Déclaration de transparence

de la hiérarchie certSIGN ROOT CA G2

Version 2.20

Date : 31 janvier 2022

Remarque importante

Ce document est la propriété de certSIGN SA

Adresse: 29 A Boulevard Tudor Vladimirescu,

AFI Tech Park 1, Bucarest 050881, Roumanie

Téléphone : 0 805 98 80 04

Web : www. certsign.fr

Historique des documents

Version	Date d'entrée en vigueur	Motif	La personne qui a effectué le changement
1.0	28 février 2017	Publication de la première version	Responsable de la sécurité de l'information
2.0	15 mars 2017	Deuxième version après l'audit à mi-parcours	Responsable de la sécurité de l'information
2.1	3 avril 2017	Mise à jour mineure pour clarification	Responsable de la sécurité de l'information
2.2	14 août 2017	Mise à jour mineure pour clarification	Responsable de la sécurité de l'information
2.3	5 février 2018	Examen annuel	Responsable de la sécurité de l'information
2.4	25 juin 2018	Mise à jour pour l'ajout de profils certifiés	Gestionnaire des politiques de l'ICP
2.5	27 août 2018	Mise à jour pour ajouter une nouvelle méthode d'identification initiale	Gestionnaire des politiques de l'ICP
2.6	25 septembre 2018	Signature à distance avec RQSCD	Gestionnaire des politiques de l'ICP
2.7	1er novembre 2018	Mise à jour pour l'ajout de profils de certificats simples, signature à distance	Gestionnaire des politiques de l'ICP
2.8	5 novembre 2018	Mise à jour en raison d'un changement de lieu	Gestionnaire des politiques de l'ICP
2.9	14 janvier 2019	Examen annuel	Gestionnaire des politiques de l'ICP
2.10	9 mars 2019	Mise à jour pour l'ajout de profils certifiés (Trusted List)	Gestionnaire des politiques de l'ICP
2.11	1er avril 2019	Mise à jour pour l'ajout de profils de certificat (dnQualifier)	Gestionnaire des politiques de l'ICP
2.12	22 juillet 2019	Mise à jour pour l'ajout de profils de certificats (DSP2)	Gestionnaire des politiques de l'ICP
2.13	30 septembre 2019	Mise à jour mineure pour clarification (identification des citoyens non RO)	Gestionnaire des politiques de l'ICP
2.14	31 janvier 2020	Examen annuel	Gestionnaire des politiques de l'ICP
2.15	3 février 2020	Mise à jour pour ajouter des profils de certificat qualifiés pour les cachets	Gestionnaire des politiques de l'ICP
2.16	15 avril 2020	Mise à jour de la responsabilité de certSIGN	Gestionnaire des politiques de l'ICP
2.17	31 juillet 2020	Ajout d'un OID avec pseudonyme	Gestionnaire des politiques de l'ICP
2.18	7 janvier 2021	Ajout d'OIDs EO 140/2020	Gestionnaire des politiques de l'ICP

2.19	29 janvier 2021	Mise à jour annuelle	Gestionnaire des politiques de l'ICP
2.20	31 janvier 2022	Mise à jour annuelle + protection du courrier électronique OID	Gestionnaire des politiques de l'ICP

Ce document a été créé par et est la propriété de :

Propriétaire	Auteur	Date de création
Responsable de la sécurité de l'information	Responsable de la sécurité de l'information	Décembre 2016

Liste de distribution

Destination	Date de la distribution
Internet public	Février 2017
Internet public	Mars 2017
Internet public	Avril 2017
Internet public	Août 2017
Internet public	Février 2018
Internet public	Juin 2018
Internet public	Août 2018
Internet public	Septembre 2018
Internet public	Novembre 2018
Internet public	Novembre 2018
Internet public	Janvier 2019
Internet public	Mars 2019
Internet public	Avril 2019
Internet public	Juillet 2019
Internet public	Septembre 2019
Internet public	Janvier 2020
Internet public	Février 2020
Internet public	Avril 2020
Internet public	Juillet 2020
Internet public	Janvier 2021
Internet public	Janvier 2022

Ce document a été approuvé par :

Version	Nom	Date
1.0	Comité de gestion des politiques et procédures	Février 2017

2.0	Comité de gestion des politiques et procédures	Mars 2017
2.1	Comité de gestion des politiques et procédures	Avril 2017
2.2	Comité de gestion des politiques et procédures	Août 2017
2.3	Comité de gestion des politiques et procédures	Février 2018
2.4	Comité de gestion des politiques et procédures	Juin 2018
2.5	Comité de gestion des politiques et procédures	Août 2018
2.6	Comité de gestion des politiques et procédures	Septembre 2018
2.7	Comité de gestion des politiques et procédures	Novembre 2018
2.8	Comité de gestion des politiques et procédures	Novembre 2018
2.9	Comité de gestion des politiques et procédures	Janvier 2019
2.10	Comité de gestion des politiques et procédures	Mars 2019
2.11	Comité de gestion des politiques et procédures	Avril 2019
2.12	Comité de gestion des politiques et procédures	Juillet 2019
2.13	Comité de gestion des politiques et procédures	Septembre 2019
2.14	Comité de gestion des politiques et procédures	Janvier 2020
2.15	Comité de gestion des politiques et procédures	Février 2020
2.16	Comité de gestion des politiques et procédures	Avril 2020
2.17	Comité de gestion des politiques et procédures	Juillet 2020
2.18	Comité de gestion des politiques et procédures	Janvier 2021
2.19	Comité de gestion des politiques et procédures	Janvier 2021
2.20	Comité de gestion des politiques et procédures	Janvier 2022

Coupons

1 Coordonnées de certSIGN

Coordonnées :

certSIGN S.A.

Adresse : 29A Tudor Vladimirescu Boulevard, AFI Tech Park 1, Bucarest 050881, Roumanie

Registre du Commerce n° : J40/484/2006

Code d'enregistrement fiscal : RO 18288250

Site : www.certsign.fr

Ventes

Téléphone : 0 805 98 80 04

Email : office@certsign.fr

Ressources humaines certSIGN

Téléphone : 0 805 98 80 04

Assistance technique

Téléphone : 0 805 98 80 04

Courriel : suport@certsign.fr

Contact :

Téléphone : 0 805 98 80 04

Courriel : office@certsign.fr

2 Type de certificat, procédures de validation et utilisation

certSIGN émet les types de certificats suivants, comme décrit ci-dessous.

Au niveau de l'AC ROOT G2, certSIGN émet les types de certificats suivants :

Niveau Root CA G2	Type	Sous-type
certSIGN ROOT CA G2	**Certificats AC**	***Certificat certSIGN ROOT CA G2*** ***certSIGN Certificat de l'autorité de certification publique*** ***Certificat d'AC qualifiée certSIGN*** ***Certificat d'AC Web certSIGN***
certSIGN ROOT CA G2	**Certificat OCSP**	***s.o.***

Au niveau de l'AC secondaire du ROOTA CA G2, certSIGN émet les types de certificats suivants :

Niveau Root CA G2	Type	Sous-type
AC publique certSIGN	**Certificats non qualifiés**	***Certificats non qualifiés pour la signature et l'authentification*** ▪ Sans dispositif HW et clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par certSIGN ▪ Avec un dispositif HW et une clé générée et stockée par certSIGN pour la signature et l'authentification à distance ▪ Avec le dispositif HW et la clé générée et stockée par certSIGN pour la signature et l'authentification à distance qui ne peut être utilisée que dans la relation entre le Sujet et le Bénéficiaire. ▪ Sans dispositif HW et clé générée par certSIGN ▪ Avec le dispositif HW et la clé générée et stockée par certSIGN pour la signature à distance avec pseudonyme ▪ Aucun dispositif HW et une clé générée par certSIGN pour l'authentification, la signature et la protection des e-mails. ***Certificats non qualifiés pour le cryptage*** ▪ Sans dispositif HW et clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par certSIGN ▪ Sans dispositif HW et clé générée par certSIGN

Niveau Root CA G2	Type	Sous-type
		Certificats non qualifiés pour le cachet électronique ▪ Sans dispositif HW et clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par le Sujet ▪ Avec le dispositif HW et la clé générée par certSIGN ▪ Avec un dispositif HW et une clé générée et stockée par certSIGN pour le cachet électronique à distance ▪ Sans dispositif HW et clé générée par certSIGN ***Certificat OCSP***
AC qualifiée certSIGN	**Certificats qualifiés**	***Certificats qualifiés pour la signature*** ▪ avec QSCD et la clé générée par le Sujet ▪ avec QSCD et la clé générée par certSIGN o avec QSCD et clé générée et stockée par certSIGN pour la signature à distance o avec QSCD et clé générée et stockée par certSIGN pour la signature à distance qui ne peut être utilisée que dans le cadre de la relation entre le Sujet et le Bénéficiaire. o avec QSCD et la clé générée et stockée par certSIGN avec dnQualifier ▪ sans QSCD et clé générée par le Sujet ▪ sans QSCD et clé générée par certSIGN ▪ avec QSCD et la clé générée par certSIGN pour la signature de la liste de confiance ▪ Selon GEO 140/2020 avec QSCD ▪ Selon GEO 140/2020 avec QSCD et clé générée et stockée par certSIGN pour la signature à distance ***Certificats qualifiés pour le cachet*** ▪ avec QSCD et la clé générée par le Sujet ▪ avec QSCD et la clé générée par certSIGN ▪ avec QSCD et clé générée et stockée par certSIGN pour le cachet électronique à distance ▪ avec QSCD et clé générée et stockée par certSIGN pour les prestataires de services de paiement dans le cadre de la directive EU/PSD2 ▪ sans QSCD et clé générée par le Sujet ▪ sans QSCD et clé générée par certSIGN ▪ sans QSCD et clé générée et stockée par le Sujet pour les prestataires de services de paiement en vertu de la directive UE/PSD2 ***Certificat du serveur pour l'horodatage*** ***Certificat OCSP***

Niveau Root CA G2	Type	Sous-type
AC Web certSIGN	**Certificats de serveur Web**	***Certificat d'authentification de site Web qualifié (QWAC)*** ***Certificat qualifié pour l'authentification des sites web pour les prestataires de services de paiement dans le cadre de la directive européenne (PSD2)*** ***Certificat non qualifié pour l'authentification de sites Web - avec validation de l'organisation (OV)*** ***Certificat OCSP***

certSIGN s'assurera que la preuve de l'identification des Sujets et de l'exactitude de leurs noms et des données associées est soit correctement examinée dans le cadre du service défini, soit, le cas échéant, vérifiée par l'examen d'attestations provenant de sources appropriées et autorisées, comme indiqué dans le tableau suivant :

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
Certificat qualifié pour la signature électronique	Pour la signature électronique	***Avec le QSCD et la clé générée par le Sujet*** CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.1** Cette politique est conforme à la norme ETSI EN 319 411-2.	La personne physique est tenue de présenter les documents suivants à la demande de l'autorité d'enregistrement : • Accord contractuel • Modalités et conditions • Documents d'identification (carte d'identité ou passeport, dans le cas des citoyens roumains ; carte d'identité, passeport ou document d'identité délivré par les autorités roumaines, dans le cas des citoyens étrangers) confirmant l'identité du Sujet, Et si le Sujet ou le Bénéficiaire souhaite inclure les données d'une institution (entité juridique) pour laquelle il travaille : • Extrait valide du Registre du Commerce (ou équivalent pour les sociétés étrangères enregistrées en vertu d'un droit étranger) ; • Extrait du Registre des associations et fondations (ou équivalent pour les associations et fondations étrangères) • Mandat officiel, lorsque la personne physique représentant la personne morale n'est pas le représentant légal de l'entité. • Dans le cas d'entités sans personnalité juridique, l'identification du Sujet se fera sur la base de l'acte juridique d'établissement. • certSIGN vérifie également la relation contractuelle du Bénéficiaire avec les Sujets.
		Avec QSCD et la clé générée par certSIGN CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.2** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Avec QSCD et clé générée et stockée par certSIGN pour la signature à distance CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.2.1** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Avec le QSCD et la clé générée et stockée par certSIGN pour la signature à distance qui ne peut être utilisée que dans la relation entre le Sujet et le Bénéficiaire. CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.2.2** Cette politique est conforme à la norme ETSI EN 319 411-2.	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		Avec QSCD et la clé générée et stockée par certSIGN avec dnQualifier CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.2.3** Cette politique est conforme à la norme ETSI EN 319 411-2.	L'identification doit se faire en face à face ou par des méthodes d'identification qui fournissent un niveau d'assurance équivalent en fiabilité à la présence physique, devant un notaire ou en utilisant un certificat qualifié délivré uniquement par certSIGN.
		Avec QSCD et certSIGN, clé générée pour la signature de la liste de confiance CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.7** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Pas de QSCD et de clé générée par le Sujet CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.8** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Sans QSCD et clé générée par certSIGN CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.9** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Selon GEO 140/2020 avec QSCD CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.14**	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Selon GEO 140/2020 avec QSCD et clé générée et stockée par certSIGN pour la signature à distance CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.15** Cette politique est conforme à la norme ETSI EN 319 411-2.	
Certificat qualifié pour le cachet électronique	Pour le cachet électronique	***Avec le QSCD et la clé générée par le Sujet*** CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.3** Cette politique est conforme à la norme ETSI EN 319 411-2.	Les représentants autorisés de l'institution sont tenus de présenter les documents suivants à la demande de l'Autorité d'enregistrement : • Accord contractuel • Modalités et conditions • Extrait valide du Registre du Commerce (ou équivalent pour les sociétés étrangères enregistrées en vertu d'un droit étranger) ; • Extrait du Registre des associations et fondations (ou équivalent pour les associations et fondations étrangères) • Mandat officiel, lorsque la personne physique représentant la personne morale n'est pas le représentant légal de l'entité. • Dans le cas d'entités sans personnalité juridique, l'identification du Sujet se fera sur la base de l'acte juridique d'établissement.
		Avec QSCD et la clé générée par certSIGN CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.4** Cette politique est conforme à la norme ETSI EN 319 411-2.	
		Avec QSCD et clé générée par certSIGN pour l'application du cachet électronique à distance CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.4.1**	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		Cette politique est conforme à la norme ETSI EN 319 411-2. ***Avec QSCD et clé générée par certSIGN pour les prestataires de services de paiement dans le cadre de la directive EU/PSD2*** CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.10** Cette politique est conforme à la norme ETSI EN 319 411-2. ***Pas de QSCD et de clé générée par le Sujet*** CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.11** Cette politique est conforme à la norme ETSI EN 319 411-2. ***Sans QSCD et clé générée par certSIGN pour le cachet électronique à distance*** CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.12** Cette politique est conforme à la norme ETSI EN 319 411-2.	L'identification doit se faire en face à face ou par des méthodes d'identification qui fournissent un niveau d'assurance équivalent en fiabilité à la présence physique, devant un notaire ou en utilisant un certificat qualifié délivré uniquement par certSIGN.

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		Pas de QSCD et de clé générée par le Sujet pour les prestataires de services de paiement dans le cadre de la directive UE/PSD2 CPP AC qualifiée certSIGN **OID: 1.3.6.1.4.1.25017.3.1.3.13** Cette politique est conforme à la norme ETSI EN 319 411-2.	
Certificat du serveur pour l'horodatage	Uniquement pour la signature des jetons d'horodatage	**Horodatage** CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.5** Cette politique est conforme à la norme ETSI EN 319 411-2.	Voir le certificat qualifié pour le cachet électronique.
Certificat OCSP	Uniquement pour la signature des réponses OCSP	**OCSP** CPP AC qualifiée certSIGN **OID : 1.3.6.1.4.1.25017.3.1.3.6** Cette politique est conforme à la norme ETSI EN 319 411-2.	Voir le certificat qualifié pour le cachet électronique
Certificat non qualifié pour l'authentification et la signature	Pour la signature et l'authentification électroniques	***Pas de dispositif HW et de clé générée par le Sujet*** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.1** Cette politique est conforme à la norme ETSI EN 319 411-1.	La personne physique est tenue de présenter les documents suivants à la demande de l'autorité d'enregistrement : • Accord contractuel • Modalités et conditions, • Documents d'identité (carte d'identité ou passeport dans le cas des citoyens roumains, passeport dans le cas des citoyens étrangers et passeport ou document d'identité délivré par les autorités roumaines dans le cas des citoyens
		Avec le dispositif HW et la clé générée par le Sujet CPP certSIGN Public CA	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		OID:1.3.6.1.4.1.25017.3.1.2.2 Cette politique est conforme à la norme ETSI EN 319 411-1.	étrangers qui ont le droit de résidence sur le territoire roumain) confirmant l'identité du Sujet, Et si le Sujet ou le Bénéficiaire souhaite inclure les données d'une institution (entité juridique) pour laquelle il travaille : • Documents officiels montrant que la personne morale agit en tant qu'employeur de la personne physique ou qu'il existe un lien juridique entre eux. Aucune identification en face à face n'est requise.
		Avec le dispositif HW et la clé générée par certSIGN CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.3** ○ ***Avec un dispositif HW et une clé générée et stockée par certSIGN pour la signature et l'authentification à distance OID:1.3.6.1.4.1.25017.3.1.2.3.1*** ○ ***Avec le dispositif HW et la clé générée et stockée par certSIGN pour la signature et l'authentification à distance qui ne peut être utilisée que dans la relation entre le Sujet et le Bénéficiaire. OID:1.3.6.1.4.1.25017.3.1.2.3.2*** Ces politiques sont conformes à la norme ETSI EN 319 411-1.	
		Pas de dispositif HW et clé générée par certSIGN CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.4** Cette politique est conforme à la norme ETSI EN 319 411-1.	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
Certificat non qualifié pour l'authentification et la signature	Pour la signature et l'authentification électroniques	***Avec le dispositif HW et la clé générée et stockée par certSIGN pour la signature et l'authentification à distance, avec pseudonyme*** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.14** Cette politique est conforme à la norme ETSI EN 319 411-1.	Le Sujet déclare un pseudonyme, un courriel et un numéro de téléphone, et accepte les conditions spécifiques. Seuls le courriel et le téléphone sont vérifiés.
Certificat non qualifié pour l'authentification et la signature	Pour la signature électronique, l'authentification et la protection du courrier électronique	***Pas de dispositif HW et clé générée par certSIGN pour la protection des emails*** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.15** Cette politique est conforme à la norme ETSI EN 319 411-1.	La personne physique est tenue de présenter les documents suivants à la demande de l'autorité d'enregistrement : • Accord contractuel • Modalités et conditions, • Documents d'identité (carte d'identité ou passeport dans le cas des citoyens roumains, passeport dans le cas des citoyens étrangers et passeport ou document d'identité délivré par les autorités roumaines dans le cas des citoyens étrangers qui ont le droit de résidence sur le territoire roumain) confirmant l'identité du sujet, Et si le Sujet ou le Bénéficiaire souhaite inclure les données d'une institution (entité juridique) pour laquelle il travaille : • Documents officiels montrant que la personne morale agit en tant qu'employeur de la personne physique ou qu'il existe un lien juridique entre eux. Aucune identification en face à face n'est requise. En plus de la procédure de validation ci-dessus, le courriel est validé par une méthode de questions-réponses. La validation du contrôle des adresses e-mail est vérifiée en envoyant un e-mail avec un lien contenant une URL aléatoire, et en vérifiant que l'URL a été consulté.

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
Certificats non qualifiés pour le cachet électronique	Pour le cachet électronique uniquement	***Pas de dispositif HW et de clé générée par le Sujet*** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.9** Cette politique est conforme à la norme ETSI EN 319 411-1.	Les représentants autorisés de l'institution sont tenus de présenter les documents suivants à la demande de l'autorité d'enregistrement : • Contrat, • Modalités et conditions, • Extrait valide du Registre du Commerce (ou équivalent étranger des sociétés étrangères enregistrées en vertu du droit étranger) ; • Mandat officiel, lorsque la personne physique représentant l'entité juridique n'est pas le dirigeant légal de l'entité. • Documents prouvant l'identité du Sujet (carte d'identité ou passeport dans le cas des citoyens roumains, passeport dans le cas des citoyens étrangers et passeport ou document d'identité délivré par les Autorités roumaines dans le cas des citoyens étrangers qui ont le droit de résidence sur le territoire roumain) ; Aucune identification en face à face n'est requise.
		Avec le dispositif HW et la clé générée par le Sujet CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.10** Cette politique est conforme à la norme ETSI EN 319 411-1.	
		Avec le dispositif HW et la clé générée par certSIGN CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.11** ***Avec un dispositif HW et une clé générée et stockée par certSIGN pour le cachet à distance*** ***OID:1.3.6.1.4.1.25017.3.1.2.11.1*** Ces politiques sont conformes à la norme ETSI EN 319 411-1.	
		Pas de dispositif HW et clé générée par certSIGN CPP certSIGN Public CA	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
		OID:1.3.6.1.4.1.25017.3.1.2.12 Cette politique est conforme à la norme ETSI EN 319 411-1.	
Certificats non qualifiés pour le cryptage	Pour le cryptage des données uniquement	***Pas de dispositif et de clé générée par le Sujet*** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.5** Cette politique est conforme à la norme ETSI EN 319 411-1.	Afficher les certificats non qualifiés pour l'authentification et la signature
		Avec le dispositif HW et la clé générée par le Sujet CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.6** Cette politique est conforme à la norme ETSI EN 319 411-1.	
		Avec le dispositif HW et la clé générée par certSIGN CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.7** Cette politique est conforme à la norme ETSI EN 319 411-1.	
		Sans dispositif et sans clé générée par certSIGN CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.8** Cette politique est conforme à la norme ETSI EN 319 411-1.	

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
Certificat OCSP	Uniquement pour la signature des réponses OCSP	**OCSP** CPP certSIGN Public CA **OID:1.3.6.1.4.1.25017.3.1.2.13** Cette politique est conforme à la norme ETSI EN 319 411-1.	Voir les certificats non qualifiés pour le cachet électronique.
Certificat pour l'authentification du site web (OV SSL)	Pour l'authentification du serveur Web uniquement	**Certificat pour l'authentification du site web (OV SSL)** AC Web CPP certSIGN pour OV SSL **OID : 1.3.6.1.4.1.25017.3.1.4.2** Cette politique est conforme à la norme ETSI EN 319 411-1 et aux exigences du CAB Forum Baseline.	Les organisations roumaines sont authentifiées sur la base de documents récents et d'attestations valables en Roumanie. Les organisations d'autres pays de l'UE étant authentifiées sur la base de documents et d'attestations équivalents applicables au pays en question. Les représentants autorisés de l'organisation sont tenus de présenter les documents suivants à la demande de l'autorité d'enregistrement : • Copie certifiée conforme du certificat d'enregistrement de la société ; • Documents prouvant l'identité du demandeur (carte d'identité ou passeport) et procuration confirmant qu'il est le représentant de la société ; • Demande d'achat ; • Déclaration standard du propriétaire du domaine La procédure de l'AE pour vérifier l'identité de l'entité juridique et de ses représentants autorisés consiste à : • Vérification des documents présentés par le Bénéficiaire, • Vérification de la demande, qui consiste en : o Vérification de la conformité des données spécifiées dans la demande avec celles des documents soumis,

Type/sous-type de certificat	Utilisation	Politique de certification	Procédure de validation
			○ Vérifiez la preuve de la propriété de la clé privée et que le nom distinctif est le bon, ○ Vérification de l'autorisation et de l'identité du représentant de la personne morale qui présente la demande au nom de l'entité.
Certificat d'authentification Web qualifié (QWAC SSL)	Pour l'authentification du serveur Web uniquement	***Certificat qualifié pour l'authentification des sites Web (QWAC SSL)*** CPP certSIGN Web CA pour les certificats qualifiés pour l'authentification des sites web. **OID : 1.3.6.1.4.1.25017.3.1.4.1** Cette politique est conforme à la norme ETSI EN 319 411-2 et aux exigences du Forum CA/B EV.	Selon les lignes directrices EV du Forum CA/B (www.cabforum.org), section 11. Exigences de vérification
		Certificat qualifié pour l'authentification de sites Web pour les prestataires de services de paiement en vertu de la directive UE/PSD2 (QWAC/PSD2) CPP certSIGN Web CA pour les certificats qualifiés pour l'authentification des sites web. **OID : 1.3.6.1.4.1.25017.3.1.4.4** Cette politique est conforme à la norme ETSI EN 319 411-2 et aux exigences du Forum CA/B EV.	Selon les lignes directrices EV du Forum CA/B (www.cabforum.org), section 11. Exigences de vérification
Certificat OCSP	Uniquement pour la signature des réponses OCSP	**OCSP** CPP certSIGN Web CA pour SSL OV **OID : 1.3.6.1.4.1.25017.3.1.4.**3Cette politique est conforme à la norme ETSI EN 319 411-1 et aux exigences du CAB Forum Baseline.	Voir le serveur Web du certificat SSL OV

3 Limiter la confiance

certSIGN couvre les dommages qu'elle peut causer en fournissant des services de certification à des personnes qui fondent leur comportement sur les effets juridiques de certificats qualifiés jusqu'à l'équivalent en lei de la somme de 10 000 euros par risque assuré. Le risque assuré représente tous les dommages causés, même s'il y en a plusieurs, après que le prestataire a manqué à ses obligations légales.

certSIGN couvrira tout dommage qu'elle pourrait causer en fournissant des services de certification à des personnes qui fondent leur conduite sur les effets juridiques des certificats qualifiés pour les certificats d'authentification des sites web (QWAC), comme l'exige le Forum CAB.

4 Obligations des bénéficiaires

Les bénéficiaires s'engagent à :

- Suivre les règles de l'accord conclu avec certSIGN ;
- Ne pas utiliser les paires de clés qu'aux fins définies au point 2 ci-dessus et conformément à toute autre limitation qui pourrait être notifiée au Bénéficiaire ;
- Soumettre ou envoyer les documents nécessaires confirmant les informations incluses dans la demande de certification ;
- Prendre des précautions raisonnables pour éviter toute utilisation non autorisée de la clé privée du sujet.
- Notifier certSIGN, sans retard excessif, si l'un des événements suivants se produit avant la fin de la période de validité indiquée dans le Certificat :
    - La clé privée du sujet a été perdue, volée ou compromise,
    - Le contrôle de la clé privée du sujet a été perdu en raison de la compromission potentielle ou réelle des données d'activation (par exemple, le code PIN) ou pour d'autres raisons,
    - Les inexactitudes ou les modifications du contenu de l'attestation telles que notifiées au Bénéficiaire.
- S'assurer que si le Bénéficiaire ou le Sujet génère des paires de clés du Sujet, seul le Sujet détient la clé privée,
- Utiliser le certificat et la clé privée correspondante seulement dans le but indiqué dans le certificat et conformément aux objectifs et restrictions énoncés dans le présent document.

5 Obligations des Entités Partenaires de vérifier le statut du certificat

Les entités partenaires doivent utiliser toutes les ressources que certSIGN met à disposition via son référentiel pour vérifier le statut d'un certificat à tout moment avant de s'y fier. CertSIGN met à jour les OCSP et les CRL en conséquence.

6 Garantie limitée et clause de non-responsabilité/limitation de responsabilité

Dans les limites fixées par la loi roumaine, certSIGN ne sera en aucun cas responsable (sauf en cas de fraude ou de faute intentionnelle) pour :

- Tout manque à gagner ;
- Toute perte de données ;
- Tout dommage indirect, consécutif ou punitif découlant de l'utilisation, de la livraison, de l'octroi de licences et de l'exécution ou de la non-exécution de certificats ou de signatures électroniques ;
- Tout autre dommage.

Nonobstant ce qui précède, si certSIGN n'a pas délivré ou géré le certificat conformément aux exigences de base et à la politique de certification, certSIGN couvrira tout dommage direct aux Bénéficiaires ou aux parties faisant confiance aux certificats pour une réclamation reconnue et prouvée jusqu'à un montant de deux mille dollars US par Bénéficiaire ou Entité Partenaire.

7 Accords applicables, CPP, Politique de certification

certSIGN publie les documents suivants dans le référentiel disponible à l'adresse www.certsign.fr/ressources:

- CPP de **certSIGN ROOT CA G2**
- CPP de **l'AC qualifiee certSIGN**
- CPP de l'**AC publique certSIGN**
- CPP de l'**AC Web certSIGN pour le SSL OV**
- CPP de l'**AC Web certSIGN pour les certificats d'authentification de site Web qualifiés (**QWAC SSL)

8 Politique de confidentialité

Toutes les informations ont été obtenues, stockées et traitées conformément aux lois applicables, en particulier au règlement UE 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et à la loi n° 506/2004 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques. La relation entre un Bénéficiaire, une Entité Partenaire et certSIGN est basée sur la confiance.

9 Politique de remboursement

La politique de remboursement est définie dans la politique de tarification interne. Si un Bénéficiaire ou une Entité Partenaire n'est pas satisfait(e) des services, il/elle peut demander le remboursement de la taxe, uniquement si *certSIGN ne remplit pas ses obligations* et devoirs spécifiés dans l'Accord de Bénéficiaire et dans le présent document et conformément au droit roumain.

10 Droit applicable, plaintes et règlement des litiges

Les lois roumaines régissent l'applicabilité, la construction, l'interprétation et la validité du présent document (sans créer de conflit avec les dispositions légales qui entraîneraient l'application d'autres lois).

11 Licences de dépositaire et de TSA, marques de confiance et audit

L'AC émet des certificats en utilisant les produits développés en interne par certSIGN qui ont été accrédités par l'OTAN (Catalogue OTAN - NIAPC) et par l'Office du Registre National des Informations Secrètes de l'Etat (ORNISS) comme étant capables de protéger les informations CLASSIFIEES.

En fournissant des services fiables, certSIGN détient plusieurs accréditations et certifications. Il s'agit notamment de :

- Webtrust pour les Autorités de certification - menée annuellement par Ernst&Young, cette certification assure aux Entités Partenaires potentielles qu'un professionnel qualifié a évalué les contrôles et les pratiques commerciales de l'Autorité de certification afin de déterminer s'ils sont conformes aux principes et critères WebTrust de l'AICPA/CICA pour les Autorités de certification, et a émis un rapport avec une opinion sans réserve indiquant la conformité avec ces principes.
- ISO/IEC 20000-1, qui certifie que le Système de gestion des services informatiques exploité par certSIGN est conforme à cette norme, pour la fourniture des services suivants : développement et maintenance de logiciels et de systèmes d'information ; cybersécurité (par exemple, réponse et analyse d'incidents, évaluation de vulnérabilité et tests de pénétration, Advanced Threat Intelligence & Correlation) ;
- ISO 9001, qui démontre la mise en œuvre d'un système de gestion de la qualité, qui est le mécanisme qui garantit que certSIGN répond aux besoins des clients et des autres parties prenantes, y compris les activités de formation.
- ISO 27001, qui démontre l'utilisation par l'entreprise d'un Système de gestion de la sécurité de l'information fiable.
- Autorisation de traiter les données personnelles conformément au droit de l'Union européenne (UE) et au droit roumain.
- ISO 14001 démontrant que certSIGN a mis en place et maintient un système de gestion environnementale conforme à cette norme ;
- ISO 18001 démontrant que certSIGN a mis en place et maintient un système de gestion de la santé et de la sécurité en conformité avec cette norme ;