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 aux services de confiance

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée ;

Vu la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique ;

Vu l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu 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 aux services de confiance ;

Vu l'arrêté ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié ;

Vu l'arrêté ministériel n° 2017-56 du 1er février 2017 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu l'arrêté ministériel n° 2019-741 du 17 septembre 2019 portant application de l'article 2, a) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée ;

Vu la délibération du Conseil de Gouvernement en date du 24 juin 2019 ;

TABLE DES MATIERES

ARRETONS :

ARTICLE PREMIER.

Les règles applicables par les organismes du secteur public et les personnes physiques ou morales de droit privé visées à l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, susvisée, sont énoncées dans le présent arrêté et ses annexes qui constituent le Référentiel Général de Sécurité de la Principauté.

ART. 2.

Dans un délai de cinq ans à compter de la publication du présent arrêté, les organismes du secteur public mettant en œuvre des services et produits de confiance recourent à l'usage exclusif de produits de sécurité qualifiés et de services de confiance qualifiés ou à défaut, si ces produits ou services qualifiés n'existent pas, ils s'assurent de la conformité des produits de sécurité et des services de confiance qu'ils choisissent au présent référentiel. Dans ce cas, ils attestent formellement de ladite conformité auprès de l'Agence Monégasque de Sécurité Numérique.

Cette disposition ne fait pas obstacle à ce que l'Agence Monégasque de Sécurité Numérique puisse octroyer des dérogations au cas par cas lorsqu'elle le juge nécessaire.

Les règles applicables aux systèmes d'information des organismes du secteur public sont listées en Annexe I.

Les personnes physiques ou morales de droit privé recourent à l'usage de produits de sécurité et de services de confiance conformes au présent arrêté.

ART. 3.
APPLICABILITE DES SERVICES DE CONFIANCE.

Conformément à l'article 14 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, susvisée, les produits et les services de confiance, fournis par un prestataire de services de confiance établi dans un État membre de l'Union Européenne, qui sont conformes à l'annexe au présent arrêté sont autorisés à être utilisés et circuler librement au sein de la Principauté.

ART. 4.
RECONNAISSANCE.

Conformément à l'article 15 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, susvisée, les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans un pays tiers sont reconnus équivalents, sur le plan juridique, à des services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans la Principauté dès lors qu'un accord international a été conclu entre la Principauté et ledit pays.

ART. 5.
ACCESSIBILITE AUX PERSONNES HANDICAPEES.

Dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services, sont accessibles aux personnes handicapées.

ART. 6.
ORGANE DE CONTROLE.

L'Agence Monégasque de Sécurité Numérique constitue, au sens du présent arrêté, l'organe de contrôle, ayant pour missions de procéder à des contrôles, de vérifier l'existence des plans d'arrêt des services de confiance qualifiés et leur mise en œuvre effective et d'établir et tenir à jour la liste de confiance.

Le Directeur de L'Agence Monégasque de Sécurité Numérique a notamment pour mission de vérifier l'accréditation des organismes d'évaluation de la conformité conformément au Référentiel Général de Sécurité de la Principauté, d'accorder, de suspendre ou de retirer le statut qualifié aux prestataires de services de confiance et aux services de confiance.

L'Agence Monégasque de Sécurité Numérique s'assure, par des activités de contrôle a priori et a posteriori, que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences prévues au présent arrêté.

Lorsque l'Agence Monégasque de Sécurité Numérique exige d'un prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues par le présent référentiel et que ce dernier n'agit pas en conséquence dans le délai qu'elle a fixé, le directeur de l'Agence Monégasque de Sécurité Numérique, tenant compte de l'ampleur, de la durée et des conséquences de ce manquement, peut, les intéressés étant dûment entendus, suspendre ou retirer son statut qualifié lui interdisant momentanément ou définitivement la commercialisation de l'ensemble de ses services de confiance qualifiés en Principauté. L'Agence Monégasque de Sécurité Numérique met à jour la liste de confiance en conséquence.

L'Agence Monégasque de Sécurité Numérique prend, si nécessaire, des mesures en ce qui concerne les prestataires de services de confiance non qualifiés, par des activités de contrôle a posteriori, lorsqu'elle est informée que ces prestataires de services de confiance non qualifiés ou les services de confiance qu'il fournissent ne satisferaient pas aux exigences fixées au présent arrêté.

Si un manquement est constaté à la suite d'un contrôle a posteriori sur un prestataire de services de confiance non qualifié, l'Agence Monégasque de Sécurité Numérique impose à ce dernier qu'il corrige le manquement aux exigences prévues par le présent référentiel. Si ce dernier n'agit pas en conséquence dans le délai qu'elle a fixé, le directeur de l'Agence Monégasque de Sécurité Numérique, tenant compte de l'ampleur, de la durée et des conséquences de ce manquement, peut lui interdire momentanément ou définitivement la commercialisation de ses services de confiance en Principauté.

Les contrôles prévus aux troisième, cinquième et sixième alinéas ci-dessus sont effectués pour partie par un organisme d'évaluation de la conformité aux frais du prestataire de services de confiance qualifié ou non qualifié, et pour partie par l'Agence Monégasque de Sécurité Numérique.

ART. 7.
ASSISTANCE MUTUELLE.

En application d'accords internationaux liant la Principauté, l'Agence Monégasque de Sécurité Numérique peut coopérer avec les organes de contrôle d'un autre État en vue d'échanger des bonnes pratiques.

Elle peut fournir, après réception d'une demande justifiée d'un autre organe de contrôle d'un autre État, à cet organe une assistance afin que les activités des organes de contrôle puissent être exécutées de façon cohérente.

L'Agence Monégasque de Sécurité Numérique saisie d'une demande d'assistance peut refuser cette demande sur la base de l'un ou l'autre des motifs suivants :

- elle n'est pas compétente pour fournir l'assistance demandée ;

- l'assistance demandée n'est pas proportionnée à ses activités de contrôle ;
- la fourniture de l'assistance demandée serait incompatible avec le présent arrêté.

ART. 8.
ORGANISMES D'EVALUATION DE LA CONFORMITE.

Des organismes d'évaluation de la conformité sont chargés d'évaluer la conformité aux dispositions du présent référentiel des prestataires de services de confiance qualifiés, ainsi que des services de confiance qualifiés qu'ils fournissent, selon des modalités fixées par arrêté ministériel.

Lesdits organismes d'évaluation sont également chargés d'évaluer la conformité aux dispositions du présent référentiel des prestataires de services de confiance non qualifiés ainsi que des services de confiance qu'ils fournissent, dans le cadre de contrôles a posteriori diligentés par l'organe de contrôle.

L'accréditation des organismes d'évaluation de la conformité est vérifiée, conformément au présent arrêté, par le directeur de l'Agence Monégasque de Sécurité Numérique dans des conditions fixées par arrêté ministériel.

Les organismes d'évaluation de la conformité peuvent être localisés sur le territoire de la Principauté ou sur le territoire d'un État membre de l'Union Européenne.

ART. 9.
PRESTATAIRE DE SERVICES DE CONFIANCE.

Un prestataire de services de confiance est un prestataire conforme à la définition contenue en Annexe VI.

ART. 10.
EXIGENCES DE SECURITE APPLICABLES AUX PRESTATAIRES DE SERVICES DE CONFIANCE.

Conformément aux articles 39 et 39-1 de la loi n° 1.383 du 2 août 2011, modifiée, susvisée, les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent.

Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

Les prestataires de services de confiance qualifiés et non qualifiés notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'Agence Monégasque de Sécurité Numérique et, le cas échéant, à la Commission de Contrôle des Informations Nominatives, 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.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni, le prestataire de services de confiance notifie aussi, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité. Le cas échéant, notamment lorsqu'une atteinte à la sécurité ou une perte d'intégrité concerne un ou des autre(s) État(s) membres de l'Union Européenne, l'Agence Monégasque de Sécurité Numérique peut informer le ou les organe(s) de contrôle de ce(s) État(s) concerné(s).

L'Agence Monégasque de Sécurité Numérique informe le public ou exige du prestataire de services de confiance qu'il le fasse, dès lors qu'il constate qu'il est dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité.

ART. 11.
INFORMATION DES PRESTATAIRES DE SERVICES DE CONFIANCE A LEURS CLIENTS.

Les prestataires de services de confiance qualifiés et non qualifiés doivent élaborer les Conditions Générales d'Utilisation applicables à leurs services de confiance.

Ces Conditions Générales d'Utilisation doivent être mises à disposition de leurs clients avant toute relation contractuelle.

ART. 12.
PRESTATAIRE DE SERVICES DE CONFIANCE QUALIFIE.

Le prestataire de services de confiance qualifié doit respecter un référentiel défini par arrêté ministériel.

Le respect du référentiel visé au précédent alinéa est vérifié, pour partie, par un organisme d'évaluation de la conformité visé à l'article 8, aux frais du prestataire de services de confiance, et pour partie par l'Agence Monégasque de Sécurité Numérique.

Le statut qualifié est accordé à un prestataire de services de confiance par le directeur de l'Agence Monégasque de Sécurité Numérique sur la base du rapport élaboré par l'organisme d'évaluation de la conformité et du résultat de la vérification de conformité effectuée par l'Agence Monégasque de Sécurité Numérique.

Le statut qualifié est accordé à un prestataire de services de confiance pour une durée et selon des modalités de demande définies par arrêté ministériel.

Tout prestataire de services de confiance qualifié doit procéder à la demande de renouvellement de son statut qualifié de sorte à éviter toute rupture dans la validité de son statut. À défaut, il doit mettre en œuvre les plans d'arrêts des services qualifiés qu'il fournit. Un prestataire de services de confiance qualifié qui cesse ses activités doit aussi mettre en œuvre les plans d'arrêts pour ses services qualifiés.

Les prestataires de services de confiance qualifiés sont, dans le respect des dispositions législatives et réglementaires en matière de responsabilité, réputés responsables des dommages causés en raison d'un manquement aux obligations prévues au présent Référentiel Général de Sécurité de la Principauté à toute personne physique ou morale au titre de la fourniture d'un service de confiance qualifié.

ART. 13.
EXIGENCES APPLICABLES AUX PRESTATAIRES DE SERVICES DE CONFIANCE QUALIFIES.

Conformément aux articles 40-3 et suivants de la loi n° 1.383 du 2 août 2011, modifiée, susvisée :

Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, par des moyens appropriés et conformément au droit monégasque, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié.

Les informations visées au premier alinéa sont vérifiées par le prestataire de services de confiance qualifié directement ou en ayant recours à un tiers :

a) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale ; ou

b) au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b) ; ou

c) à l'aide d'autres méthodes d'identification reconnues par la Principauté fournissant une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité visé à l'article 8 ;

d) à distance, à l'aide d'un moyen d'identification électronique répondant au niveau d'exigence élevé conforme aux exigences de la législation monégasque et délivré avant le certificat qualifié.

Un prestataire de services de confiance qualifié qui fournit des services de confiance qualifiés :

- informe l'Agence Monégasque de Sécurité Numérique de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ces activités ;
- emploie, du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, qui ont reçu une formation appropriée en ce qui concerne les règles en matière de sécurité et de protection des données à caractère personnel et appliquent des procédures administratives et de gestion correspondant à des normes européennes ou internationales ;
- en ce qui concerne le risque de responsabilité pour dommages, maintien des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée, conformément au droit monégasque ;
- avant d'établir une relation contractuelle, informe, de manière claire et exhaustive, toute personne désireuse d'utiliser un service de confiance qualifié, des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation ;
- utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge ;
- utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que :
    - les données 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 des données et modifier les données conservées ;
    - l'authenticité des données puisse être vérifiée ;
- prend des mesures appropriées contre la falsification et le vol de données ;
- enregistre et maintient accessibles pour une durée appropriée, y compris après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique ;
- a un plan actualisé d'arrêt par service afin d'assurer la continuité du service conformément aux dispositions vérifiées par l'Agence Monégasque de Sécurité Numérique ;
- assure le traitement licite de données à caractère personnel conformément à la loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

- au cas où le prestataire de services de confiance qualifié délivre des certificats qualifiés, il établit et tient à jour, une base de données relative aux certificats.

Lorsqu'un prestataire de services de confiance qualifié qui délivre des certificats qualifiés décide de révoquer un certificat, il enregistre cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication.

Les prestataires de services de confiance qualifiés qui délivrent des certificats qualifiés fournissent, à toute partie utilisatrice, des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace.

L'Agence Monégasque de Sécurité Numérique détermine les références des normes applicables aux systèmes et produits fiables, qui satisfont aux exigences des quatrième et cinquième tirets du quatrième alinéa ci-dessus. Les systèmes et les produits fiables sont présumés satisfaire aux exigences fixées au présent article lorsqu'ils respectent ces normes. Elles sont publiées par arrêté ministériel.

ART. 14.

CONTROLE DES PRESTATAIRES DE SERVICES DE CONFIANCE QUALIFIES.

Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité visé à l'article 8\. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le Référentiel Général de Sécurité de la Principauté.

Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'Agence Monégasque de Sécurité Numérique dans un délai de trois jours ouvrables qui suivent sa réception.

Sans préjudice des dispositions prévues au premier alinéa, l'Agence Monégasque de Sécurité Numérique peut à tout moment, soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité, visé à l'article 8, de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces prestataires de services de confiance, afin de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent Référentiel Général de Sécurité de la Principauté. L'Agence Monégasque de Sécurité Numérique informe la Commission de Contrôle des Informations Nominatives des résultats de ces audits lorsqu'il apparaît que les règles en matière de protection des informations nominatives ont été violées.

ART. 15.
LANCEMENT D'UN SERVICE DE CONFIANCE QUALIFIE.

Lorsque des prestataires de services de confiance, sans statut qualifié, ont l'intention de commencer à offrir des services de confiance qualifiés, ils soumettent à l'Agence Monégasque de Sécurité Numérique une notification de leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un organisme d'évaluation de la conformité.

L'Agence Monégasque de Sécurité Numérique vérifie que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le Référentiel Général de Sécurité de la Principauté, en particulier les exigences en ce qui concerne les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

Si l'Agence Monégasque de Sécurité Numérique conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier alinéa, le directeur de l'Agence Monégasque de Sécurité Numérique accorde le statut « qualifié » au prestataire de services de confiance et aux services de confiance qu'il fournit et publie sur le site de l'Agence Monégasque de Sécurité Numérique la mise à jour de la liste de confiance, au plus tard trois mois suivant la notification conformément au 1er alinéa.

Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'Agence Monégasque de Sécurité Numérique en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

Les prestataires de services de confiance qualifiés peuvent commencer à fournir le service de confiance qualifié une fois que le statut qualifié est indiqué sur la liste de confiance publiée.

L'Agence Monégasque de Sécurité Numérique définit les formats et les procédures applicables aux fins de l'application du premier et second alinéa. Ils sont publiés par arrêté ministériel.

ART. 16.
LISTE DE CONFIANCE.

L'Agence Monégasque de Sécurité Numérique établit, tient à jour et rend publique la liste de confiance, y compris les informations relatives aux prestataires de services de confiance qualifiés dont il est responsable, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent.

L'Agence Monégasque de Sécurité Numérique établit, tient à jour et publie, de façon sécurisée et sous une forme adaptée au traitement automatisé, la liste de confiance visée au premier alinéa du présent article, portant une signature électronique ou un cachet électronique.

Les informations visées au premier alinéa du présent article sont définies par arrêté ministériel. L'Agence Monégasque de Sécurité Numérique définit les spécifications techniques et les formats de la liste de confiance.

ART. 17.
LABEL DE CONFIANCE DE LA PRINCIPAUTE POUR LES SERVICES DE CONFIANCE QUALIFIES.

Il est créé un label de confiance de la Principauté pour les services de confiance qualifiés délivrés par les prestataires de services de confiance qualifiés. Les spécifications relatives à la forme et notamment à la présentation, à la composition, à la taille et à la conception du label de confiance de la Principauté sont définies par arrêté ministériel.

Une fois que le statut qualifié visé à l'article 15 a été indiqué sur la liste de confiance visée au même Article, les prestataires de services de confiance qualifiés peuvent utiliser le label de confiance de la Principauté pour indiquer d'une manière simple, claire et reconnaissable les services de confiance qualifiés qu'ils fournissent.

Lorsqu'ils utilisent le label de confiance de la Principauté pour les services de confiance qualifiés visé au premier alinéa du présent article, les prestataires de services de confiance qualifiés veillent à ce qu'un lien vers la liste de confiance concernée soit disponible sur leur site Internet.

ART. 18.
EXIGENCES RELATIVES A UNE SIGNATURE ELECTRONIQUE AVANCEE.

Une signature électronique avancée satisfait aux exigences suivantes :

- être liée au signataire de manière univoque ;
- permettre d'identifier le signataire ;
- avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif et ;
- être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Le format et les spécifications d'une signature avancée sont précisés par arrêté ministériel.

ART. 19.
SIGNATURES ELECTRONIQUES DANS LE CADRE DE LA RELATION ENTRE ADMINISTRATION ET ADMINISTRES.

Une signature électronique doit être qualifiée, pour être utilisée dans un téléservice dans le cadre des relations entre les organismes du secteur public et les administrés.

ART. 20.
CERTIFICATS QUALIFIES DE SIGNATURE ELECTRONIQUE.

Les certificats qualifiés de signature électronique satisfont aux exigences fixées à l'Annexe II.

Si un certificat qualifié de signature électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

Si un certificat qualifié de signature électronique a été temporairement suspendu, ce certificat perd sa validité pendant la période de suspension.

La période de suspension est clairement indiquée et le statut de suspension est visible, pendant la période de suspension, sur le site de l'organe de contrôle.

Les normes applicables aux certificats qualifiés de signature électronique sont définies par arrêté ministériel.

Un certificat qualifié de signature électronique est présumé satisfaire aux exigences fixées à l'Annexe II lorsqu'il respecte ces normes.

ART. 21.
EXIGENCES APPLICABLES AUX DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE QUALIFIEE.

Les dispositifs de création de signature électronique qualifiée respectent les exigences fixées à l'Annexe III.

Les normes applicables aux dispositifs de création de signature électronique qualifiée sont définies par arrêté ministériel.

Un dispositif de création de signature électronique qualifiée est présumé satisfaire aux exigences fixées à l'Annexe III lorsqu'il respecte ces normes.

ART. 22.
CERTIFICATION DES DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE QUALIFIEE.

La conformité des dispositifs de création de signature électronique qualifiée avec les exigences fixées à l'Annexe III, est certifiée par le directeur de l'Agence Monégasque de Sécurité Numérique après évaluation par les organismes publics ou privés compétents qu'elle désigne.

L'Agence Monégasque de Sécurité Numérique rend publics le nom et l'adresse du ou des organismes publics ou privés visés au premier alinéa.

La certification visée au premier alinéa est fondée sur un processus d'évaluation de la sécurité mis en œuvre conformément à l'une des normes relatives à l'évaluation de la sécurité des produits informatiques.

L'Agence Monégasque de Sécurité Numérique établit une liste de normes relatives à l'évaluation de la sécurité des produits informatiques visés au troisième alinéa. Elle est publiée par arrêté ministériel.

ART. 23.
PUBLICATION D'UNE LISTE DES DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE QUALIFIEE.

L'Agence Monégasque de Sécurité Numérique publie, dans les meilleurs délais et au plus tard un mois après la conclusion de la certification, des informations sur les dispositifs de création de signature électronique qualifiée qui ont été certifiés.

Elle notifie également dans les meilleurs délais et au plus tard un mois après l'annulation de la certification, des informations sur les dispositifs de création de signature électronique qui ne sont plus certifiés.

ART. 24.
EXIGENCES APPLICABLES A LA VALIDATION DES SIGNATURES ELECTRONIQUES QUALIFIEES.

Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée à condition que :

- le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme à l'Annexe II ;
- le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;
- les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;
- l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice ;
- l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature ;
- la signature électronique ait été créée par un dispositif de création de signature électronique certifié ;
- l'intégrité des données signées n'ait pas été compromise ;

- les exigences prévues à l'article 18 aient été satisfaites au moment de la signature.

Le système utilisé pour valider la signature électronique qualifiée fournit à la partie utilisatrice le résultat correct du processus de validation et permet à celle-ci de détecter tout problème pertinent relatif à la sécurité.

Les normes applicables à la validation des signatures électroniques qualifiées sont définies par arrêté ministériel.

La validation des signatures électroniques qualifiées est présumée satisfaire aux exigences fixées au premier alinéa lorsqu'elle respecte ces normes.

ART. 25.
SERVICE DE VALIDATION QUALIFIE DES SIGNATURES ELECTRONIQUES QUALIFIEES.

Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui :

- fournit une validation en conformité avec le premier alinéa de l'article 24 ; et
- permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

L'Agence Monégasque de Sécurité Numérique détermine les normes applicables au service de validation qualifié visé au premier alinéa du présent article. Elles sont publiées par arrêté ministériel.

Le service de validation de signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au premier alinéa lorsqu'il respecte ces normes.

ART. 26.
SERVICE DE CONSERVATION QUALIFIE DES SIGNATURES ELECTRONIQUES QUALIFIEES.

Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

L'Agence Monégasque de Sécurité Numérique détermine les normes applicables au service de conservation qualifié des signatures électroniques qualifiées. Lesdites normes sont publiées par arrêté ministériel. Le service de conservation qualifié des signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au premier alinéa lorsqu'il respecte ces normes.

ART. 27.
EXIGENCES DU CACHET ELECTRONIQUE AVANCE.

Un cachet électronique avancé satisfait aux exigences suivantes :

- être lié au créateur du cachet de manière univoque ;
- permettre d'identifier le créateur du cachet ;
- avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ; et
- être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.

ART. 28.
CACHETS ELECTRONIQUES DANS LES ORGANISMES DU SECTEUR PUBLIC.

La Principauté exige un cachet électronique avancé qui repose sur un certificat qualifié pour utiliser un service en ligne proposé par les organismes du secteur public, ou pour l'utiliser au nom de cet organisme, elle reconnaît les cachets électroniques avancés qui reposent sur un certificat qualifié et les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes définis par arrêté ministériel.

L'Agence Monégasque de Sécurité Numérique détermine les normes applicables aux cachets électroniques avancés qui reposent sur un certificat qualifié et aux cachets électroniques qualifiés. Elles sont publiées par arrêté ministériel. Un cachet électronique avancé qui repose sur un certificat qualifié est présumé satisfaire aux exigences applicables aux cachets électroniques avancés visées au premier alinéa et à l'article 28, lorsqu'il respecte ces normes.

ART. 29.
CERTIFICATS QUALIFIES DE CACHET ELECTRONIQUE.

Les certificats qualifiés de cachet électronique satisfont aux exigences fixées à l'Annexe IV.

Les certificats qualifiés de cachet électronique ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences fixées à l'Annexe IV.

Si un certificat qualifié de cachet électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

Si un certificat qualifié de cachet électronique a été temporairement suspendu, ce certificat perd sa validité pendant la période de suspension.

La période de suspension est clairement indiquée dans la base de données relative aux certificats et le statut de suspension est visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut du certificat.

L'Agence Monégasque de Sécurité Numérique détermine les normes applicables aux certificats qualifiés de cachet électronique. Elles sont publiées par arrêté ministériel. Un certificat qualifié de cachet électronique est présumé satisfaire aux exigences fixées à l'Annexe IV lorsqu'il respecte ces normes.

ART. 30.
DISPOSITIFS DE CREATION DE CACHET ELECTRONIQUE QUALIFIE.

L'article 21 s'applique, en tant que de besoin, aux exigences applicables aux dispositifs de création de cachet électronique qualifié.

L'article 22 s'applique, en tant que de besoin, à la certification des dispositifs de création de cachet électronique qualifié.

L'article 23 s'applique, en tant que de besoin, à la publication d'une liste de dispositifs de création de cachet électronique qualifié.

ART. 31.
VALIDATION ET CONSERVATION DES CACHETS ELECTRONIQUES QUALIFIES.

L'article 24 et l'article 25 s'appliquent, en tant que de besoin, à la validation et à la conservation des cachets électroniques qualifiés.

ART. 32.
REGLES RELATIVES A L'HORODATAGE ELECTRONIQUE.

Les exigences concernant le composant « contremarque de temps » sont définies par arrêté ministériel. Elles portent sur le contenu des contremarques de temps et sur les conditions dans lesquelles il est émis par un prestataire de services de confiance.

Une fonction d'horodatage permet d'attester qu'une donnée sous forme électronique existe à un instant donné. Cette fonction met en œuvre une contremarque de temps générée à l'aide d'un mécanisme cryptographique respectant les règles et, si possible, les recommandations contenues dans les textes réglementaires.

Cette contremarque, délivrée par un prestataire de services de confiance, doit respecter les exigences définies par un arrêté ministériel qui ne distingue qu'un niveau unique de sécurité, auquel les organismes du secteur public doivent se conformer dès lorsqu'ils souhaitent mettre en œuvre la fonction d'horodatage électronique au sein de leur système d'information.

Un horodatage électronique doit être qualifié, pour être utilisé dans un téléservice dans le cadre des relations entre les organismes du secteur public et les administrés.

ART. 33.
EXIGENCES APPLICABLES AUX HORODATAGES ELECTRONIQUES QUALIFIES.

Un horodatage électronique qualifié satisfait aux exigences suivantes :

- il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ;
- il est fondé sur une horloge exacte liée au temps universel coordonné ; et
- il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.

L'Agence Monégasque de Sécurité Numérique établit les normes en ce qui concerne l'établissement du lien entre la date et l'heure et les données, et les horloges exactes. Elles sont publiées par arrêté ministériel.

L'établissement des liens entre la date et l'heure et les données et les horloges exactes sont présumés satisfaire aux exigences fixées au premier alinéa du présent article lorsqu'ils respectent ces normes.

ART. 34.
EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIES D'AUTHENTIFICATION DE SITE INTERNET.

Les certificats qualifiés d'authentification de site Internet satisfont aux exigences fixées à l'Annexe V.

L'Agence Monégasque de Sécurité Numérique détermine les normes applicables aux certificats qualifiés d'authentification de site Internet. Elles sont publiées par arrêté ministériel.

Un certificat qualifié d'authentification de site Internet est présumé satisfaire aux exigences fixées à l'Annexe V lorsqu'il respecte ces normes.

ART. 35.
RECONNAISSANCE

Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée pour les pratiques administratives monégasques dans le but d'accéder à un service en ligne fourni par les organismes du secteur public le moyen d'identification électronique délivré dans un autre État de l'Union Européenne est reconnu dans la Principauté aux fins de l'authentification transfrontalière pour ce service en ligne, à condition que les conditions suivantes soient remplies :

- la délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique conforme au présent référentiel ;
- le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par les organismes du secteur public concernés pour accéder à ce service en ligne dans la Principauté, à condition que le niveau de garantie de ce moyen d'identification électronique corresponde au niveau de garantie substantiel ou élevé ;
- lesdits organismes du secteur public concernés utilisent le niveau de garantie substantiel ou élevé pour ce qui concerne l'accès à ce service en ligne.

Un moyen d'identification électronique dont la délivrance relève d'un schéma d'identification électronique figurant sur la liste publiée par la Commission européenne en vertu de l'article 9 du Règlement (UE) 910/2014 et qui correspond au niveau de garantie faible peut être reconnu par les organismes du secteur public aux fins de l'authentification transfrontalière du service fourni en ligne par ces organismes.

ART. 36.
NIVEAUX DE GARANTIE DES SCHEMAS D'IDENTIFICATION ELECTRONIQUE.

Un schéma d'identification électronique détermine les spécifications des niveaux de garantie, faible, substantiel et/ou élevé des moyens d'identification électronique délivrés dans le cadre dudit schéma.

Les niveaux de garantie faible, substantiel et élevé satisfont, respectivement, aux critères suivants :

- le niveau de garantie faible renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie substantiel renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie élevé renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Compte tenu des normes internationales pertinentes et sous réserve du deuxième alinéa du présent article, l'Agence Monégasque de Sécurité Numérique fixe les spécifications techniques, normes et procédures minimales sur

la base desquelles les niveaux de garantie faible, substantiel et élevé sont spécifiés pour les moyens d'identification électronique aux fins du premier alinéa. Lesdites spécifications sont publiées par arrêté ministériel.

Les spécifications techniques, normes et procédures minimales sont fixées par référence à la fiabilité et à la qualité des éléments suivants :

- la procédure visant à prouver et vérifier l'identité des personnes physiques ou morales demandant la délivrance de moyens d'identification électronique ;
- la procédure de délivrance des moyens d'identification électronique demandés ;
- le mécanisme d'authentification au moyen duquel la personne physique ou morale utilise le moyen d'identification électronique pour confirmer son identité à une partie utilisatrice ;
- l'entité délivrant les moyens d'identification électronique ;
- tout autre organisme associé à la demande de délivrance de moyens d'identification électronique ; et
- les spécifications techniques et de sécurité des moyens d'identification électronique délivrés.

ART. 37.
ATTEINTE A LA SECURITE.

En cas d'atteinte ou d'altération partielle du schéma d'identification électronique, ou de l'authentification telle qu'elle affecte la fiabilité de l'authentification de ce schéma, l'Agence Monégasque de Sécurité Numérique suspend ou révoque, immédiatement, cette authentification ou les éléments altérés en cause et le rend public.

Lorsqu'il a été remédié à l'atteinte ou à l'altération visée au premier alinéa, l'Agence Monégasque de Sécurité Numérique rétablit l'authentification et le rend public.

S'il n'est pas remédié à l'atteinte ou à l'altération visée au premier alinéa dans un délai de trois mois à compter de la suspension ou de la révocation, l'Agence Monégasque de Sécurité Numérique notifie le retrait, les intéressés étant dument entendus, du schéma d'identification électronique en le rendant public.

ART. 38.
RESPONSABILITE

Conformément au deuxième alinéa de l'article 17 de la loi n° 1.383 du 17 décembre 2019, susvisée, la partie qui délivre le moyen d'identification électronique est responsable, du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent.

La partie qui gère la procédure d'authentification est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale pour ne pas avoir assuré la gestion correcte de l'authentification.

ART. 39.
COOPERATION ET INTEROPERABILITE.

Les schémas d'identification électronique des organismes du secteur public peuvent être interopérables avec les schémas définis par l'Union Européenne.

Le cadre d'interopérabilité satisfait aux critères suivants :

- il vise à être neutre du point de vue technologique et n'opère pas de discrimination entre l'une ou l'autre des solutions techniques particulières destinées à l'identification électronique ;
- il suit les normes européennes et internationales, dans la mesure du possible ;
- il facilite la mise en œuvre du principe du respect de la vie privée dès la conception ; et
- il garantit que les informations nominatives sont traitées conformément à la législation et réglementation en vigueur en matière de protection des données personnelles.

L'Agence Monégasque de Sécurité Numérique fixe les modalités de procédure nécessaires pour faciliter la coopération entre la Principauté et les États membres de l'Union Européenne, en vue de favoriser un niveau de confiance et de sécurité approprié au degré de risque.

ART. 40.

L'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, est abrogé.

ART. 41.

Dans les Ordonnances Souveraines, les arrêtés ministériels et règlements actuellement en vigueur, les termes : « arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée » sont remplacés par les termes : « 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 aux services de confiance ».

ART. 42.

Le Secrétaire Général du Gouvernement et le Directeur de l'Agence Monégasque de Sécurité Numérique sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le six juillet deux mille vingt.

Le Ministre d'État,

S. TELLE.

RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ DE LA PRINCIPAUTÉ DE MONACO (RGSP)

Règles applicables aux systèmes d'information aux services de confiance pour les transactions électroniques

Annexes à l'arrêté ministériel n° 2020-461 du 6 juillet 2020

TABLE DES MATIERES

ANNEXE I
RÈGLES APPLICABLES AUX SYSTÈMES D'INFORMATION

Paragraphe 1
Les règles de base - Principes.

Afin de mettre leur système d'information en conformité avec le présent Référentiel Général de Sécurité, les organismes du secteur public doivent adopter une démarche en cinq (5) étapes :

1. réalisation d'une analyse des risques ;
2. définition des objectifs de sécurité ;
3. choix et mise en œuvre des mesures appropriées de protection et de défense du système d'information ;
4. homologation de sécurité du système d'information ;
5. suivi opérationnel de la sécurité du système d'information.

Dans l'éventualité où le système d'information serait déjà en service sans avoir fait l'objet de cette démarche, ou bien a été modifié, la procédure simplifiée suivante peut être mise en œuvre :

1. réalisation d'un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire qualifié par l'Agence Monégasque de Sécurité Numérique ;
2. réalisation d'une analyse des risques simplifiée ;
3. mise en œuvre des mesures correctives fixées dans le rapport d'audit ;
4. décision d'homologation de sécurité du système d'information ;
5. suivi opérationnel de la sécurité du système d'information.

Au-delà des mesures techniques et organisationnelles, lesdits organismes doivent veiller :

- aux clauses relatives à la sécurité dans les contrats qu'elles passent avec des prestataires chargés de les assister dans leur démarche de sécurisation et de mise en œuvre de leurs systèmes. Ces services peuvent être de nature intellectuelle (audit de la sécurité du système d'information, traitement d'incident de sécurité, notamment) ou technique (mécanisme de détection, externalisation, infogérance, hébergement et stockage de tout ou partie du système d'information, tierce maintenance applicative, etc.) ;
- au facteur humain : la sensibilisation du personnel aux questions de sécurité est primordiale, ainsi que la formation de ceux qui interviennent plus spécifiquement dans la mise en œuvre et le suivi opérationnel de la sécurité du système d'information (surveillance, détection, prévention).

Les personnes physiques ou morales de droit privé peuvent s'appuyer sur la même démarche aux fins de sécuriser leur système d'information.

D'une manière générale, il est recommandé de s'appuyer sur les guides et sur les documents produits par l'Agence Monégasque de Sécurité Numérique.

Paragraphe 2
Les règles de base - Description des étapes.

1. Analyse de risques.

L'analyse de risques précise les besoins de sécurité du système d'information en fonction de la menace et des enjeux.

La démarche d'analyse de risques consiste à identifier les évènements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels puis de décider des actions à réaliser pour chacun des risques identifiés (éviter, réduire, transférer, accepter) afin de réduire le risque global à un niveau acceptable.

Les menaces[1] à prendre en compte sont celles qui pèsent réellement sur le système et sur les informations qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe.

Lorsque le système d'information intègre des certificats électroniques ou de l'horodatage électronique, l'analyse des risques doit permettre de décider des niveaux des services de confiance utilisés (signature, authentification, confidentialité, etc.) :

- simple ; à ce niveau, l'objectif est simplement de réduire le risque d'utilisation abusive ou d'altération d'identité ;
- avancé ; à ce niveau, l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération d'identité ;
- qualifié ; à ce niveau, l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité qui sera mise en œuvre.

Il est recommandé de s'appuyer sur la norme ISO 27005, qui fixe un cadre théorique de la gestion des risques. Sa mise en œuvre pratique peut être facilitée par les explications et les outils, notamment logiciels, proposés par la méthode « Expression des Besoins et Identification des Objectifs de Sécurité » (EBIOS) ou toutes autres.

2. Définition des objectifs de sécurité.

Une fois les risques appréciés, les organismes du secteur public ou les personnes physiques ou morales de droit privé doivent énoncer les objectifs de sécurité à satisfaire.

Aux trois grands domaines traditionnels (disponibilité et intégrité des données et du système, confidentialité des données et des éléments critiques du système) peuvent s'ajouter deux domaines complémentaires :

- l'authentification, afin de garantir que la personne identifiée est effectivement celle qu'elle prétend être ;
- la traçabilité, afin de pouvoir associer les actions sur les données et les processus aux personnes effectivement connectées au système et ainsi permettre de déceler toute action ou tentative d'action illégitime.

Les objectifs de sécurité doivent être exprimés aussi bien en termes de protection que de défense des systèmes d'information. Lesdites personnes doivent formuler précisément ces objectifs de sécurité.

[1] Une menace est considérée par la norme « ISO/CEI Guide 73 : 2002 » comme une « cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système et d'un organisme ».

3. Choix et mise en œuvre des mesures de sécurité adaptées.

L'expression des objectifs de sécurité permet d'apprécier les fonctions de sécurité qui peuvent être mises en œuvre pour les atteindre. Ces fonctions de sécurité sont matérialisées par le choix de moyens et de mesures de nature :

- technique : produits de sécurité (matériels ou logiciels), prestations de services de confiance informatiques ou autres dispositifs de sécurité (blindage, détecteur d'intrusion, ...) ;
- organisationnelle : organisation des responsabilités (habilitation du personnel, contrôle des accès, protection physique des éléments sensibles), gestion des ressources humaines (affectation d'agents responsables de la gestion du système d'information, formation du personnel spécialisé, sensibilisation des utilisateurs).

Ces mesures de sécurité peuvent être sélectionnées au sein des référentiels et normes existants. Elles peuvent également en être adaptées ou bien être créées *ex nihilo*.

4. Homologation de sécurité du système d'information.

Les systèmes d'information qui entrent dans le champ du présent texte réglementaire doivent faire l'objet, avant leur mise en service opérationnelle, d'une décision d'homologation de sécurité.

Elle est prononcée par l'autorité administrative compétente pour les services de l'État ou par les responsables des entités privées.

La décision d'homologation atteste que le système d'information est protégé conformément aux objectifs de sécurité fixés et que les risques résiduels sont acceptés. La décision d'homologation s'appuie sur un dossier d'homologation. Lorsqu'elle concerne un téléservice, cette décision est rendue accessible aux usagers.

Il est recommandé que les systèmes d'information homologués fassent l'objet d'une revue périodique.

Les recommandations rendues publiques par l'Agence Monégasque de Sécurité Numérique pourront être utilisées afin d'homologuer les systèmes d'information.

5. Suivi opérationnel de la sécurité du système d'information.

Les mesures de protection d'un système d'information doivent être accompagnées d'un suivi opérationnel quotidien ainsi que de mesures de surveillance et de détection, afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux.

Le suivi opérationnel consiste à collecter et à analyser les journaux d'évènements et les alarmes, à mener des audits réguliers, à appliquer des mesures correctives après un audit ou un incident, à mettre en œuvre une chaîne d'alerte en cas d'intrusion supposée ou avérée sur le système, à gérer les droits d'accès des utilisateurs, à assurer une veille sur les menaces et les vulnérabilités, à entretenir des plans de continuité et de reprise d'activité, à sensibiliser le personnel et à gérer les crises lorsqu'elles surviennent.

Paragraphe 3
Les règles de base - Règles relatives à la cryptologie et à la protection des échanges électroniques.

Les règles techniques énoncées par le présent Référentiel portent sur la sécurisation des infrastructures utilisées pour procéder aux échanges électroniques avec les organismes du secteur public ainsi qu'avec les personnes physiques ou morales de droit privé mais également pour les personnes privées pour les échanges entres elles ou avec leurs clients.

Le Référentiel Général de Sécurité de la Principauté n'impose aucune technologie particulière et laisse auxdits organismes et personnes le choix des mesures à mettre en œuvre. Il fixe cependant des exigences relatives à certaines fonctions de sécurité, notamment la certification, l'horodatage et l'audit.

En fonction de leur besoin de sécurité, issu de l'analyse de risques, il appartient auxdits organismes et personnes de déterminer les fonctions de sécurité ainsi que les niveaux de sécurité associés, en s'appuyant sur les méthodes, les outils et les bonnes pratiques en vigueur.

Lorsqu'ils choisissent de mettre en œuvre des fonctions de sécurité traitées dans le présent référentiel, lesdits organismes et personnes choisissent le niveau de sécurité adapté à leur besoin et appliquent les règles correspondantes. Dans tous les cas, l'usage de produits qualifiés par l'Agence Monégasque de Sécurité Numérique, quand ils existent, s'impose.

1. Règles relatives à la cryptologie.

Lorsqu'ils mettent en place des mesures de sécurité comprenant des mécanismes cryptographiques, les organismes du secteur public et les personnes physiques ou morales de droit privé, doivent respecter les règles publiées par textes réglementaires communs à tous les mécanismes cryptographiques, ainsi que ceux dédiés aux mécanismes d'authentification.

2. Règles relatives à la protection des échanges électroniques.

Les règles de sécurité à respecter pour les fonctions de sécurité d'authentification et de signature électronique reposent sur l'emploi de certificats électroniques.

Les règles de sécurité à respecter pour la fonction de confidentialité peuvent reposer sur des certificats électroniques.

3. Règles relatives aux certificats électroniques.

Les exigences concernant le composant « certificat électronique » sont définies par arrêté ministériel. Elles portent sur le contenu des certificats et sur les conditions dans lesquelles il est émis par un Prestataire de Services de Confiance (PSCO), ainsi que sur le dispositif de stockage des clés.

a. L'authentification d'une entité par certificat électronique.

L'authentification[2] a pour but de vérifier l'identité dont se réclame une personne ou une machine. La mise en œuvre par les organismes publics ou par les personnes physiques ou morales de droit privé des fonctions de sécurité « Authentification » ou « Authentification serveur » peut se faire selon trois (3) niveaux de sécurité aux exigences croissantes : Faible, Substantiel, Élevé.

b. La signature et le cachet électroniques.

La signature électronique d'une personne permet de garantir l'identité du signataire, l'intégrité du document signé et le lien entre le document signé et la signature. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées.

[2] S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification.

Dans le cas des échanges dématérialisés faisant intervenir des services applicatifs, la fonction de « cachet » permet de garantir l'origine et l'intégrité des informations échangées et l'identification du service ayant « cacheté » ces informations.

La mise en œuvre par des organismes du secteur public ou par des personnes physiques ou morales de droit privé des fonctions de sécurité « Signature électronique » ou « cachet » peut se faire selon trois (3) niveaux de sécurité aux exigences croissantes : Simple, Avancé, Qualifié. Ces exigences, décrites par arrêté ministériel, couvrent, pour les trois (3) niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la bi-clé et le certificat électronique dont l'usage est la signature électronique ou le cachet ;
- le dispositif de création de signature électronique ou de cachet ;
- l'application de création de signature électronique ou de cachet ;
- le module de vérification de signature électronique ou de cachet.

Cas particulier de la signature des actes administratifs :

Les organismes du secteur public doivent respecter les exigences du présent Référentiel Général de Sécurité de la Principauté lorsqu'ils mettent en œuvre, pour la signature de leurs actes administratifs, des systèmes d'information utilisant des fonctions de sécurité décrites dans le présent Référentiel (certificats électroniques, audit, etc.).

c. La confidentialité.

Le chiffrement constitue le mécanisme essentiel de protection de la confidentialité. Cependant, la confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun (en lecture, en écriture ou en modification) aux données contenues dans le système d'information. À cet effet, il est recommandé de mettre en place des mécanismes techniques afin de s'assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d'en connaître. Ces mécanismes doivent être robustes et implémentés au plus près du lieu de stockage des données.

La mise en œuvre par des organismes du secteur public ou par des personnes physiques ou morales de droit privé de la fonction de sécurité « Confidentialité » peut se faire selon trois (3) niveaux de sécurité aux exigences croissantes : Faible, Substantiel et Élevé.

Ces exigences, dont les modalités sont définies par arrêté ministériel couvrent, pour les trois (3) niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- la bi-clé et le certificat électronique dont l'usage est le chiffrement ;
- le dispositif de chiffrement ;
- le module de chiffrement ;
- le module de déchiffrement.

Paragraphe 4
Les règles de base - Règles relatives aux accusés d'enregistrement et aux accusés de réception.

Conformément à l'article 51 de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, les accusés d'enregistrement et les accusés de réception sont émis, dans le cadre des téléservices mis en place par les organismes du secteur public, selon un procédé conforme au présent Référentiel. Ces accusés ne constituent pas en eux-mêmes des fonctions de sécurité. En revanche, ils peuvent s'appuyer sur des fonctions de sécurité telles que la signature, le cachet et l'horodatage.

Les accusés d'enregistrement et de réception sont générés et émis par les organismes du secteur public à destination des administrés.

Lesdits organismes doivent déterminer les fonctions de sécurité nécessaires à la protection des accusés précités ainsi que leur niveau de sécurité.

Dans le cas général, il est recommandé que lesdits accusés d'enregistrement et de réception :

- soient horodatés avec des contremarques de temps conformes aux exigences prévues par arrêté ministériel en ce qui concerne le niveau de sécurité unique prévu par ce document ;
- soient signés par un agent de l'organisme du secteur public (ou cachetés par une machine dudit organisme) conformément aux exigences définies par arrêté ministériel ;
- utilisent des mécanismes cryptographiques définis par arrêté ministériel.

S'agissant de la gestion des accusés, la sauvegarde des accusés d'enregistrement et de réception doit être assurée dans tous les cas, tant que peuvent survenir d'éventuelles réclamations de la part des usagers.

Paragraphe 5
Les règles de base - Qualification des produits de sécurité.

La qualification de produits de sécurité prévoit trois (3) niveaux de qualification :

- qualification élémentaire également appelée Certification de Sécurité de Premier Niveau (CSPN) ;
- qualification standard ;
- qualification renforcée.

Un produit de sécurité est qualifié s'il a fait l'objet d'une attestation de qualification et d'un maintien de conditions de sécurité conforme aux procédures décrites par textes réglementaires.

L'Agence Monégasque de Sécurité Numérique instruit les demandes et délivre les attestations de qualification. La procédure de qualification repose, en vertu du programme de coopération avec l'Agence Nationale de Sécurité des Systèmes d'Information française (ANSSI), sur une certification préalable par celle-ci.

Le catalogue des produits de sécurité qualifiés est publié sur le site de l'Agence Monégasque de Sécurité Numérique https://amsn.gouv.mc/Produits-qualifies/.

Paragraphe 6
Les règles de base - Organiser la Sécurité des Systèmes d'Information.

1. Organiser les responsabilités liées à la sécurité des systèmes d'information.

Les organismes publics et privés doivent mettre en œuvre une organisation responsable de la Sécurité des Systèmes d'Information.

Cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter. Elle est chargée du pilotage, de la gestion et du suivi des moyens de Sécurité des Systèmes d'Information. Elle est constituée notamment du Responsable de la Sécurité des Systèmes d'Information (RSSI) et du responsable informatique.

L'organisation mise en place doit assurer les missions suivantes :

- coordination des actions permettant l'intégration des clauses liées à la Sécurité des Systèmes d'Information dans les contrats ou les conventions impliquant un accès par des tiers à des informations ou à des ressources informatiques ;
- formalisation de la répartition des responsabilités liées à la Sécurité des Système d'Information (définition des périmètres de responsabilité, des délégations de compétences, etc.) ;
- établissement des relations nécessaires avec l'Agence Monégasque de Sécurité Numérique, notamment pour la gestion des intrusions et des attaques sur les systèmes.

2. Mettre en place un système de management de la sécurité des systèmes d'information.

Il est recommandé de mettre en œuvre des processus permettant de rechercher une amélioration constante de la Sécurité des Systèmes d'Information. Par exemple, la mise en place d'un système de management de la sécurité de l'information, tel que défini dans la norme ISO 27001, permet non seulement de planifier et de mettre en œuvre les mesures de protection du système d'information, mais également d'en vérifier la pertinence et la conformité par rapport aux objectifs établis.

3. Appliquer la politique de sécurité des systèmes d'information.

La Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E) est applicable dans tous les organismes du secteur public. Les personnes physiques ou morales de droit privé doivent mettre en place une politique de sécurité des systèmes d'information adaptée à leurs besoins.

4. Impliquer les instances décisionnelles.

Les autorités hiérarchiques des organismes du secteur public ou lorsqu'il y a lieu, les instances décisionnelles des personnes physiques ou morales de droit privé doivent être impliquées dans la sécurisation des systèmes d'information dont elles ont, in fine, la responsabilité, afin de donner les orientations adéquates, notamment en termes d'investissement humain et financier, et de valider les objectifs de sécurité et les orientations stratégiques. La norme ISO 27001 fournit, à titre indicatif, une liste de sujets susceptibles d'être traités au niveau de la direction d'un organisme.

5. Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la Sécurité des Systèmes d'Information dans les projets.

La Sécurité d'un Système d'Information doit être adaptée aux enjeux du système lui-même et aux besoins de sécurité desdits organismes et personnes, afin d'y consacrer les moyens financiers et humains nécessaires et suffisants. Dans ce but, il est recommandé d'utiliser les guides élaborés par l'Agence Monégasque de Sécurité Numérique. Ils permettent, dans le cadre du développement d'un projet de système d'information, de déterminer les enjeux relatifs à la sécurité et d'identifier l'ensemble des livrables relatifs à la Sécurité des Systèmes d'Information.

6. Adopter une démarche globale.

L'ensemble de la démarche de sécurisation des systèmes d'information doit procéder d'une volonté cohérente et globale, afin d'éviter la dispersion des efforts des équipes en charge de la Sécurité des Systèmes d'Information ou la mise en œuvre de mesures de sécurité parcellaires.

Chaque décision doit être prise au juste niveau hiérarchique. Il est ainsi recommandé :

- de prendre en considération tous les aspects qui peuvent affecter la Sécurité des Systèmes d'Information, qu'ils soient techniques (matériels, logiciels, réseaux) ou non (organisations, infrastructure, personnel) ;
- d'envisager tous les risques et menaces, quelle que soit leur origine ;
- de prendre en compte la Sécurité des Systèmes d'Information à tous les niveaux hiérarchiques. La Sécurité des Systèmes d'Information repose sur une vision stratégique et nécessite des choix d'autorité (enjeux, moyens humains et financiers, risques résiduels acceptés) ainsi qu'un contrôle des actions et de leur légitimité ;
- de responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage et d'œuvre, utilisateurs) ;
- d'intégrer la Sécurité des Systèmes d'Information tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

D'une manière similaire, la sécurité doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, afin de :

- limiter les surcoûts inhérents à l'application tardive de mesures de sécurité ;
- garantir l'efficacité des mesures mises en œuvre ;
- favoriser l'appropriation de la sécurité par les équipes en charge du système d'information.

7. Informer et sensibiliser le personnel.

L'ensemble des utilisateurs des organismes du secteur public et des services proposés par des personnes physiques ou morales de droit privé et le cas échéant les contractants et les utilisateurs tiers, doivent suivre une formation adaptée sur la sensibilisation et recevoir régulièrement les mises à jour des politiques et des procédures qui concernent leurs missions. Cette formation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation du personnel doit être régulière.

8. Prendre en compte la sécurité dans les contrats et les achats sur le modèle des guides publiés sur le site de l'Agence Monégasque de Sécurité Numérique (https://amsn.gouv.mc/Informations-pratiques/Guidespratiques/).

Les exigences de sécurité relatives aux produits ou aux prestations acquis doivent faire l'objet d'une étude et doivent être clairement formalisées et intégrées dans les dossiers d'appels d'offres, au même titre que les exigences fonctionnelles, réglementaires, de performance ou de qualité.

Ces exigences peuvent concerner le système qui fait l'objet de la consultation, mais aussi la gestion du projet lui-même (formation ou habilitation des personnels), en incluant les phases opérationnelles et de maintenance.

Il convient notamment de :

- veiller à intégrer aux règlements de consultation ou aux cahiers des charges, les référentiels élaborés par l'Agence Monégasque de Sécurité Numérique applicables (produits qualifiés, …) ;
- demander à ce que les produits de sécurité soient fournis avec l'ensemble des éléments permettant d'en apprécier le niveau de sécurité ;
- préciser les clauses relatives à la maintenance des produits acquis ;
- préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants ;
- préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- préciser les conditions de propriété des codes sources ;
- prévoir, le cas échéant, la réversibilité des prestations et la portabilité des données générées en s'assurant en particulier que les bases de données sont extractibles, que celles-ci peuvent être distinguées du système lui-même et que les formats utilisés sont ouverts ;
- préciser la nature et les modalités de réalisation des tableaux de bord et mécanismes de suivi des prestations de sécurité ;
- prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- prévoir des points de contact compétents à même de répondre aux besoins urgents ;
- vérifier, dans les réponses à appel d'offres, la couverture des exigences sécurité inscrites dans la consultation.

Une attention particulière devra être portée aux mécanismes de validation et de recette des composants mettant en œuvre les exigences de sécurité

9. Prendre en compte la sécurité dans les projets d'externalisation, d'hébergement et d'informatique en nuage.

Le recours à l'externalisation ou à l'hébergement ou le stockage à distance présente des risques spécifiques qu'il convient d'évaluer avant d'aborder une telle démarche. Ces risques peuvent être liés au contexte même de l'opération d'externalisation ou à des spécifications contractuelles déficientes ou incomplètes.

Dans cette hypothèse, il est recommandé d'appliquer les prescriptions décrites dans le guide de l'Agence Monégasque de Sécurité Numérique « Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information ». Ce guide fournit :

- une démarche cohérente de prise en compte des aspects Sécurité des Systèmes d'Information lors de la rédaction du cahier des charges d'une opération d'externalisation ;
- un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et à personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

10. Mettre en place des mécanismes de défense des systèmes d'information.

En complément des mécanismes de protection des systèmes d'information, et en fonction de leurs enjeux de sécurité les organismes du secteur public et les personnes physiques ou morales de droit privé publics doivent adopter des mesures complémentaires relatives à la défense des systèmes d'information. Ces mesures consistent, en particulier, à assurer :

- la connaissance des systèmes exploités par le service, ou en relation avec lui (cartographie des systèmes d'information, répertoire des interconnexions, etc.) ;
- la détection des malveillances, des erreurs et des imprudences, en périphérie ou à l'intérieur des systèmes d'informations desdits organismes ;
- la traçabilité des actions et des accès réalisés sur les systèmes d'information (journalisation, notamment) ;
- la pérennisation des savoir-faire et des compétences, notamment en termes d'exploitation des systèmes d'information ;
- la conservation de la preuve des infractions découvertes.

11. Utiliser des produits de sécurité et des prestataires de services de confiance qualifiés.

La qualification permet d'attester de la confiance que l'on peut accorder, notamment, à des produits de sécurité et à des Prestataires de Services de Confiance (PSCO), ainsi que de leur conformité aux règles du Référentiel Général de Sécurité de la Principauté qui leurs sont applicables. D'autres qualifications existent pour attester de la compétence des professionnels, notamment en matière de Sécurité des Systèmes d'Information.

Le recours à des produits de sécurité ou à des prestataires de services de confiance est une nécessité.

Ainsi, il est recommandé :

- d'utiliser, chaque fois qu'ils existent, des produits de sécurité qualifiés par l'Agence Monégasque de Sécurité Numérique ;
- de recourir chaque fois que possible à des prestataires de services de confiance qualifiés ;
- de prendre en considération, pour le choix des prestataires, en plus de leur qualification, leur éventuelle certification selon la norme ISO 27001 ou d'autres normes équivalentes ;
- de prendre en considération, pour le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

12. Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité.

Les services des organismes du secteur public ou les personnes physiques ou morales de droit privé doivent se préparer à faire face à des incidents de sécurité pour lesquels toutes les mesures préventives auraient échoué. À ce titre, ils doivent mettre en œuvre un plan de continuité d'activité pour continuer le travail et un plan de reprise d'activité qui identifient les moyens et les procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas d'incident grave. Ces documents doivent être régulièrement mis à jour. Les plans et les procédures qui en découlent doivent faire l'objet de tests réguliers.

13. Procéder à des audits réguliers de la sécurité du système d'information.

Les organismes du secteur public ou les personnes physiques ou morales de droit privé doivent réaliser ou faire réaliser des audits réguliers de leurs systèmes d'information.

À cet effet, le référentiel d'exigences relatif aux Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI) publié par l'arrêté ministériel n° 2017-625 du 16 août 2017 fixe les règles que doivent respecter les prestataires tiers qui réalisent des audits de la Sécurité des Systèmes d'Information des organismes du secteur public ou des personnes physiques ou morales de droit privé.

Ledit arrêté ministériel définit également des recommandations à l'intention des commanditaires d'audits, dans le cadre de la passation de marchés publics ou d'un accord contractuel, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

Afin de s’assurer qu’ils recourent à des prestataires qui respectent ces exigences, les organismes du secteur public ou les personnes physiques ou morales de droit privé doivent, autant que possible, faire appel à des prestataires ayant obtenu une qualification PASSI.

14. Réaliser une veille sur les menaces et les vulnérabilités.

Les organismes du secteur public ou les personnes physiques ou morales de droit privé doivent se tenir informés sur l’évolution des menaces et des vulnérabilités, en identifiant les incidents qu’elles favorisent ainsi que leurs impacts potentiels. Les sites institutionnels, comme celui de l’Agence Monégasque de Sécurité Numérique, CERT-MC, ou ceux des éditeurs de logiciels et de matériels constituent des sources d’information essentielles sur les vulnérabilités identifiées, ainsi que sur les contre-mesures et les correctifs éventuels. Les mises à jour des logiciels et d’autres équipements, les correctifs des systèmes d’exploitation et des applications font l’objet d’alertes et d’avis qu’il est indispensable de suivre.

ANNEXE II
EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS DE SIGNATURE ÉLECTRONIQUE.

Les certificats qualifiés de signature électronique contiennent :

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature électronique ;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi, et :
   - pour une personne morale : le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;
   - pour une personne physique : le nom de la personne ;

c) au moins le nom du signataire ou un pseudonyme ; si un pseudonyme est utilisé, cela est clairement indiqué ;

d) des données de validation de la signature électronique qui correspondent aux données de création de la signature électronique ;

e) des précisions sur le début et la fin de la période de validité du certificat ;

f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;

h) l'endroit où peut être obtenu gratuitement le certificat sur lequel repose la signature électronique avancée ou le cachet électronique avancé mentionnés au point g) ;

i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;

j) lorsque les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif qualifié de création de signature électronique, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

ANNEXE III
EXIGENCES APPLICABLES AUX DISPOSITIFS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE QUALIFIÉE.

1. Les dispositifs de création de signature électronique qualifiée garantissent au moins, par des moyens techniques et des procédures appropriés, que :

a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;

b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;

c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;

d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs de création de signature électronique qualifiée ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

3. La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.

4. Sans préjudice du point d) du chiffre 1, un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :

a) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;

b) le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

ANNEXE IV
EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS DE CACHET ÉLECTRONIQUE.

Les certificats qualifiés de cachet électronique contiennent :

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de cachet électronique ;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et :
   - pour une personne morale : le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;
   - pour une personne physique : le nom de la personne ;

c) au moins le nom du créateur du cachet et, le cas échéant, son numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;

d) des données de validation du cachet électronique, qui correspondent aux données de création du cachet électronique ;

e) des précisions sur le début et la fin de la période de validité du certificat ;

f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;

h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g) ;

i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;

j) lorsque les données de création du cachet électronique associées aux données de validation du cachet électronique se trouvent dans un dispositif qualifié de création de cachet électronique, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

ANNEXE V
EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS D'AUTHENTIFICATION DE SITE INTERNET.

Les certificats qualifiés d'authentification de site internet contiennent :

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de site internet ;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et :
   - pour une personne morale : le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;
   - pour une personne physique : le nom de la personne ;

c) pour les personnes physiques : au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme. Si un pseudonyme est utilisé, cela est clairement indiqué ;

d) pour les personnes morales : au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels ;

e) des éléments de l'adresse, dont au moins la ville et l'État, de la personne physique ou morale à laquelle le certificat est délivré et, le cas échéant, ces éléments tels qu'ils figurent dans les registres officiels ;

f) le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;

g) des précisions sur le début et la fin de la période de validité du certificat ;

h) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

i) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;

j) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé visés au point h) ;

k) l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

ANNEXE VI
DÉFINITIONS

Aux fins du présent référentiel, on entend par :

- Cachet :

  « cachet électronique », des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières ;

  « cachet électronique avancé », un cachet électronique qui satisfait aux exigences énoncées à l'article 27 ;

  « cachet électronique qualifié », un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ;

  « dispositif de création de cachet électronique », un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique ;

  « dispositif de création de cachet électronique qualifié », un dispositif de création de cachet électronique qui satisfait mutatis mutandis aux exigences fixées à l'Annexe III ;

  « données de création de cachet électronique », des données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

  « créateur de cachet », une personne morale qui crée un cachet électronique ;

- Certificat :

  « certificat de cachet électronique », une attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne ;

  « certificat qualifié de cachet électronique », un certificat de cachet électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'Annexe IV ;

  « certificat d'authentification de site Internet », une attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré ;

  « certificat qualifié d'authentification de site Internet », un certificat d'authentification de site internet, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'Annexe V ;

  - « Certification de Sécurité de Premier Niveau ou CSPN », elle consiste en des tests en « boîte noire » (sans connaissance du fonctionnement du système testé) effectués en temps et délais contraints. La CSPN est une alternative aux évaluations « Critères Communs », dont le coût et la durée peuvent être un obstacle, et lorsque le niveau de confiance visé est moins élevé. Cette certification s'appuie sur des critères, une méthodologie et un processus élaborés par l'Agence Nationale de la Sécurité des Systèmes d'Information française ;

- « critères communs », les critères communs sont un ensemble de normes internationalement reconnues (ISO 15408) dont l'objectif est d'évaluer de façon impartiale la sécurité des systèmes et des logiciels informatiques ;

  « document électronique », tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel ;

- Homologation :

  « homologation de sécurité », l'homologation de sécurité est la déclaration par l'autorité d'homologation que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le système d'information opère dans les conditions approuvées par l'autorité d'homologation ;

  « autorité d'homologation », l'autorité d'homologation est la personne physique qui prononce l'homologation de sécurité du système d'information, c'est-à-dire qui prend la décision d'accepter les risques résiduels identifiés sur le système. L'autorité d'homologation doit être désignée à un niveau

hiérarchique suffisant pour assumer toutes les responsabilités. Il est donc nécessaire que l'autorité d'homologation se situe à un niveau de direction dans le service exécutif de l'État ;

- Horodatage :

« horodatage électronique », des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ;

« horodatage électronique qualifié », un horodatage électronique qui satisfait aux exigences fixées à l'article 32 ;

- Identité :

« identification électronique », le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ;

« authentification », un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique ;

« données d'identification personnelles », un ensemble d'informations permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

« moyen d'identification électronique », un élément matériel et/ou immatériel contenant des données d'identification personnelles utilisé pour s'authentifier pour un service en ligne ;

« partie utilisatrice », une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance ;

« schéma d'identification électronique », un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales ;

« Organismes du secteur public », personnes morales de droit public, autorités publiques, organismes de droit privé investis d'une mission d'intérêt général ou concessionnaires d'un service public ;

- Prestataire :

« Prestataire de Services de Confiance (PSCO) », une personne physique ou morale qui fournit un ou plusieurs services de confiance ;

« prestataire de services de confiance qualifié », un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'Agence Monégasque de Sécurité Numérique le statut qualifié ;

- Produit :

« produit », un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance ;

- Service :

« service de confiance », un service électronique normalement fourni contre rémunération qui consiste :

- en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques et de certificats relatifs à ces services ; ou
- en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou
- en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services ;

« service de confiance qualifié », un service de confiance fourni par un prestataire qualifié de services de confiance et qui a obtenu le statut qualifié par le Directeur de l'Agence Monégasque de Sécurité Numérique ;

« organisme d'évaluation de la conformité », un organisme compétent pour effectuer l'évaluation de la conformité d'un « prestataire de services de confiance qualifié » et des « services de confiance qualifiés » qu'il doit fournir ;

- Signature :

« signature électronique », des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ;

« signature électronique avancée », une signature électronique qui satisfait aux exigences énoncées à l'article 18 ;

« signature électronique qualifiée », une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ;

« signataire », une personne physique qui crée une signature électronique ;

« données de création de signature électronique », des données uniques qui sont utilisées par le signataire pour créer une signature électronique ;

« certificat de signature électronique », une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne ;

« certificat qualifié de signature électronique », un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'Annexe II ;

« dispositif de création de signature électronique », un dispositif logiciel ou matériel configuré servant à créer une signature électronique ;

« dispositif de création de signature électronique qualifié », un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'Annexe III ;

« données de validation », des données qui servent à valider une signature électronique ou un cachet électronique ;

« validation », le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique.