CRITÈRES D'ÉVALUATION DE LA CONFORMITÉ AU RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DES PRESTATAIRES DE SERVICES DE CONFIANCE QUALIFIÉS

Annexe à l'arrêté ministériel n° 2020-893
du 18 décembre 2020

ANNEXE AU « JOURNAL DE MONACO » N° 8.519

DU 1ER JANVIER 2021

TABLE DES MATIÈRES

1. Introduction

1.1. Objet

Dans le cadre du Référentiel Général de Sécurité de la Principauté (RGSP), l'Agence Monégasque de Sécurité numérique, désignée comme organe de contrôle, a la charge de contrôler le respect des exigences dudit Référentiel par les prestataires de service de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

La présente annexe décrit les exigences générales relatives à la qualification, selon le Référentiel Général de Sécurité de la Principauté, de l'ensemble des prestataires de services de confiance, indépendamment de la nature des services de confiance qualifiés qu'ils fournissent.

Ces exigences générales, précitées, sont complétées par des exigences spécifiques applicables à chaque type de service de confiance qualifié, publiées par arrêtés ministériels.

1.2. Cadre juridique

Les prestataires de services de confiance qualifiés, respectant les exigences spécifiées au paragraphe 2 de la présente annexe ainsi que les exigences spécifiques à chaque service de confiance qualifié qu'ils fournissent, bénéficient des effets juridiques prévus par loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée.

Ces effets juridiques sont précisés dans les référentiels d'exigences spécifiques applicables à chacun des services de confiance qualifiés.

1.3. Mise à jour

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en fonction des évolutions législatives et règlementaires en matière de sécurité des systèmes d'information.

Ladite mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1.4. Liste des Abréviations

AMSN Agence Monégasque de Sécurité Numérique.

ANSSI Agence nationale de la sécurité des systèmes d'Information française.

CCRA Common Criteria Recognition Agreement.

CESTI Centre d'Evaluation de la Sécurité des Technologies de l'Information.

OID Object Identifier.

PSCo Prestataire de Services de Confiance.

RGSP Règlement Général de Sécurité de la Principauté: arrêté ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative au service de confiance.

SOG-IS Senior Officials Group – Information systems Security.

2. Exigences relatives aux prestataires de services de confiance qualifiés

2.1. Modalités de qualification

2.1.1. Processus de qualification

L'AMSN accorde la qualification à un prestataire de services de confiance sur la base d'un rapport d'évaluation de la conformité élaboré par un organisme d'évaluation de la conformité tels que définit à l'article 8 du Référentiel Général de Sécurité de la Principauté.

Ledit rapport d'évaluation doit permettre de vérifier le respect de l'ensemble des exigences applicables au prestataire de service de confiance telles que spécifiées dans le présent arrêté, ainsi que des exigences applicables aux services de confiance faisant l'objet de la demande de qualification.

Le processus de qualification est décrit dans un document édité par l'ANSSI sous la référence [QUAL_SERV][1].

2.1.2. Durée de validité et maintien de la qualification

La qualification du prestataire de services de confiance est délivrée pour une durée maximale de deux ans, conformément à l'article 14 du Référentiel Général de Sécurité de la Principauté.

Pour permettre un maintien ininterrompu du statut qualifié d'un service de confiance, un rapport d'évaluation de la conformité établi par un organisme répondant aux critères détaillés dans le document édité par l'ANSSI sous la référence [CRITERES_OEC] doit être transmis à l'AMSN trois mois au moins avant l'expiration de la qualification.

[1] Processus de qualification d'un service n°271/ANSSI/SDE du 12 janvier 2017, publié sur les sites ssi.gouv.fr et amsn.gouv.mc

2.1.3. Inscription dans la liste de confiance

L'identification d'un service de confiance qualifié dans la liste de confiance visée à l'article 16 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 doit respecter les exigences techniques définies dans la clause 5.5.3 de la norme ETSI [TS_119_612].

En particulier, il est attendu que la valeur de l'attribut « Organization », figurant dans le certificat électronique identifiant le service de confiance qualifié, corresponde au nom du prestataire de services de confiance qualifié tel qu'indiqué dans le champ « TSP Name » de la liste de confiance.

Les référentiels d'exigences publiés par arrêté ministériel précisent, pour chaque service de confiance qualifié selon le Référentiel Général de Sécurité de la Principauté, les moyens autorisés d'identification du service pour son inscription dans la liste de confiance.

Note : Le périmètre de l'évaluation de la conformité doit être cohérent avec le niveau de précision de l'identifiant retenu pour le service de confiance qualifié dans la liste de confiance qualifié.

L'inscription, dans la liste de confiance, d'un nouvel élément d'identification pour un service déjà qualifié (par exemple, l'ajout d'un nouveau certificat électronique d'unité d'horodatage ou d'autorité de certification, ou d'un nouvel OID de politique de certification) doit faire l'objet d'une demande auprès de l'AMSN suivant les modalités de contact définies dans le document [QUAL_SERV], précité. Il est recommandé de prévoir un délai minimal de trois mois avant mise en service de ces nouveaux éléments, permettant l'instruction de la demande par l'AMSN.

2.2. Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences applicables du Référentiel Général de Sécurité de la Principauté ainsi qu'au textes législatifs et règlementaires en vigueur à l'ensemble des prestataires de services de confiance qualifiés, spécifiées dans les textes ou paragraphes du RGSP suivants :

- La protection et le traitement des informations nominatives est effectué conformément à la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives;

- Limitation de responsabilité : 4ème alinéa de l'article 40 de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée ;

- Accessibilité : article 5 du RGSP ;

- Gestion des risques : 1er et 2ème alinéa de l'article 10 du RGSP ;
- Notification des incidents : 3ème, 4ème, 5ème et 6ème alinéa de l'article 10 du RGSP ;
- 2ème alinéa de l'article 13 du RGSP
  - Information de l'organe de contrôle relative aux modifications des services ;
  - Expertise, fiabilité, expérience et qualification des personnels et sous-traitants ;
  - Maintien de ressources financières suffisantes et/ou assurance responsabilité ;
  - Information des conditions et limites d'utilisation des services ;
  - Utilisation de produits et systèmes fiables ;
  - Utilisation de systèmes fiables pour le stockage des données ;
  - Mesures contre la falsification et le vol des données ;
  - Traitement licite des informations nominatives.

Le respect de la norme européenne ETSI [EN_ 319_401], relative à la signature électronique et des compléments précisés dans le chapitre 2.3 du présent document permet d'apporter une présomption de conformité à ces exigences.

Note : le 2ème alinéa de l'article 13, du RGSP concernant l'utilisation des produits et systèmes fiables, fait également l'objet de précisions dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

La conformité à « l'enregistrement et le maintien de l'accessibilité pour une durée appropriée » ainsi que « l'actualisation d'un plan d'arrêt par service » prévu au 2ème alinéa de l'article 13 du RGSP n'est pas abordé dans le présent document ; elle est traitée dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

2.3. Compléments à la norme européenne ETSI [EN_ 319_401]

2.3.1. Compléments relatifs à la notification des changements apportés aux services fournis

En cas de modification importante dans la fourniture de ses services de confiance qualifiés, le PSCo doit informer l'AMSN, selon les modalités décrites dans le document [QUAL_SERV], précité.

Ces modifications importantes comprennent notamment, sans être exhaustif :

- les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
- les changements de sous-traitants ;
- les modifications des conditions d'hébergement ;
- les changements de matériels cryptographiques ;
- les modifications d'architecture technique ;
- les changements de procédures d'enregistrement et d'identification ;
- les changements dans la gouvernance du PSCo.

Les modifications entrainant des changements dans la liste de confiance publiée par l'AMSN, sur son site, doivent être notifiées sur celui-ci dans les meilleurs délais.

Le PSCo doit adresser à l'AMSN une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés, impactant les constats présentés dans le rapport d'évaluation de la conformité, à une fréquence annuelle.

2.3.2. Compléments relatifs aux systèmes fiables pour le stockage des données

Le PSCo doit utiliser des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière à ce que :

- les informations nominatives ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;
- seules des personnes autorisées puissent introduire et modifier les informations nominatives conservées ;
- l'authenticité de ces informations nominatives puisse être vérifiée.

2.3.3. Compléments au chapitre 5 de la norme [EN_319_401] : « Risk Assessment »

Le PSCo doit effectuer une analyse de risques sur le système d'information utilisé pour mettre en œuvre le service de confiance et procéder à son homologation conformément au guide d'homologation publiée par l'AMSN. Cette homologation doit être réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les 2 ans.

Le périmètre de l'analyse de risques et d'homologation doit notamment inclure le système d'information utilisé par le service de confiance et la protection des informations nominatives.

Le PSCo doit évaluer l'opportunité de mettre à jour l'analyse de risques tous les ans.

Le PSCo doit mettre à jour l'analyse de risques à chaque modification ayant un impact important sur le service de confiance fourni, notamment en cas de modification des politiques ou pratiques relatives à la fourniture du service.

L'analyse de risque et la décision d'homologation doivent être jointes au rapport d'évaluation de la conformité transmis lors de la demande de qualification, selon les modalités précisées dans le document [QUAL_SERV].

2.3.4. Compléments au chapitre 7 de la norme [EN_319_401] : « TSP Management and Operation »

§ 7.2.i : « Human ressources »

Le PSCo doit mettre en œuvre tous les moyens légaux dont il peut disposer pour s'assurer de l'honnêteté de ses personnels. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

À ce titre, le PSCo peut demander à ses personnels la communication d'une copie du bulletin n° 3 de leur casier judiciaire. L'employeur peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Ces vérifications doivent être menées préalablement à l'affectation à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

§ 7.4 : « Access control »

Le PSCo doit appliquer l'ensemble des règles définies dans le guide d'hygiène informatique [GH] édité par l'ANSSI pour le niveau « standard ».

Il est recommandé d'appliquer les mesures au niveau « renforcé ».

§ 7.9 : « Incident management »

Le PSCo doit notifier à l'AMSN dans un délai maximal de 24 heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les informations nominatives qui y sont conservées.

Cette notification est réalisée au moyen du formulaire mis à disposition par l'AMSN, selon les modalités définies dans le document [QUAL_SERV].

2.3.5. Compléments relatifs à la certification des modules cryptographiques

Les fonctions cryptographiques sensibles[2] doivent être mises en œuvre dans des modules cryptographiques répondant aux critères définis dans le tableau ci-dessous[3] :

Labellisation	**Schéma**	**Référentiel**	**Commentaire / modalités**
Certification Critères Communs[4]	ANSSI	Profils de protection reconnus par l'ANSSI, référencés sur le site https://www.ssi.gouv.fr	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[4]	SOG-IS	Profils de protection HSM[5] recommandés sur le site https://sogis.org	Présomption de conformité à l'exigence d'utilisation de produits fiables

[2] Les référentiels d'exigences applicables à chaque type de service de confiance qualifié précisent les fonctions cryptographiques sensibles concernées selon le cas.

[3] Dans le cas particulier des fonctions de signature électronique qualifiée ou de cachet électronique qualifié, le dispositif de création de signature ou de cachet électronique qualifié utilisé doit être certifié conformément à l'article 22 du RGSP.

[4] La certification selon les Critères Communs doit avoir une ancienneté inférieure à 10 ans.

[5] L'AMSN vérifiera que le profil de protection est bien approprié pour le cas d'usage prévu du module crypto graphique au sein de l'environnement du PSCo.

Labellisation	Schéma	Référentiel	Commentaire / modalités
Certification Critères Communs[4]	SOG-IS	Cible de sécurité vérifiée par l'AMSN comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences du règlement.	Présomption de conformité à l'exigence d'utilisation de produits fiables
Certification Critères Communs[4]	CCRA	Cible de sécurité vérifiée par l'AMSN comme étant comparable en terme d'assurance avec les profils de protection reconnus par l'ANSSI et conforme aux exigences du règlement.	L'ANSSI demande à ce que les travaux correspondant aux augmentations non reconnues dans le cadre du CCRA soient réalisés dans un schéma du SOG-IS (avec fourniture du rapport technique d'évaluation au CESTI en charge de l'évaluation et au centre de certification).
Autre	Le demandeur doit fournir un argumentaire visant à démontrer à l'AMSN que sa méthode d'évaluation, le laboratoire utilisé, le référentiel d'évaluation, etc. sont de même niveau qu'une certification Critères Communs réalisées dans le cadre du SOG-IS selon un des profils de protection reconnus par l'ANSSI. Le rapport d'évaluation doit être fourni à l'AMSN pour analyse. L'AMSN se réserve le droit de demander des analyses complémentaires au frais du demandeur dans un laboratoire agréé et reconnu compétent pour ce type de produit au sein du SOG-IS.		

2.3.6. Compléments relatifs aux algorithmes et mécanismes cryptographiques

Les algorithmes et mécanismes cryptographiques mis en œuvre doivent être conformes aux spécifications du document [SOGIS-CRYPTO].

Pour les modules cryptographiques employés par le PSCo, certifiés conformément aux dispositions du chapitre 2.3.5 du présent document, la vérification de la conformité à cette exigence nécessite, dans le cadre de leur certification :

- une analyse théorique des mécanismes cryptographiques mis en œuvre ; et
- une expertise de l'implémentation de ces mécanismes dans le module cryptographique.

2.3.7. Langue des documents publiés par le PSCo

Les documents publiés par le prestataire de services de confiance à destination du public (conditions générales d'utilisation, politiques relatives à la fourniture des services) doivent être rédigés en langue française.

En complément, il est recommandé qu'une version rédigée en langue anglaise de ces documents soit mise à disposition du public.

APPENDICE : RÉFÉRENCES

DOCUMENTAIRES

Renvoi	Document
[CRITERES_OEC]	Organismes d'évaluation de la conformité – Critères de reconnaissance au titre du règlement eIDAS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[RGSP]	Règlement Général de Sécurité de la Principauté : Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative au service de confiance. Disponible sous https://amsn.gouv.mc
[EN_319_401]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
[GH]	Guide d'hygiène informatique. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, version en vigueur. Disponible sur https://amsn.gouv.mc
[QUAL_SERV]	Processus de qualification d'un service, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms - Version en vigueur. Disponible sur https://sogis.org
[TS_119_612]	ETSI TS 119 612 v2.1.1 (2015-07): Electronic Signatures and Infrastructures (ESI); Trusted Lists.

imprimé sur papier recyclé

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO