Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Bureau Qualifications et Agréments

Paris, le 26 MARS 2020
N° 519 /ANSSI/SDE

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

PANORAMA E² version 2020

(version de build supérieure à 20.00.010)

CODRA INGENIERIE INFORMATIQUE

RCS 338 767 296 Evry

Immeuble Hélios – 2 rue Christophe Colomb
91300 MASSY
France

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

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

Vu le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information ;

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 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu la décision du 22 octobre 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale) ;

Vu l'Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles ;

Vu le processus de qualification d'un produit, référence QUAL-PROD-PROCESS, version en vigueur ;

Vu le dossier de demande de qualification d'un produit fourni par la société CODRA INGENIERIE INFORMATIQUE le 21 août 2017,

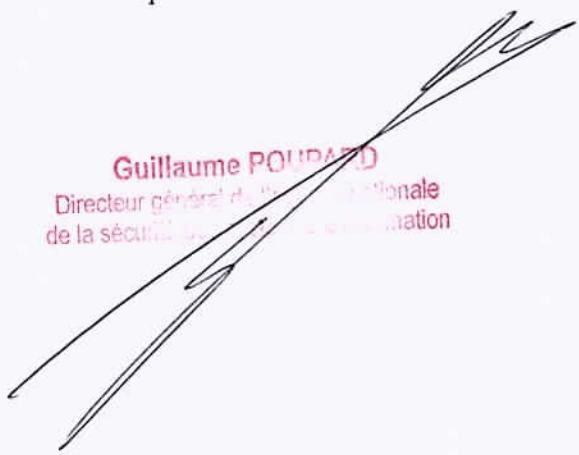
Vu le rapport d'analyse d'impact – Panorama E2 7.00 vers 2020, version 1.1 du 10 février 2020, fourni par CODRA INGENIERIE INFORMATIQUE ;

Décide :

Art. 1er – Le produit fourni par la société CODRA INGENIERIE INFORMATIQUE portant le nom « PANORAMA E^2 » en version 2020 respecte les règles fixées par le décret n° 2015-350 du 27 mars 2015 et est qualifié au niveau élémentaire sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La présente décision est valable pour une durée de 3 ans.

Art. 3 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.



Fiche 1

Description du produit

Désignation et versions

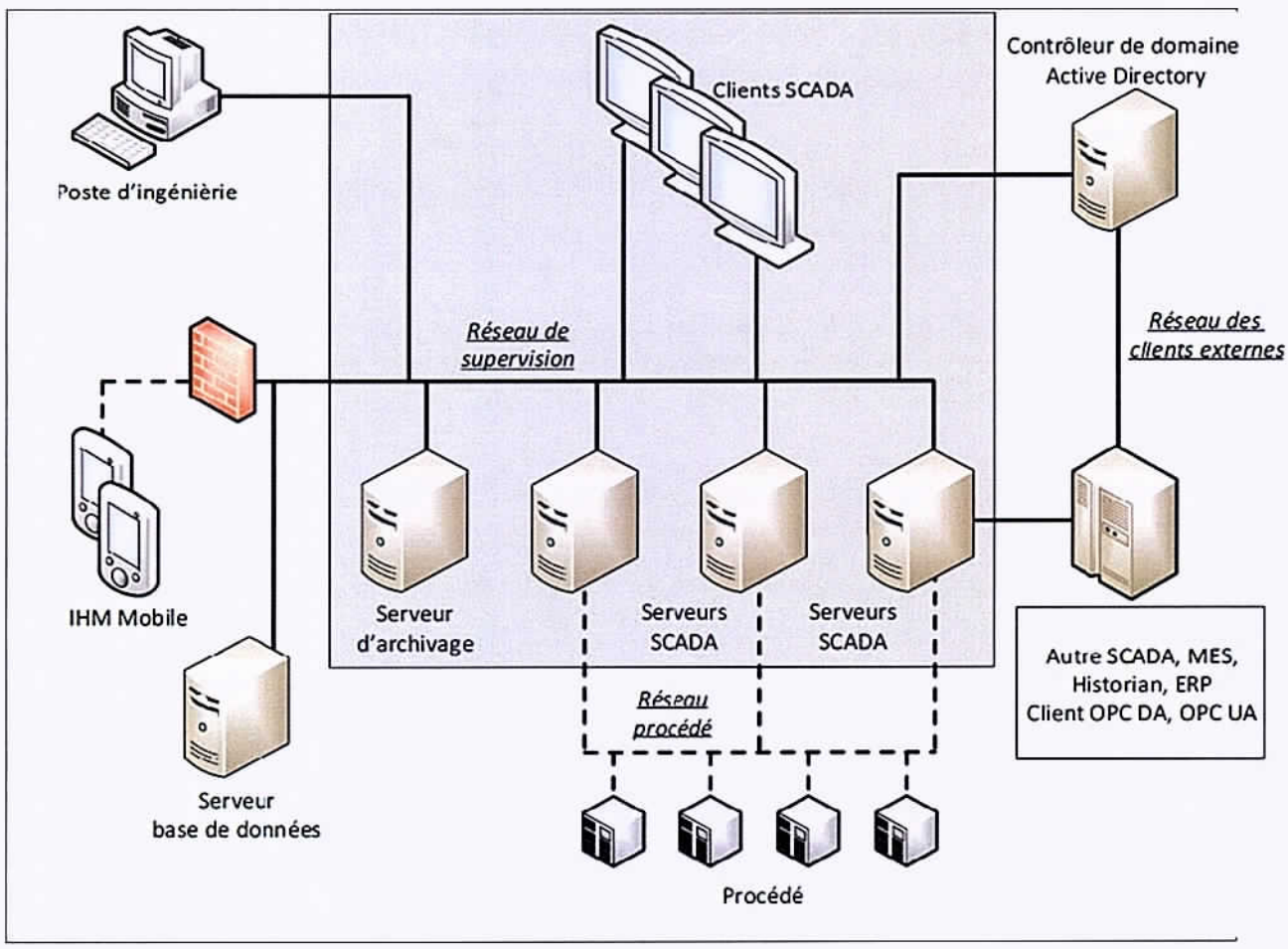
Le produit qualifié est la solution logicielle « Panorama E^2 » en version 2020 fournie par l'entreprise *CODRA INGENIERIE INFORMATIQUE.*

Présentation générale

Conçu pour être déployé au sein de réseaux industriels, la solution Panorama E^2 inclut un serveur SCADA (*Supervisory Control And Data Acquisition*) pouvant être connecté à des équipements de terrain de niveau 1 au sens de la classification CIM (*Computer-Integrated Manufacturing*). Ce serveur permet l'acquisition de données terrain et l'envoi de commandes, ainsi que la gestion des alarmes.

La solution Panorama E^2 inclut également un client SCADA, qui permet notamment de présenter une interface homme-machine (IHM) à l'utilisateur.

Panorama E^2 peut enfin être connecté à d'autres équipements de niveaux CIM 2 et CIM 3, en particulier via un serveur OPC-UA (*Open Platform Communication – Unified Architecture*) avec liaison de type HTTPS.



- *Figure 1. Architecture de déploiement du produit*

Les fonctions de sécurité du produit sont :

- la gestion des entrées malformées ;
- la protection de l'intégrité et de l'authenticité des flux des réseaux de supervision et du réseau de clients externes ;
- la protection de la confidentialité des secrets de connexion des utilisateurs ;
- l'intégrité des certificats des utilisateurs des interfaces OPC-UA ;
- l'intégrité des secrets de connexion aux serveurs de données OPC-UA ;
- l'authentification des accès aux bases de données via l'Active Directory ;
- l'authentification sécurisée ;
- la gestion des droits d'accès ;
- la signature du logiciel ;
- l'intégrité et la confidentialité de la configuration ;
- l'intégrité des journaux.

Fiche 2

Conditions et limites de la qualification

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 :

C1. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [CERTIF] du produit doivent être respectées ; l'utilisateur du produit certifié 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].

C2. Les guides [GUIDES] du produit doivent être mis en œuvre lors de l'installation, du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie.

C3. L'utilisateur doit consulter les bulletins de sécurité [BDS] publiés par le développeur. En particulier, il convient de mettre en place une politique de surveillance de l'état d'expiration des certificats et de mise à jour de la liste pour retirer les empreintes des certificats expirés pour OPC-UA et les remplacer par celles des certificats renouvelés.

C4. Le réseau de supervision, le réseau des clients externes et le réseau procédé doivent être des réseaux séparés.

Limites

L1. Seules les fonctions décrites dans la fiche 1 sont couvertes par la présente décision de qualification.

L2. Les protocoles LON et IOT ne doivent pas être utilisés.

L3. La fonction Agent SNMP ne doit pas être utilisée.

L4. Les liaisons de type HTTP, Net.TCP et OPC.TCP ne doivent pas être utilisées.

L5. Les fonctions suivantes ne font pas partie du périmètre du produit qualifié :

- les fonctions Astreinte et Messagerie ;
- la fonction Réseau (FTP, Ping) ;
- la fonction IHM Mobile et l'accès SmartBMS ;
- la fonction GeoScada ;
- la fonction Historian : Export, y compris le reversement d'archives ;
- l'ajout d'objets utilisateurs.

L6. Les parties de fonction suivantes ne font pas partie du périmètre du produit qualifié :

- l'acquisition IoT de la fonction Acquisition ;
- les objets Navigateur Internet de la fonction IHM ;
- l'authentification Panorama et la modification en exploitation des profils utilisateurs de la fonction Gestion des utilisateurs et contrôle d'accès ;
- la fonction de pilotage des serveurs de la fonction de Déploiement réseau.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus
[LPM]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur https://www.legifrance.fr
[RGS]	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. Disponible sur https://www.legifrance.fr

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation CSPN Panorama - référence : OPPIDA/CESTI/PANORAMA/RTE/1.1 - version : 1.1 - en date du : 26 septembre 2019

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification Panorama E^2 Version 2020, référence : ANSSI-CSPN-2019/14 en date du 7novembre 2019.
[CRYPTO]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques,_annexée au Référentiel général de sécurité (RGS_B1), disponible sur www.ssi.gouv.fr. - version : 2.03 - en date du : 21 février 2014

Guides d'utilisation et documentations techniques de l'industriel

[GUIDES]	Guide technique programmeur, intégré en tant qu'aide en ligne dans le produit.
[BDS]	Bulletins de sécurité publiés à l'adresse : https://codra.net/fr/service/bulletin-securite-informatique
[CDS]	Cible de sécurité CSPN Panorama, Serveur et client Court-terme - référence : PANO/CibleCSPN Court-terme-V4.0 - version : 4.0 - en date du : 10 février 2020
[IAR]	Rapport d'analyse d'impact, Panorama E2 7.00 vers 2020 - référence : PANO/IAR E2 7.00-vers-2020 - version : 1.1 - en date du : 10 février 2020