

PREMIER MINISTRE

20 DEC. 2017

Secrétariat général
de la défense
et de la sécurité nationale

Paris, le
N° ~~6369~~ /ANSSI/SDE/PSS/BQA

Agence nationale de la sécurité
des systèmes d'information

Bureau Qualifications et Agréments

DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU STANDARD

NOKIA 9500 MICROWAVE PACKET RADIO en version 07.01.0B

Logiciel embarqué dans le multiplexeur avec sa carte *COREVO*, version 34.09.00

ALCATEL-LUCENT INTERNATIONAL
493 378 939 R.C.S. EVRY
Route de Villejust, Nokia Paris Saclay,
91 602 Nozay
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 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, notamment son article 9 ;

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° 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 ;

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^{er} ;

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 l'instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'*UNION EUROPEENNE* ;

Vu l'instruction générale interministérielle n° 2100 du 1^{er} décembre 1975 sur l'application en France du système de sécurité de l'*ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD* ;

Vu le *processus* de qualification d'un produit,

Décide :

- Art. 1^{er} – Le produit fourni par la société *NOKIA* portant le nom *NOKIA 9500 MICROWAVE PACKET RADIO* en version 07.01.0B respecte les règles fixées par les décrets n° 2010-112 du 2 février 2010 et n° 2015-350 du 27 mars 2015 et est qualifié au niveau standard sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.
- Art. 2 – La fonction chiffrement des paquets *ethernet* au niveau de la couche 1 du produit est agréée pour la protection des informations marquées *Diffusion Restreinte* ou classifiées au niveau *Diffusion Restreinte OTAN* ou *Restreint UE/UE Restricted*.
- Art. 3 – La présente décision est valable pour une durée de 3 ans.
- Art. 4 – 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.

Guillaume POURARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information



Fiche 1

Description du produit

Désignation et versions

Le produit qualifié est le logiciel *NOKIA 9500 MICROWAVE PACKET RADIO* en version 07.01.0B fourni par l'entreprise *NOKIA*. Cette qualification couvre le produit embarqué dans le multiplexeur avec sa carte *COREVO* en version 34.09.00.

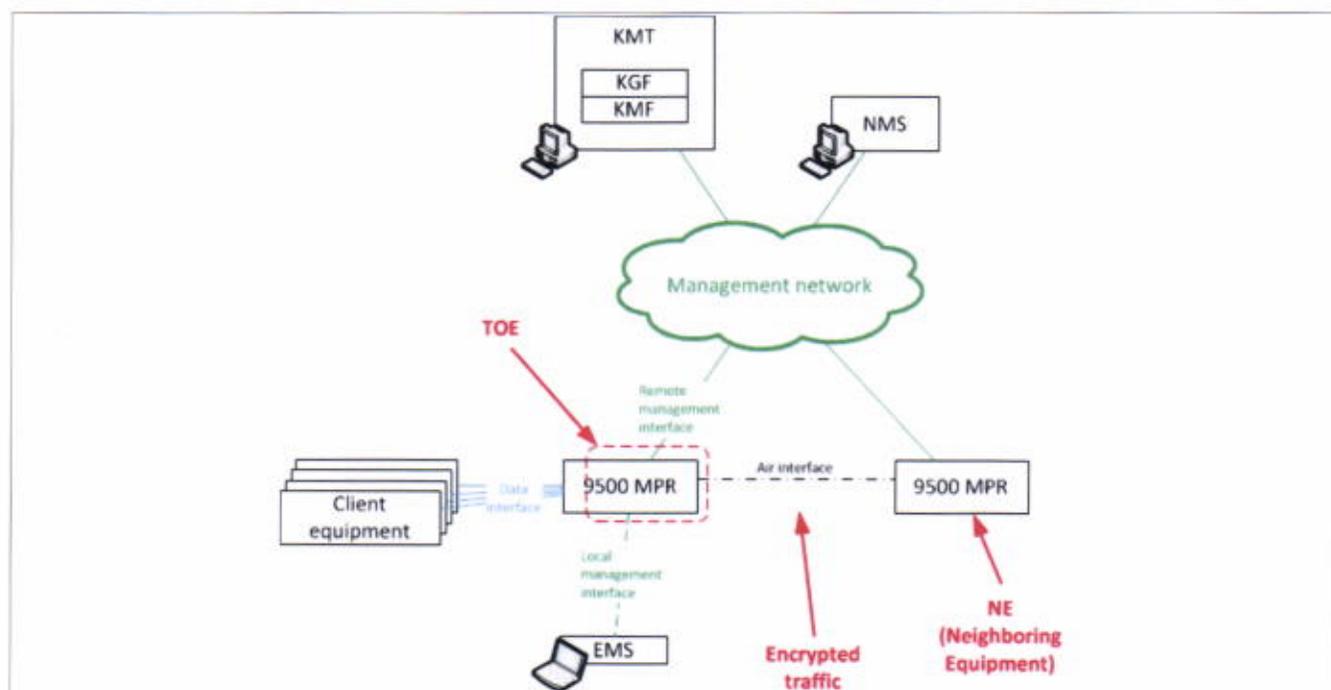


Figure 1. Cas d'usage classique du produit

Présentation générale

Le produit est un multiplexeur pour les faisceaux hertziens numériques, il supporte les technologies PDH¹, SDH² et *ethernet* afin de transformer le multiplexage temporel (TDM³) en « paquets *ethernet* ». Le produit est une plateforme modulaire générique *ethernet* (niveau 2+) adaptée pour la diffusion / réception sécurisée de données par voie hertzienne tels les réseaux 2G, 3G, 4G, HSDPA⁴ et *WiMAX* vers les réseaux *metro ethernet*⁵.

Les principaux services de sécurité fournis par le produit sont :

- le chiffrement des paquets *ethernet* au niveau de la couche 1 ;
- l'identification et l'authentification des utilisateurs ;
- la journalisation des logs ;
- la redondance.

¹ Plesiochronous Digital Hierarchy.

² Synchronous Digital Hierarchy.

³ Time-Division Multiplexing.

⁴ High Speed Downlink Packet Access (3.5G, 3G+, H, turbo 3G) est un protocole de communication pour la téléphonie mobile.

⁵ Réseau de télécommunications à haut débit basé sur le standard Ethernet qui permet de couvrir de larges zones géographiques.

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. L'utilisateur du produit certifié respecte les objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS], et en particulier la localisation du produit dans une zone sécurisée afin de prévenir toute manipulation non autorisée.
- C2. Les guides d'installation [GUIDE_INSTALL], d'administration et utilisateurs [GUIDE_UTIL] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie.
- C3. Le multiplexeur 9500 MPR est paramétré selon le *CERTIFIED SECURE MODE* [GUIDE_INSTALL] de manière à être conforme à la configuration évaluée telle que spécifiée dans [CDS].
- C4. Le réseau d'administration est protégé en intégrité, confidentialité, authentification et anti-rejeu, en outre, les tâches d'administration sont réalisées depuis des postes sécurisés comme précisé dans la cible de sécurité [CDS].
- C5. Les clés générées pour la sécurisation des sessions MPT répondent aux recommandations de l'ANSSI [CRYPTO].
- C6. Les mots de passe respectent les règles préconisées à la page 67 du guide d'installation *CERTIFIED SECURE MODE* [GUIDE_INSTALL].

Limites

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

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
[II 901]	Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles. Disponible sur https://www.legifrance.gouv.fr/ .
[IGI 2100]	Instruction générale interministérielle n° 2100 du 1er décembre 1975 sur l'application en France du système de sécurité de l'Organisation du traité de l'atlantique nord.
[IGI 2102]	Instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation, AMOSSYS <ul style="list-style-type: none"> - référence : OPPIDA/ ETR-LAPLACE-1.01 - version : 1.01 - en date du : 14 septembre 2017
-------	---

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

[CERTIF]	Rapport de certification, référence : ANSSI-CC-2017/57 en date du 5 octobre 2017
[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 . <ul style="list-style-type: none"> - version : 2.03 - en date du : 21 février 2014

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	<i>CERTIFIED SECURE MODE – Software Erase and Reload for radios and μSD manual</i> <ul style="list-style-type: none"> - référence : 3DB 19419SDAATQZZA - version 1 - en date du : 15 avril 2017 <i>Hardware Installation and Replacement Manual</i> <ul style="list-style-type: none"> - référence : 3DB19285ADAATQZZA - version 1 - en date du : 15 avril 2017
-----------------	---

<p>[GUIDE_UTIL]</p>	<p>Guide d'utilisation du produit : <i>CERTIFIED SECURE MODE – User Manuel</i></p> <ul style="list-style-type: none"> - Référence : 3DB19420SDAATQZZA - version 1 - en date du : 19 septembre 2017
<p>[CDS]</p>	<p>Cible de sécurité, <i>NOKIA, 9500 MICROWAVE PACKET RADIO (MPR)</i></p> <ul style="list-style-type: none"> - référence : 3DB19413AAAADTZZA - version : 0.16 - en date du : 19 septembre 2017