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

ANNEXE AU « JOURNAL DE MONACO » N° 8.495

DU 17 JUILLET 2020

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, 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.

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 ».

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.

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.

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.).

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.

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, basée sur une Certification de Sécurité de Premier Niveau (CSPN) ;
- qualification standard, basée sur une évaluation Critères Communs EAL 3+ ;
- qualification renforcée, basée sur une évaluation Critères Communs EAL4+.

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 la 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/Guides-pratiques/).

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 appropriées, 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 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 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 repose 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.

imprimé sur papier recyclé

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