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

Annexe à l'arrêté ministériel n° 2018-66
du 30 janvier 2018

ANNEXE AU « JOURNAL DE MONACO » N° 8.368

DU 9 FÉVRIER 2018

SOMMAIRE

1 Introduction

1.1 Objet

Conformément à l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée, l'Agence Monégasque de Sécurité Numérique est l'autorité nationale en charge de la sécurité des systèmes d'information.

Elle est, en outre, l'organe de contrôle de la Principauté pour les prestataires de services de confiance et les services de confiance ayant notamment pour mission, de procéder à des contrôles aux fins de vérifier que lesdits prestataires et les services de confiance qualifiés qu'ils fournissent respectent les exigences du Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, de vérifier l'existence des plans d'arrêt des services de confiance qualifiés et leur mise en œuvre effective ainsi que d'établir et tenir à jour la liste de confiance prévue au paragraphe 26 dudit référentiel.

La présente annexe décrit, dans le respect des règles posées par le Référentiel Général de Sécurité précité, les exigences générales relatives à la qualification de l'ensemble des prestataires de services de confiance, indépendamment de la nature des services de confiance qualifiés qu'ils fournissent.

Seul le respect, par les prestataires de service de confiance qualifiés, desdites exigences générales, déclinées au chapitre 2, permet de donner plein effet aux règles posées par le référentiel général de sécurité, précité, pour les services de confiance qualifiés.

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

1.2 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 réglementaires 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.

1.3 Liste des abréviations

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (de l'État français)
PSCo	Prestataire de Services de Confiance
CCRA	Common Criteria Recognition Agreement

CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
OID	Object Identifier
PSCo	Prestataire de Services 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'Agence Monégasque de Sécurité Numérique 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 au paragraphe 18 du Référentiel Général de Sécurité.

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 au service 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 [QUALIF_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 au paragraphe 24 du Référentiel Général de Sécurité.

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'Agence Monégasque de Sécurité Numérique trois mois au moins avant l'expiration de la qualification.

2.1.3 Inscription dans la liste de confiance

L'identification d'un service de confiance qualifié dans la liste de confiance visée au paragraphe 26 du Référentiel Général de Sécurité 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, les moyens autorisés d'identification du service pour son inscription dans la liste de confiance.

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,…) doit faire l'objet d'une demande auprès de l'Agence Monégasque de Sécurité Numérique suivant les modalités de contact définies dans le document [QUALIF_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'Agence Monégasque de Sécurité Numérique.

2.2 Critères d'évaluation de la conformité

L'évaluation doit permettre de démontrer le respect des exigences applicables du Référentiel Général de Sécurité à l'ensemble des prestataires de services de confiance qualifiés, spécifiées dans les paragraphes suivants dudit référentiel :

23(2) j	Protection et traitement des informations nominatives ;
13(2)	Limitation de responsabilités ;
15	Accessibilité ;
20(1)	Gestion des risques ;
20(2)	Notification des incidents ;
23(2) a.	Information de l'organe de contrôle relative aux modifications des services ;
b.	Expertise, fiabilité, expérience et qualification des personnels et sous-traitants ;

[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

c. Maintien de ressources financières suffisantes et/ou assurance responsabilité ;

d. Information des conditions et limites d'utilisation des services ;

e. Utilisation de produits et systèmes fiables ;

f. Utilisation de systèmes fiables pour le stockage des données ;

g. Mesures contre la falsification et le vol des données ;

j. 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.

L'article 23(2).e fait également l'objet de précisions dans les référentiels d'exigences spécifiques applicables à chaque service de confiance.

La conformité aux articles 23(2).h et 28(2).i 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'Agence Monégasque de Sécurité Numérique, selon les modalités décrites dans le document [QUALIF_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 entraînant des changements dans la liste de confiance publiée, sur son site par l'Agence Monégasque de Sécurité Numérique, doivent être notifiées sur celui-ci dans les meilleurs délais.

Le PSCo doit adresser à l'Agence Monégasque de Sécurité Numérique 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 informations nominatives 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 : « 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. 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 [QUALIF_SERV], précité.

2.3.4 Compléments au chapitre 7 : « TSP Management and Operation »

§ 7.2.i : « *Human ressources* »

Le PSCo doit s'assurer que ceux de ses personnels, exerçant des rôles de confiance (officiers de sécurité, administrateurs système, opérateurs, auditeurs), ne font pas l'objet d'une inscription au bulletin n° 3 du casier judiciaire incompatible avec leurs attributions.

§ 7.4 : « *Access control* »

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

Pour le niveau renforcé, l'application des règles suivantes est obligatoire :

- le PSCo élabore et tient à jour un schéma d'architecture précis du système d'information du service de confiance. Ce schéma doit notamment identifier l'ensemble des interconnexions du système d'information du service de confiance ;
- le PSCo interdit la connexion d'équipements personnels au système d'information du service de confiance ;
- le PSCo met en place des réseaux cloisonnés ;
- le PSCo interdit l'accès sans fil au système d'information du service de confiance ;
- le PSCo interdit tout accès à Internet depuis les comptes d'administration ;
- le PSCo dispose d'un réseau d'administration dédié, l'ensemble des opérations d'administration devant être exclusivement réalisées depuis ce réseau ;
- le PSCo n'autorise l'accès à distance au réseau d'entreprise, y compris pour l'administration du réseau, que depuis des postes de l'entreprise qui mettent en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes ;
- le PSCo contacte sans délai l'Agence Monégasque de Sécurité Numérique pour tout incident relatif au service de confiance selon les modalités décrites dans le document [QUALIF_SERV], précité.

§ 7.9 : « *Incident management* »

Le PSCo doit notifier à l'Agence Monégasque de Sécurité Numérique 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 données à caractère personnel qui y sont conservées.

Cette notification est réalisée au moyen du formulaire mis à disposition par l'Agence Monégasque de Sécurité Numérique, selon les modalités définies dans le document [QUALIF_SERV], précité.

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	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	SOG-IS	Profils de protection HSM recommandés sur le site www.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 au paragraphe 32 du Référentiel Général de Sécurité.

Certification Critères Communs	SOG-IS	Cible de sécurité vérifiée par l'ANSSI 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	CCRA	Cible de sécurité vérifiée par l'ANSSI 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'ANSSI 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'ANSSI pour analyse. L'ANSSI 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]	Document de l'ANSSI, Organismes d'évaluation de la conformité – Critères de reconnaissance au titre du règlement eIDAS, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[eIDAS]	Règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE. Disponible sur http://www.europa.eu

[EN_319_401]	Norme européenne 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 édité par l'ANSSI. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	Document de l'ANSSI, L'homologation de sécurité en neuf étapes simples, version en vigueur. Disponible sur https://amsn.gouv.mc
[QUALIF_SERV]	Document de l'ANSSI, 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 http://sogis.org
[TS_119_612]	Standard ETSI TS 119 612 v2.1.1 (2015-07) : Electronic Signatures and Infrastructures (ESI) ; Trusted Lists

imprimé sur papier PEFC

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