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

Type	Texte réglementaire
Nature	Arrêté ministériel
Date du texte	6 juillet 2020
Publication	Journal de Monaco du 17 juillet 2020[1 p.12]
Thématiques	Pouvoir exécutif et Administration ; Nouvelles technologies et télécommunications

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 2020 ;

Article 1er

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.

Article 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.

Article 3 - Applicabilité 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.

Article 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.

Article 5 - Accessibilité aux personnes handicapées

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.

Article 6 - Organe de contrôle

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.

Article 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.

Article 8 - Organismes d'évaluation de la conformité

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.

Article 9 - Prestataire de Services de Confiance.

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

Article 10 - Exigences de sécurité 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.

Article 11 - Information des prestataires de services de confiance à 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.

Article 12 - Prestataire de services de confiance qualifié[1]

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.

Article 13 - Exigences applicables aux prestataires de services de confiance qualifiés[2]

Modifié par la loi n° 1.565 du 3 décembre 2024

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° 1.565 du 3 décembre 2024 ;
- 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.

Article 14 - Contrôle des prestataires de services de confiance qualifiés

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.

Article 15 - Lancement d'un service de confiance qualifié

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.

Article 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.

Article 17 - Label de confiance de la Principauté pour les services de confiance qualifiés

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.

Article 18 - Exigences relatives à une signature électronique avancée

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.

Article 19 - Signatures électroniques dans le cadre de la relation entre Administration et administrés

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.

Article 20 - Certificats qualifiés de signature électronique[3]

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.

Article 21 - Exigences applicables aux dispositifs de création de signature électronique qualifiée[4]

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.

Article 22 - Certification des dispositifs de création de signature électronique qualifiée[5]

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.

Article 23 - Publication d'une liste des dispositifs de création de signature électronique qualifiée

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.

Article 24 - Exigences applicables à la validation des signatures électroniques qualifiées.

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.

Article 25 - Service de validation qualifié des signatures électroniques qualifiées

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.

Article 26 - Service de conservation qualifié des signatures électroniques qualifiées

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.

Article 27 - Exigences du cachet électronique avancé

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.

Article 28 - Cachets électroniques 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.

Article 29 - Certificats qualifiés de cachet électronique[6]

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.

Article 30 - Dispositifs de création de cachet électronique qualifié[7]

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

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

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

Article 31 - Validation et conservation des cachets électroniques qualifiés

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

Article 32 - Règles relatives à l'horodatage électronique[8]

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.

Article 33 - Exigences applicables aux horodatages électroniques qualifiés[9]

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.

Article 34 - Exigences applicables aux certificats qualifiés d'authentification de site Internet.[10]

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.

Article 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.

Article 36 - Niveaux de garantie des schémas d'identification électronique[11]

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.

Article 37 - Atteinte à la sécurité

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.

Article 38 - Responsabilité

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.

Article 39 - Coopération et interopérabilité

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.

Article 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.

Article 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* ».

Article 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.

Annexe - Référentiel Général de Sécurité de la Principauté de Monaco (RGSP) - Règles applicables aux systèmes d'information aux services de confiance pour les transactions électroniques

Voir le document associé.

Notes

Notes de la rédaction

1. ^ [p.4] Voir l'arrêté ministériel n° 2020-893 du 18 décembre 2020 et l'arrêté ministériel n° 2022-461 du 8 septembre 2022
2. ^ [p.4] Voir l'arrêté ministériel n° 2020-892 du 18 décembre 2020
3. ^ [p.7] Voir l'arrêté ministériel n° 2020-894 du 18 décembre 2020
4. ^ [p.7] Voir l'arrêté ministériel n° 2020-463 du 6 juillet 2020
5. ^ [p.7] Voir l'arrêté ministériel n° 2020-463 du 6 juillet 2020
6. ^ [p.8] Voir l'arrêté ministériel n° 2020-894 du 18 décembre 2020
7. ^ [p.9] Voir l'arrêté ministériel n° 2020-463 du 6 juillet 2020
8. ^ [p.9] Voir l'arrêté ministériel n° 2021-151 du 18 février 2021
9. ^ [p.9] Voir l'arrêté ministériel n° 2021-151 du 18 février 2021
10. ^ [p.9] Voir l'arrêté ministériel n° 2020-894 du 18 décembre 2020
11. ^ [p.10] Voir l'arrêté ministériel n° 2020-462 du 6 juillet 2020

Liens

1. Journal de Monaco du 17 juillet 2020
   ^ [p.1] https://journaldemonaco.gouv.mc/Journaux/2020/Journal-8495