Arrêté Ministériel n° 2018-634 du 2 juillet 2018 portant application de 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

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

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

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

Vu l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée, et notamment son article 54 ;

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

Vu l'Ordonnance Souveraine n° 6.525 du 16 août 2017 portant application des articles 18, 19 et 25 de la loi n° 1.383 du 2 août 2011 sur l'Économie Numérique, modifiée ;

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° 2017-835 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 la délibération du Conseil de Gouvernement en date du 20 juin 2018 ;

ARRÊTONS :

ARTICLE PREMIER.

La liste de confiance, visée au paragraphe 26 du Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, susvisé, comporte outre les informations sur les prestataires de service de confiance qualifiés et les services qu'ils fournissent, des spécifications techniques ainsi que les formats de la liste.

Cette liste de confiance fait l'objet, conformément au point 2 du paragraphe visé au précédent alinéa, d'une signature électronique ou d'un cachet électronique sous une forme adaptée au traitement automatisé mis en œuvre, dans le respect des spécifications techniques détaillées dans l'annexe au présent arrêté.

Lorsque ladite liste est publiée par voie électronique dans une version directement lisible, elle doit contenir les mêmes données que celles destinées à un traitement automatisé et faire également l'objet d'une signature électronique ou d'un cachet électronique, dans le respect des spécifications techniques précitées.

ART. 2.

Les spécifications techniques et les formats de la liste de confiance applicables sont annexés au présent arrêté.

ART. 3.

Le Ministre d'État, le Conseiller de Gouvernement-Ministre de l'Équipement, de l'Environnement et de l'Urbanisme, le Conseiller de Gouvernement-Ministre des Finances et de l'Économie, le Conseiller de Gouvernement-Ministre des Relations Extérieures et de la Coopération, le Conseiller de Gouvernement-Ministre de l'Intérieur et le Conseiller de Gouvernement-Ministre des Affaires Sociales et de la Santé sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le deux juillet deux mille dix-huit.

Le Ministre d'État,
S. TELLE.

SPÉCIFICATIONS TECHNIQUES ET FORMATS DE LA LISTE DE CONFIANCE

Annexe à l'Arrêté Ministériel n° 2018-634 du 2 juillet 2018

SOMMAIRE

1. Exigences générales

La liste de confiance comprend des informations actualisées et tous les historiques, à compter de l'inscription d'un prestataire de services de confiance dans la liste de confiance, sur l'état des services de confiance répertoriés.

Les informations figurant sur la liste de confiance visent principalement à soutenir la validation des jetons de service de confiance qualifié, à savoir des objets physiques ou binaires (logiques) générés ou émis à la suite de l'utilisation d'un service de confiance qualifié, par exemple des signatures/cachets électroniques nommément qualifiés, des signatures/cachets électroniques avancés accompagnés d'un certificat qualifié, des horodatages qualifiés, etc.

2. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

CRL Certificate Revocation List (liste des certificats révoqués) ;

IEC International Electrotechnical Commission ;

IETF Internet Engineering Task Force ;

ISO International Organization for Standardization (Organisation internationale de normalisation) ;

ITU International Telecommunication Union (Union internationale des télécommunications) ;

PDF Portable Document Format ;

PKI Public Key Infrastructure (infrastructure de gestion de clés) ;

RFC Request For Comments (documents publiés par l'IETF) ;

TS Technical Specification (spécification technique) ;

URI Uniform Resource Identifier.

3. Spécifications détaillées pour le modèle de liste de confiance

Les présentes spécifications se fondent sur le standard ETSI TS 119 612 v2.1.1 « Electronic Signatures and Infrastructures (ESI) ; Trusted Lists » (ci-après dénommée ETSI TS 119 612).

La liste de confiance contient un certain nombre de champs prescrits soit dans l'ETSI TS 119 612 soit dans le présent paragraphe.

Lorsqu'aucune prescription n'est prévue dans les présentes spécifications, les prescriptions des clauses 5 et 6 d'ETSI TS 119 612 doivent être appliquées dans leur intégralité.

Lorsque des prescriptions spécifiques sont établies dans les présentes spécifications, elles prévalent sur les prescriptions correspondantes d'ETSI TS 119 612.

En cas de divergence entre les présentes prescriptions et les prescriptions d'ETSI TS 119 612, les prescriptions définies à la présente annexe prévalent.

3.1. Champ Scheme Name (Clause 5.3.6)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.6 d'ETSI TS 119 612, selon lesquelles la dénomination suivante doit être utilisée pour le système :

« EN_name_value » = Liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par la Principauté, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent.

3.2. Champ Scheme Information URI (Clause 5.3.7)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.7 d'ETSI TS 119 612, selon lesquelles « les informations appropriées concernant le système » doivent inclure au minimum :

a) Des informations introductives concernant la portée et le contexte de la liste de confiance, du système de contrôle sous-jacent et du système d'homologation. Le texte à utiliser est le suivant, la chaîne de caractères « [nom de l'État membre concerné] » devant être remplacée par le nom de la Principauté :

- La présente liste constitue la liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par la Principauté, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent ;
- La liste de confiance est un élément essentiel pour établir la confiance entre les acteurs du marché électronique en permettant aux utilisateurs de déterminer le statut qualifié et l'historique du statut des prestataires de services de confiance et de leurs services ;
- La liste de confiance de la Principauté inclut, au minimum, les informations visées à l'article premier de l'Arrêté auquel est rattachée la présente annexe ;
- La Principauté peut inclure dans sa liste de confiance des informations relatives à des prestataires de services de confiance non qualifiés, ainsi que des informations relatives aux services de confiance non qualifiés qu'ils fournissent. Il doit être clairement indiqué qu'ils ne sont pas qualifiés.

b) Informations spécifiques sur le système de contrôle sous-jacent et, le cas échéant, sur le système d'homologation en particulier les informations sur le système de contrôle applicable aux prestataires de services de confiance qualifiés et non qualifiés et aux services de confiance qualifiés et non qualifiés qu'ils fournissent.

Ces informations spécifiques doivent comprendre, au minimum, pour chaque système sous-jacent énuméré ci-dessus :

- une description générale ;
- des informations sur le processus suivi pour le système de contrôle et pour l'homologation en vertu du système d'homologation ;
- des informations sur les critères de contrôle ou d'approbation des prestataires de services de confiance ;
- des informations sur les critères et les règles utilisés pour sélectionner les organismes de surveillance ou d'audit et sur la manière dont les prestataires de services de confiance et les services de confiance qu'ils fournissent sont évalués par ces organismes ;
- le cas échéant, d'autres informations de contact et informations générales applicables au fonctionnement du système.

3.3. Champ Scheme Type/Community/Rules (Clause 5.3.9)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.9 d'ETSI TS 119 612.

Il inclut seulement les URI anglais.

Il comprend deux URI dont la structure est précisée par l'Agence Monégasque de Sécurité Numérique.

3.4. Champ TSL Policy/Legal Notice (Clause 5.3.11)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.3.11 d'ETSI TS 119 612. Il doit contenir le texte suivant :

Cadre juridique applicable en version anglaise :

« The applicable legal framework for the present trusted list is the ministerial order number 2017-835, of November 29th, 2017, modified, concerning the general security repository. »

Cadre juridique applicable en version française :

« Le cadre juridique applicable de la présente liste de confiance est l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017, modifié, définissant le Référentiel Général de Sécurité). »

3.5. Champ Service Current Status (Clause 5.5.4)

Ce champ est obligatoire et doit être conforme aux spécifications de la clause 5.5.4 d'ETSI TS 119 612.

4. Spécifications pour la version directement visible de la liste de confiance

Lorsqu'une version directement lisible de la liste de confiance est établie et publiée, elle doit être fournie sous la forme d'un document PDF (Portable Document Format) conforme à la norme ISO 32000[1] qui doit être formaté conformément au profil PDF/A [ISO 19005[2]].

Le contenu de la version directement lisible fondée sur PDF/A de la liste de confiance doit respecter les exigences suivantes :

- la structure de la version directement lisible doit refléter le modèle logique décrit dans ETSI TS 119 612,
- chaque champ présent doit être visible et indiquer :
    - l'intitulé du champ (par exemple « Service type identifier ») ;
    - la valeur du champ (par exemple http://uri.etsi.org/TrstSvc/Svctype/CA/QC) ;
    - la signification (description) de la valeur du champ, le cas échéant (par exemple « Un service de génération de certificat créant et signant des certificats basés sur l'identité et d'autres attributs vérifiés par les services d'enregistrement en question ») ;
    - le cas échéant, plusieurs versions en langage naturel telles que prévues sur la liste de confiance,

[1] ISO 32000-1 :2008 : Gestion de documents - Format de document portable - Partie 1 : PDF 1.7.
[2] ISO 19005-2 :2011 : Gestion de documents - Format de fichier des documents électroniques pour une conservation à long terme - Partie 2 : Utilisation de l'ISO 32000-1 (PDF/A-2).

- les champs et valeurs correspondantes suivants des certificats numériques[3], présents dans le champ « Service digital identity », doivent apparaître au minimum dans la version directement lisible :
    - Version ;
    - Numéro de série de certificat ;
    - Algorithme de signature ;
    - Émetteur - tous les champs de nom distingué pertinents ;
    - Période de validité ;
    - Objet - tous les champs de nom distingué pertinents ;
    - Clé publique ;
    - Identifiant de la clé de l'autorité ;
    - Identifiant de la clé de l'objet ;
    - Utilisation de la clé ;
    - Utilisation avancée de la clé ;
    - Politiques de certification - tous les identifiants de politique et « qualifiers » de politique ;
    - Tableau de correspondance des politiques ;
    - Autre nom de l'objet ;
    - Attributs d'annuaire de l'objet ;
    - Contraintes de base ;
    - Contraintes de politique ;
    - Points de distribution CRL[4] ;
    - Accès aux informations sur l'autorité ;
    - Accès aux informations sur l'objet ;
    - Déclarations de certificat qualifié[5] ;
    - Algorithme de hachage ;
    - Valeur de hachage du certificat,
- la version directement lisible doit être facilement imprimable,
- une signature ou un cachet doit être apposé par l'exploitant du système directement lisible selon la signature avancée PDF spécifiée aux points 1 et 3 de la présente annexe.

[3] Recommandation ITU-T X.509 | ISO/IEC 9594-8 : Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - L'annuaire : Cadre général des certificats de clé publique et d'attribut (voir http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).
[4] RFC 5280 : Certificat internet X.509 PKI et profil CRL.
[5] RFC 3739 : internet X.509 PKI : Profil de certificats qualifiés.