes par la présente décision de qualification.