Signature policy (PrivateSeal)

Cette signature policy specifique émane du Service d'encadrement ICT du SPF Justice. Elle s'applique aux signatures par eID non notaires de tous les actes, notariés ou non, déposés par voie électronique.

Le présent document est la version humainement lisible de la signature policy, comme prévu dans ETSI TR 102 041 V1.1.1 [1].

Il renvoie à des documents techniques,

https://signinfo.eda.just.fgov.be/SignaturePolicy/tech/PrivateSeal/BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr_Tech.xml

et

https://signinfo.eda.just.fgov.be/SignaturePolicy/tech/PrivateSeal/BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr_Tech_Ext.xml

,qui contiennent les traductions techniques de ces exigences au format xml.

Un document principal « Signature Policy (*e*DA) » se trouve à l'Url : https://signinfo.eda.just.fgov.be/SignaturePolicy/pdf

1 Signature Policy Issuer Name

Service d'encadrement ICT
SPF Justice
rue Evers 2-8
1000 Bruxelles

email : signature.eda@just.fgov.be
web : https://signinfo.eda.just.fgov.be

2 Signature Policy Identifier

BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr.pdf

Ce document se trouve à l'URL suivante :

https://signinfo.eda.just.fgov.be/SignaturePolicy/pdf/PrivateSeal/BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr.pdf

Il a également été signé électroniquement par le Service d'encadrement ICT du SPF Justice avec une clé privée, dont les certificats correspondant (AAAAMMJJeda.just.fgov.be.crt) se trouvent à l'URL suivante : https://signinfo.eda.just.fgov.be/cert/

Le document ainsi obtenu se trouve sous forme de fichier sur

https://signinfo.eda.just.fgov.be/SignaturePolicy/tech/PrivateSeal/BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr_signed_XAdES-EPES-A.xades

La validation de ce document sera rendue possible grâce à un logiciel du Service d'encadrement ICT du SPF Justice qui sera mis à disposition à l'URL suivante : http://signinfo.eda.just.fgov.be/XAdEScontentViewer.

L'URL de l'algorithme de hachage qui protège cette signature policy est la suivante :

https://www.w3.org/2000/09/xmldsig-more#sha512

La valeur de hachage elle-même se trouve dans le document :

https://signinfo.eda.just.fgov.be/SignaturePolicy/tech/PrivateSeal/BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr.pdf.hash

Pour valider ce hachage :

- sauvegardez le document dans un dossier local sous le nom BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr.pdf
- installez le logiciel openssl disponible pour tous les systèmes d'exploitation modernes (voir http://www.openssl.org).
- sur *nix, exécutez le fichier suivant dans le répertoire dans lequel vous avez sauvegardé la policy :
  cat BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.11_202111_Fr.pdf | openssl dgst -sha512
- si la valeur du hachage obtenu qui s'affiche correspond à la valeur de hachage dont question plus haut, vous pouvez être sûr que le document n'a pas été modifié depuis sa publication sur le site web. Cette valeur fait obligatoirement partie de l'élément « SignaturePolicyIdentifier » de chaque dépôt électronique.

3 Signing Period

start date	: 08-11-2021	end date	: 08-11-2026
start time	: 01:00 GMT	end time	: 08:00 GMT

4 Date of issue

08/11/2021

5 Field of application

Cette signature policy est applicable aux signature par eID non-notaire lors de tout dépôt effectué après la date de début de la « signing period » et ce, pour tout dépôt, notarié ou non, de documents signés électroniquement auprès des Tribunaux de l'entreprise. La version de cette policy spécifique aux signatures s'appliquera aux signatures qui référence la dite version au moyen du SignaturePolicyIdentifier explicite et aux documents qui sont signés par ces signatures.

Historique des documents précédents :

- Un première version (1) BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.1_200812_Fr.pdf version corrigée de la première(1) avec des nouveaux trust-points
- Une deuxième version (2) BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.3_201101_Fr.pdf version corrigée de la première(1) avec des nouveaux trust-points
- Une troisième version (3) BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.4a_201109_Fr.pdf version corrigée de la première(1) avec des nouveaux trust-points
- Une quatrième version (4), BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.4c_201404_Fr.pdf ajout des CA3 et CA4, comme trust-points.
- Une cinquième version (5), BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.5_201512_Fr.pdf renouvellement.
- Une sixième (6), BE_Justice_Signature_Policy_PrivateSeal_Hum_v0.8_202011_Fr.pdf, renouvellement, Tribunaux de Commerce → Tribunaux de l'entreprise, Trustpoint TSS et AnnexeRefs.
- 202107 : (7), Nouvelle eID, Algorithmes EC, Belgium Root CA6.
- 202110 : (8) ce document, Fedict/Bosa TSS → Bosa QTSS pour Timestamp.

6 Signature Validation

Les règles qui seront utilisées pour confirmer la validité de la signature sont fixées dans la « signature validation policy ». Nous décrivons en premier lieu les règles de validation qui s'appliquent aux dépôts effectués aussi bien par des notaires que par des citoyens.

7 Common Rules

7.1 SSCD

Le dépositaire doit utiliser un SSCD (« Secure Signature Creation Device »).

7.2 Caractères de mot de passe

Lorsque le code pin qui protège la private key est introduit, le logiciel utilisé ne peut le faire apparaître à l'écran que sous la forme non lisible de « caractères de mot de passe » (par exemple *).

7.3 Standard XAdES

Les documents déposés aux greffes des Tribunaux de l'entreprise sous forme électronique doivent satisfaire au standard XAdES version 1.3.2. Plus précisément, les citoyens doivent déposer les documents au format XAdES-EPES et les notaires, au format XAdES-XL. Dans les deux cas, il y a lieu de se référer, pour la signature policy, au présent document (via un SignaturePolicyIdentifier explicite).

7.4 TimeStampTrustCondition

Aucune « caution period » n'est exigée, mais un « timestamp delay » d'un jour maximum. Il s'agit du délai maximal

acceptable entre le moment de la signature indiqué par le signataire et le moment où la marque de date, contenue dans l'élément « SignatureTimeStamp », a été apposée.

8 Règles spécifiques pour le dépôt d'actes notariés

Voir Notary Policy

9 Règles spécifiques pour le dépôt d'actes non-notariés

9.1 SignerAndVerifierRules (Citizen eID signature)

Il s'agit, d'une part, de signerRules et, d'autre part, de verifierRules.

9.1.1 Signer Rules

9.1.1.1 MandatedSignatureProperties

Il s'agit d'éléments obligatoires au niveau de la signature éléctronique :

- L'élément keyInfo contiendra le certificate path et donc au moins 3 certificats, dont le dernier sera un des trust-points (cfr 9.2.1).

9.1.1.2 MandatedSignedProperties

Il s'agit des éléments du document déposé dont la protection au moyen d'une signature électronique est nécessaire :

- <xades:Reference URI="#D{x}"> : un élément de référence qui doit renvoyer à l'élément qui contient les données au format base 64. Le {x} doit être alternativement remplacé par un numéro d'ordre ascendant (0, 1, 2,…) jusqu'au nombre correspondant au nombre de fichiers (= nombre d'éléments déposés de type « <just:DataFile....</just:DataFile> ») moins un.
- <xades:Reference URI="#prop{x}"> : un élément de référence qui doit renvoyer à un élément qui contient les propriétés « signées ». Le {x} doit être remplacé par un numéro d'ordre (0, 1, 2,…) qui correspond au numéro d'ordre de la signature électronique à laquelle cette référence appartient (par exemple, 1 dans le cas où la référence appartient à l'élément « <xades:Signature Id="S1"> »). Ces propriétés signées doivent comprendre au moins :
  - SigningTime
  - SigningCertificate
  - SignaturePolicyIdentifier

9.1.1.3 mandatedUnsignedProperties.

Il s'agit des éléments du document déposé qui doivent obligatoirement être présents après la signature mais qui ne contribuent pas au calcul de la SignatureValue. Pas éléments de ce type obligatoires

9.1.2 Verifier Rules

Les verifier rules identifient les caractères non signés qui doivent être introduits par le responsable de la vérification lorsque ceux-ci n'ont pas été introduits par le signataire. Pour les dépôts effectués par les citoyens, les éléments suivants devront obligatoirement être ajoutés par le Service d'encadrement ICT du SPF Justice :

- SignatureTimeStamp
- CompleteCertificateRefs
- CompleteRevocationRefs
- SigAndRefsTimeStamp
- RevocationValues
- CertificateValues

De plus, les signerRules sont à nouveau validées, et les VerifierRules sont validées lorsqu'elles sont présentes.

9.2 Exigences de certificat et de révocation

9.2.1 Exigences de certificat

Les certificateTrustTrees identifient une série de certificats « auto-signés » des trust points utilisés pour commencer (terminer) la vérification du chemin d'accès du certificat. Des certificats sont spécifiés dans cette policy comme trust-points :

9.2.1.1 Certificat(s) A : Signing

- Cfr .http://repository.eid.belgium.be/ , http://repository.pki.belgium.be/ & https://repository.eidpki.belgium.be

9.2.1.1.1. Certificat CA root signed:

=> serial number : 04:00:00:00:00:00:f3:00:72:c4:a7

=> Issuer=Subject : C=BE, CN=Belgium Root CA


```
-----BEGIN CERTIFICATE-----
MIID+zCCAuOgAwIBAgILBAAAAAAA8wByxKcwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0wMzAxMjYyMzAw
MDBaFw0xNDAxMjYyMzAwMDBaMCcxCzAJBgNVBAYTAkJFMRgwFgYDVQQDEw9CZWxn
aXVtIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDIoXHp
HEZCeXhxb52uqairKLdNxyDrMJFadfXi0s/ITBSYQlitxxHFQEBqWvl0EieH6Zzl
cU4iLNESGKowXqIhudm7//Z06zEB5zt+WA+RFk12iagBT60iZnD6Sx2VwTBY6rzZ
ZdiatIjrSUZS39JTFXbLFF0ZSbFvatPT/bzCLexFPwk/WL78lO8AjIE1cr/3GOqW
Yn0rKH8VbGPSysp9BazIbQdtMr5uAVArlSYVj5m8TDo78Srk14H3jKPEnSqWzQj
VMDqbM7+NpKoCRfqoS3PbOOEHd6HLjMLPHTiIVA4lS5c4OXGMfnbQPpqoaSKk5un
IQaHHSfTxKHJTLBvAgMBAAGjgfcwgfQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB
/wQFMAMBAf8wHQYDVR0OBBYEFBDwDFabYepXOrY1l22f3bkUjtvmMEIGA1UdIAQ7
MDkwNwYFYDgBAQEwLjAsBggrBgEFBQcCARYgaHR0cDovL3JlcG9zaXRvcnkuZWlk
LmJlbGdpdW0uYmUwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL3NlY3VyZS5nbG9i
YWxzaWduLm5ldC9jcmwvcm9vdC5jcmwwEQYJYIZIAYb4QgEBBAQDAgAHMB8GA1Ud
IwQYMBaAFGB7ZhpFDZfKiVAvfQTNNKj//P1LMA0GCSqGSIb3DQEBBQUAA4IBAQA2
SSGBsGqTTSUrbh7wb9IzoUpsjiiC6qFf3NMiwknXNBhwHSIW+nxrEVsrxywPyj1o
Uf4H8cq743lLdpryGB+4XAdX38vcWFSAOdtyZRV82oDwgSgJ0sVuEFl9WF3W+yzg
lzIJwQ/d1j2PwU1H0c7qnijubf10QgQNF0DmHbQnF4IG4+feQrEo7RqvPSo+5jH/
oNMjUcfG4yhT8Go4HNzDJIanzztkq25fXqdS2Q53/iswZTYmUhxPPhoL7wJkj3Gg
m1GQeauVv9Frka0M8+zkHvuPnpWBxwNo+yjCkm3+i6jk8sqth2KruXxt6w9TdvHn
Vd5WnMUdmEjPK5Rm6Rfv
-----END CERTIFICATE-----
```


9.2.1.1.2. Certificat CA self signed:

=> serial number : 58:0b:05:6c:53:24:db:b2:50:57:18:5f:f9:e5:a6:50

=> Issuer=Subject : C=BE, CN=Belgium Root CA


```
-----BEGIN CERTIFICATE-----
MIIDlDCCAnygAwIBAgIQWAsFbFMk27JQVxhf+eWmUDANBgkqhkiG9w0BAQUFADAn
MQswCQYDVQQGEwJCRTEYMBYGA1UEAxMPQmVsZ2l1bSBSb290IENBMB4XDTAzMDEy
NjIzMDAwMFoXDTE0MDEyNjIzMDAwMFowJzELMAkGA1UEBhMCQkUxGDAWBgNVBAMT
D0JlbGdpdW0gUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMihcekcRkJ5eHFvna6pqKsot03HIOswkVp19eLSz8hMFJhCWK3HEcVAQGpa+XQS
J4fpnOVxTiIs0RIYqjBeoiG52bv/9nTrMQHnO35YD5EWTXaJqAFPrSJmcPpLHZXB
MFjqvNll2Jq0iOtJRlLf0lMVdssUXRlJsW9q09P9vMIt7EU/CT9YvvzU7wCMgTVy
v/cY6pZifSsofxVsY9LKyn0FrMhtB20yvmi4BUCuVJhWPmbxMOjvxKuTXgfeMo8S
dKpbNCNUwOpszv42kqgJF+qhLc9s44Qd3ocuMws8dOIhUDiVLlzg5cYx+dtA+mqh
pIqTm6chBocdJ9PEoclMsG8CAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYD
VR0TAQH/BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4AQEBMC4wLAYIKwYBBQUHAgEW
IGh0dHA6Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBQQ8AxW
m2HqVzq2NZdtn925FI7b5jARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAU
EPAMVpth6lc6tjWXbZ/duRSO2+YwDQYJKoZIhvcNAQEFBQADggEBAMhtIlGKYfgP
lm7VILKB+MbcoxYA2s1q52sq+llIp0xJN9dzoWoBZV4yveeX09AuPHPTjHuD79ZC
wT+oqV0PN7p20kC9zC0/00RBSZz9Wyn0AiMiW3Ebv1jZKE4tRfTa57VjRUQRDSp/
M382SbTObqkCMa5c/ciJv0J71/Fg8teH9lcuen5qE4Ad3OPQYx49cTGxYNSeCMqr
8JTHSHVUgfMbrXec6LKP24OsjzRr6L/D2fVDw2RV6xq9NoY2uiGMlxoh1OotO6y6
7Kcdq765Sps1LxxcHVGnH1TtEpf/8m6HfUbJdNbv6z195lluBpQE5KJVhzgoaiJe
4r50ErAEQyo=
-----END CERTIFICATE-----
```


9.2.1.1.3. Certificat CA2 root signed:

=> serial number : 04:00:00:00:00:01:15:6a:b1:aa:7e

=> Issuer=Subject : C=BE, CN=Belgium Root CA2


```
-----BEGIN CERTIFICATE-----
MIID/TCCAuWgAwIBAgILBAAAAABFWqxqn4wDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0wNzEwMDQxMjAw
MDBaFw0xNDAxMjYyMzAwMDBaMCgxCzAJBgNVBAYTAkJFMRkwFwYDVQQDExBCZWxn
aXVtIFJvb3QgQ0EyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxnNC
HpL/dQ+Lv3SGpz/tshgtLZf5qfuYSiPf1Y3gjMYyHBYtB0LWLbZuL6f1/MaFgl2V
3rUiAMyoU0Cfrwo1onrH4cr3YBBnDqdQcxdTlZ8inwxdb7ZBvIzr2h1GvaeUv/Ma
y9T7jQ4eM8iW1+yMU96THjQeilBxJli0XcKIidpg0okhP97XARg2buEscAMEZe+Y
BitdHmLcVWv+ZmQhX/gv4debKa9vzZ+qDEbRiMWdopWfrD8VrvJh3+/Da5oi2Cxx
/Vgd7ACkOCCVWsfVN2O6T5uq/lZGLmPZCyPVivq1I/CJG6EUDSbaQfA4jzDtBSZ5
wUtOobh+VVI6aUaEdQIDAQABo4H4MIH1MA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMB
Af8EBTADAQH/MB0GA1UdDgQWBBSFiuv0xbu+DlkDlN7WgAEV4xCcOTBDBgNVHSAE
PDA6MDgGBWA4CQEBMC8wLQYIKwYBBQUHAgEWIWh0dHA6Ly9yZXBvc2l0b3J5LmVp
ZC5iZWxnaXVtLmJlIDA6BgNVHR8EMzAxMC+gLaArhilodHRwOi8vc2VjdXJlLmds
b2JhbHNpZ24ubmV0L2NybC9yb290LmNybDARBglghkgBhvhCAQEEBAMCAAcwHwYD
VR0jBBgwFoAUYHtmGkUNl8qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEB
AH1t5NWhYEwrNe6NfOyI0orfIiEoy13BB5w214IoqfGSTivFMZBI2FQeBOquBXko
```

B253FXQq+mmZMlIl5qn0qprUQKQlicA2cSm0UgBe7SlIQkkxFusl1AgVdjk6oeNk
HqxZs+J1SLy0NofzDA+F8BWy4AVSPujQ6x1GK70FdGmea/h9anxodOyPLAvWEckP
FxavtvTuxwAjBTfdGB6Z6DvQBq0LtljcrLyojA9uwVDSvcwOTZK5lcTV54aE6KZW
X2DapbDi2KY/oL6HfhOiDh+OPqa3YXzvCesY/h5v0RerHFFk49+ItSJryzwRcvYu
zk1zYQL5ZykZc/PkVRV3HWE=
-----END CERTIFICATE-----

9.2.1.1.4. Certificat CA2 self signed:

=> serial number : 2a:ff:be:9f:a2:f0:e9:87

=> Issuer=Subject : C=BE, CN=Belgium Root CA2

-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIIKv++n6Lw6YcwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTIwHhcNMDcxMDA0MTAwMDAw
WhcNMjExMjE1MDgwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMZzQh6S
/3UPi790hqc/7bIYLS2X+an7mEoj39WN4IzGMhwWLQdC1i22bi+n9fzGhYJdld61
IgDMqFNAn68KNaJ6x+HK92AQZw6nUHMXU5WfIp8MXW+2QbyM69odRr2nlL/zGsvU
+40OHjPlltfsjFPekx40HopQcSZYtF3CiInaYNKJIT/e1wEYNm7hLHADBGXvmAYr
XR5i3FVr/mZkIV/4L+HXmymvb82fqgxG0YjFnaKVn6w/Fa7yYd/vw2uaItgscf1Y
HewApDgglVrH1Tdjuk+bqv5WRi5j2Qsj1Yr6tSPwiRuhFA0m2kHwOI8w7QUmecFL
TqG4flVSOmlGhHUCAwEAAaOBuzCBuDAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/
BAUwAwEB/zBCBgNVHSAEOzA5MDcGBWA4CQEBMC4wLAYIKwYBBQUHAgEWIGh0dHA6
Ly9yZXBvc2l0b3J5LmVpZC5iZWxnaXVtLmJlMB0GA1UdDgQWBBSFiuv0xbu+DlkD
lN7WgAEV4xCcOTARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAUhYrr9MW7
vg5ZA5Te1oABFeMQnDkwDQYJKoZIhvcNAQEFBQADggEBAFHYhd27V2/MoGyloyCc
UwnzSgEMdL8rs5qauhjyC4isHLMzr87lEwEnkoRYmhC598wUkmt0FoqW6FHvv/pK
JaeJtmMrXZRY0c8RcrYeuTlBFk0pvDVTC9rejg7NqZV3JcqUWumyaa7YwBO+mPyW
nIR/VRPmPIfjvCCkpDZoa01gZhz5v6yAlGYuuUGK02XThIAC71AdXkbc98m6tTR8
KvPG2F9fVJ3bTc0R5/0UAoNmXsimABKgX77OFP67H6dh96tK8QYUn8pJQsKpvO2F
sauBQeYNxUJpU4c5nUwfAA4+Bw11V0SoU7Q2dmSZ3G7rPUZuFF1eR1ONeE3gJ7uO
hXY=
-----END CERTIFICATE-----

9.2.1.1.5. GlobalSign Certificat CA self signed:

=> serial number : 02:00:00:00:00:00:d6:78:b7:94:05

=> Issuer=Subject : C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILAgAAAAAA1ni3lAUwDQYJKoZIhvcNAQEEBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0xNDAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIABjAdBgNVHQ4EFgQU
YHtmGkUNl8qJUC99BM00qP/8/UswDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0B
AQQFAAOCAQEArqqf/Lf5yx9fOSkoGJ40yWxPbxrwZKJwSk8ThptgKJ7ogUmYfQq7
5bCdPTbbjwVR/wkxKh/diXeeDy5slQTthsu0AD+EAk2AaioteAuubyuig0SDH81Q
gkwkr733pbTIWg/050deSY43lv6aiAU62cDbKYfmGZZHpzqmjIs8d/5GY6dT2iHR
rH5Jokvmw2dZL7OKDrssvamqQnw1wdh/1acxOk5jQzmvCLBhNIzTmKlDNPYPhyk7
ncJWWJh3w/cbrPad+D6qp1RF8PX51TFl/mtYnHGzHtdS6jIX/EBgHcl5JLL2bP2o
Zg6C3ZjL2sJETy6ge/L3ayx2EYRGinij4w==
-----END CERTIFICATE-----

9.2.1.1.6. GlobalSign Certificat CA2 self signed:

=> serial number : 04:00:00:00:00:01:15:4b:5a:c3:94

=> Issuer=Subject : C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw
MDBaFw0yODAxMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz8kHp
1Wrjsok6Vjk4bwY8iGlbKk3Fp1S4bInMm/k8yuX9ifUSPJJ4ltbcdG6TRGHRjcdG
snUOhugZitVtbNV4FpWi6cgKOOvyJBNPc1STE4U6G7weNLWLBYy5d4ux2x8gkasJ
U26Qzns3dLlwR5EiUWMWea6xrkEmCMgZK9FGqkjWZCrXgzT/LCrBbBlDSgeF59N8
9iFo7+ryUp9/k5DPAgMBAAGjQjBAMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8E
BTADAQH/MB0GA1UdDgQWBBRge2YaRQ2XyolQL30EzTSo//z9SzANBgkqhkiG9w0B
AQUFAAOCAQEA1nPnfE920I2/7LqivjTFKDK1fPxsnCwrvQmeU79rXqoRSLblCKOz
yj1hTdNGCbM+w6DjY1Ub8rrvrTnhQ7k4o+YviiY776BQVvnGCv04zcQLcFGUl5gE
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----

9.2.1.1.7. Belgium Root CA3 self signed:

=> serial number : 3b:21:02:de:96:5b:1d:a9

=> Issuer=Subject : C=BE, CN=Belgium Root CA3

-----BEGIN CERTIFICATE-----
MIIFjjCCA3agAwIBAgIIOyEC3pZbHakwDQYJKoZIhvcNAQEFBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTMwHhcNMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBMzCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAKjyAZ2L
g8kHoIX7JLc3BeZ1Tzy9MEv7Bnr59xcJezc/xJJdO4V3bwMltKFfNvqsQ5H/GQAD
FJ0GmTLLPDI5AoeUjBubRZ9hwruUuQ11+vhtoVhuEuZUxofEIU2yJtiSOONwpo/G


```
Ib9C4YZ5h+7ltDpC3MvsFyyordpzgwqSHvFwTCmls5SpU05UbF7ZVPcfVf24A5Ig
HLpZTgQfAvnzPlm++eJY+sNoNzTBoe6iZphmPbxuPNcJ6slV8qMQQk50/g+KmoPp
HX4AvoTr4/7TMTvuK8jS1dEn+fdVKdx9qo9ZZRHFW/TXEn5SrNUu99xhzlE/WBur
rVwFoKCWCjmO0CnekJlw0NTr3HBTG5D4AiDjNFUYaIcGJk/ha9rzHzY+WpGdoFZx
hbP83ZGeoqkgBr8UzfOFCY8cyUN2db6hpIaK6Nuoho6QWnn+TSNh5Hjui5miqpGx
S73gYlT2Qww16h8gFTJQ49fiS+QHlwRw5cqFuqfFLE3nFFF9KIamS4TSe7T4dNGY
2VbHzpaGVT4wy+fl7gWsfaUkvhM4b00DzgDiJ9BHiKytNLmzoa3Sneij/CKur0dJ
5OdMiAqUpSd0Oe8pdIbmQm1oP5cjckiQjxx7+vSxWtacpGowWK8+7oEsYc+7fLt3
GD6q/O5Xi440Pd/sFJmfqRf3C1PPMdBqXcwjAgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVgOAoBATAuMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS5laWQuYmVsZ2llbS5iZTAdBgNV
HQ4EFgQUuLxsAI9bGYWdJQGc8BncQI7QOCswEQYJYIZIAYb4QgEBBAQDAgAHMB8G
A1UdIwQYMBaAFLi8bACPWxmFnSUBnPAZ3ECO0DgrMA0GCSqGSIb3DQEBBQUAA4IC
AQBFYjv/mKX+VcyxEacckgx4L8XvFkIFPXzjEnDnAtCCkROU/k5n1jjVK+ODOn+Q
4kJg6Nd7K47+zTXcrSe1tB2gVMsyaCN9scy4phLX1qT48sThCjUtooxfIoRycpdl
f14HcUPCYlASTCapZU0MnAbzfpzxm49Ik/A2JWxAhxXVRHwOu3TMGiQ4W/VyVawx
jwQMO8TneBDombmkXsI9bI0OxWUh2A5dKlqu0sYvE0dz8xDxr9ZkmZqYcPIKizCZ
laP1ZsSlCi5S31gn3EUP+fd21q6ZXgU+50/qgoh/0UUaHRpedPQBES/FYc2IQZ2X
jhmeTwM+9Lk7tnzHeHp3dgCoOfceyPUaVkWiXMWcNAvvkDVELvXfJpRxwcRfS5Ks
5oafOfj81RzGUbmpwl2usOeCRwdWE8gPvbfWNQQC8MJquDl5HdeuzUesTXUqXeEk
yAOo6YnF3g0qGcLI9NXusji1egRUZ7B4XCvG52lTB7Wgd/wVFzS3f4mAmYTGJXH+
N/lrBBGKuTJ5XncJaliFUKxGP6VmNyaaLUF5IlTqC9CGHPLSXOgDokt2G9pNwFm2
t7AcpwAmegkMNpgcgTd+qk2yljEaT8wf953jUAFedbpN3tX/3i+uvHOOmWjQOxJg
2lVKkC+bkWa2FrTBDdrlEWVaLrY+M+xeIctrC0WnP7u4xg==
-----END CERTIFICATE-----
```


9.2.1.1.8. Belgium Root CA4 self signed:

=> serial number : 4f:33:20:8c:c5:94:bf:38

=> Issuer=Subject : C=BE, CN=Belgium Root CA4


```
-----BEGIN CERTIFICATE-----
MIIFjjCCA3agAwIBAgIITzMgjMWUvzgwDQYJKoZIhvcNAQELBQAwKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTQwHhcNMTMwNjI2MTIwMDAw
WhcNMjgwMTI4MTIwMDAwWjAoMQswCQYDVQQGEwJCRTEZMBcGA1UEAxMQQmVsZ2l1
bSBSb290IENBNDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJiQrvrH
Hm+O4AU6syN4TNHWL911PFsY6E9euwVml5NAWTdw9p2mcmEOYGx424jFLpSQVNxx
xoh3LsIpdWUMRQfuiDqzvZx/4dCBaeKL/AMRJuL1d6wU73XKSkdDr5uH6H2Yf19z
SiUOm2x4k3aNLyT+VryF11b1Prp67CBk63OBmG0WUaB+ExtBHOkfPaHRHFA04Mig
oVFt3gLQRGh1V+H1rm1hydTzd6zzpoJHp3ujWD4r4kLCrxVFV0QZ44usvAPlhKoe
cF0feiKtegS1pS+FjGHA9S85yxZknEV8N6bbK5YP7kgNLDDCNFJ6G7MMpf8MEygX
WMb+WrynTetWnIV6jTzZA1RmaZuqmIMDvWTA7JNkiDJQOJBWQ3Ehp+Vn7li1MCIj
XlEDYJ2wRmcRZQ0bsUzaM/V3p+Q+j8S3osma3Pc6+dDzxL+Og/lnRnLlDapXx28X
B9urUR5H03Ozm77B9/mYgIeM8Y1XntlCCELBeuJeEYJUqc0FsGxWNwjsBtRoZ4dv
a1rvzkXmjJuNIR4YILg8G4kKLhr9JDrtyCkvI9Xm8GDjqOIJ2KpQiJHBLJA0gKxl
Yem8CSO/an3AOxqTNZjWbQx6E32OPB/rsU28ldadi9c8yeRyXLWpUF4Ghjyoc4Od
rAkXmljnkzLMC459xGL8gj6LyNb6UzX0eYA9AgMBAAGjgbswgbgwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wQgYDVR0gBDswOTA3BgVgOAwBATAuMCwG
CCsGAQUFBwIBFiBodHRwOi8vcmVwb3NpdG9yeS5laWQuYmVsZ2llbS5iZTAdBgNV
HQ4EFgQUZ+jxTk+ztfMHbwicDIPZetlb50kwEQYJYIZIAYb4QgEBBAQDAgAHMB8G
A1UdIwQYMBaAFGfo8U5Ps7XzB28InAyD2XrZW+dJMA0GCSqGSIb3DQEBCwUAA4IC
AQAliTyrUcumj9h1IRKZNIKlt2hAyNW1jdkYz+fJ57PDOqtpsvmfoZmuP+6rSbhD
i1J9pfi7Yc9fIDwxGwfkiPJAiRBllaxdtpnkoAMEcxQonLnxMiS6/n6nQqIXpb0O
34YAYANJn5Lujd5V9I+iv5rrzXjvcZPNxgEB3x6fJdpVapbokhgrDrg1g7XqEY+J
YiJPmv7dXIzhZ6lN29foBzoik1o6Wp4UnC4UsFTgx/hN56cjkdXMCR9JHQMWmcCz
kk2ZUN2SPYL14xK3dCHAdPclmjVoUSZoyXEoHM14FTvV1Ode1UCJB/EE0l9M8HQa
pVXIUhSmqO1R+A3RD8cvjP9P5FDoxCmeGTrqcXKIj1qWs7gsrXZ0yDCs7HyST5/o
M+GQ9OLhU9wrH4cMwW8NsORyCqZqeghSbd5hE+Almj4SmxjPht7krtQXRGebf5o6
q+RLHXnFCzBtqJeA6U6Apr1SrSvEpkOXLIVs2nt8o/YpAoUMxOrwPRwbjqfl0UUS
6IvKZhALeMBe6GvXpMiTqmlta7cD13yKJQBAvzuE3QJMPY0XAis6CWA3zUVbznuQ
2Vtk0MBtlQEb+w3OsUh4eIg/AkONJ4/24AFfOzklmB7k93t7Xa/YuVWb8go37wtq
/A9HvFieImuusfghZ6EU9pvUPmL62NPY54g+nFm2qMtMWQ==
-----END CERTIFICATE-----
```


9.2.1.1.9. C=BE, CN=Belgium Root CA2

=> serial number : 04:00:00:00:00:01:41:a1:e1:34:ba

=> Issuer=Subject : C=BE, CN=Belgium Root CA2


```
-----BEGIN CERTIFICATE-----
MIID7jCCAtagAwIBAgILBAAAAAABQaHhNLowDQYJKoZIhvcNAQEFBQAwOzEYMBYG
A1UEChMPQ3liZXJ0cnVzdCwgSW5jMR8wHQYDVQQDExZDeWJlcnRydXN0IEdsb2Jh
bCBSb290MB4XDTEzMTAxMDExMDAwMFoXDTI1MDUxMjIyNTkwMFowKDELMAkGA1UE
BhMCQkUxGTAXBgNVBAMTEEJlbGdpdW0gUm9vdCBDQTIwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDGc0Iekv91D4u/dIanP+2yGC0tl/mp+5hKI9/VjeCM
xjIcFi0HQtYttm4vp/X8xoWCXZXetSIAzKhTQJ+vCjWiesfhyvdgEGcOp1BzF1OV
nyKfDF1vtkG8j0vaHUa9p5S/8xrL1PuNDh4zyJbX7IxT3pMeNB6KUHEmWLRdwoiJ
2mDSiSE/3tcBGDZu4SxwAwRl75gGK10eYtxVa/5mZCFf+C/h15spr2/Nn6oMRtGI
xZ2ilZ+sPxWu8mHf78NrmiLYLHH9WB3sAKQ4IJVax9U3Y7pPm6r+VkYuY9kLI9WK
+rUj8IkboRQNJtpB8DiPMO0FJnnBS06huH5VUjppRoR1AgMBAAGjggEEMIIBADAO
BgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBATBQBgNVHSAESTBHMEUG
CisGAQQBsT4BZAEwNzA1BggrBgEFBQcCARYpaHR0cDovL2N5YmVydHJ1c3Qub21u
aXJvb3QuY29tL3JlcG9zaXRvcnkwHQYDVR0OBBYEFIWK6/TFu74OWQOU3taAARXj
EJw5MDUGA1UdHwQuMCwwKqAooCaGJGh0dHA6Ly9jcmwub21uaXJvb3QuY29tL2N0
Z2xvYmFsLmNybDARBglghkgBhvhCAQEEBAMCAAcwHwYDVR0jBBgwFoAUtgh7DXrM
rCBMhlYyXs+rboUtcFcwDQYJKoZIhvcNAQEFBQADggEBALLLOUcpFHXrT8gK9htq
XI8dV3LlSAooOqLkn+yRRxt/zS9Y0X0opocf56Kjdu+c2dgw6Ph3xE/ytMT5cu/6
0jT17BTk2MFkQhoAJbM/KIGmvu4ISDGdeobiBtSeiyzRb9JR6JSuuM3LvQp1n0fh
sA5HlibT5rFrKi7Oi1luDbc4eAp09nPhAdcgUkRU9o/aAJLAJho3Zu9uSbw5yHW3
PRGnmfSO67mwsnSDVswudPrZEkCnSHq/jwOBXAWCYVu5bru3rCdojd5qCTn/Wyqb
ZdsgLAPR5Vmf/uG3d5HxTO1LLX1Zyp9iANuG32+nFusi89shA1GPDKWacEm0ASd8
iaU=
-----END CERTIFICATE-----
```


9.2.1.1.10. O=Cybertrust, Inc, CN=Cybertrust Global Root

=> serial number : 120009509 (0x7273325)

=> Issuer=Subject : O=Cybertrust, Inc, CN=Cybertrust Global Root


```
-----BEGIN CERTIFICATE-----
MIIECDCCAvCgAwIBAgIEByczJTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJJ
RTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYD
VQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTEwMDgxODE5MTE1MloX
DTIwMDgxODE5MTEwNlowOzEYMBYGA1UEChMPQ3liZXJ0cnVzdCwgSW5jMR8wHQYD
VQQDExZDeWJlcnRydXN0IEdsb2JhbCBSb290MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA+Mi8vRRQZhP/8NN57CPytxrHjoXxEnOmGaoQ25yiZXRadz5R
```


```
fVb23CO21O1fWLE3TdVJDm71aofW0ozSJ8bi/zafmGWgE07GKmSb1ZASzxQG9Dvj
1Ci+6A74q05IlG2OlTEQXO2iLb3VOm2yHLtgwEZLAfVJrn5GitB0jaEMAs7u/OeP
uGtm839EAL9mJRQr3RAwHQeWP032a7iPt3sMpTjr3kfb1V05/Iin89cqdPHoWqI7
n1C6poxFNcJQZZXcY4Lv3b93TZxiyWNzFtApD0mpSPCzqrdsxacwOUBdrsTiXSZT
8M4cIwhhqJQZugRiQOwfOHB3EgZxpzAYXSUnpQIDAQABo4H0MIHxMBIGA1UdEwEB
/wQIMAYBAf8CAQIwSgYDVR0gBEMwQTA/BgRVHSAAMDcwNQYIKwYBBQUHAgEWKWh0
dHA6Ly9jeWJlcnRydXN0Lm9tbmlyb290LmNvbS9yZXBvc2l0b3J5MAsGA1UdDwQE
AwIBBjAfBgNVHSMEGDAWgBTlnVkwgkdYzKz6CFQ2hns6tQRN8DBCBgNVHR8EOzA5
MDegNaAzhjFodHRwOi8vY2RwMS5wdWJsaWMtdHJ1c3QuY29tL0NSTC9PbW5pcm9v
dDIwMjUuY3JsMB0GA1UdDgQWBBS2CHsNesysIEyGVjJez6tuhS1wVzANBgkqhkiG
9w0BAQUFAAOCAQEAE26SCV2/KTgw6nYB6hfb6KI2EKycTynAOao331vsgBs499Zm
rTA8FCGqxfg7UdQ6RQnWCZ0ybp2lzq8NL4rmO/SNtKmSpjYNNfVERR5OeLnCOTmq
pJQpOEivmYN9lPFdeIgmglCmGcHEqvWRlo8SV7uyPvii0MxHmcoBV5vdW8UqnOP8
5ryHb6ON/d3XeYrzTx9f7eLq8VWPH+b145oMTA6dO0vJOyHtB0i1xoU8hAsrTm6P
bqjnuSmToOTuh0lx3ne3Xz1UpqoGzUvg2KvLsQ80qiTYdDnFwQTPX2TJkgrrqh0f
5nF32+sVXvGYDnhZ72qv4U9/OAar5O9EvaUHvQ==
-----END CERTIFICATE-----
```


9.2.1.1.11. C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root

=> serial number : 33554617 (0x20000b9)

=> Issuer=Subject : C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root


```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJJ
RTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYD
VQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTAwMDUxMjE4NDYwMFoX
DTI1MDUxMjIzNTkwMFowWjELMAkGA1UEBhMCSUUxEjAQBgNVBAoTCUJhbHRpbW9y
ZTETMBEGA1UECxMKQ3liZXJUcnVzdDEiMCAGA1UEAxMZQmFsdGltb3JlIEN5YmVy
VHJ1c3QgUm9vdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKMEuyKr
mD1X6CZymrV51Cni4eiVgLGw41uOKymaZN+hXe2wCQVt2yguzmKiYv60iNoS6zjr
IZ3AQSsBUnuId9Mcj8e6uYi1agnnc+gRQKfRzMpijS3ljwumUNKoUMMo6vWrJYeK
mpYcqWe4PwzV9/lSEy/CG9VwcPCPwBLKBsua4dnKM3p31vjsufFoREJIE9LAwqSu
XmD+tqYF/LTdB1kC1FkYmGP1pWPgkAx9XbIGevOF6uvUA65ehD5f/xXtabz5OTZy
dc93Uk3zyZAsuT3lySNTPx8kmCFcB5kpvcY67Oduhjprl3RjM7loGDHweI12v/ye
jl0qhqdNkNwnGjkCAwEAAaNFMEMwHQYDVR0OBBYEFOWdWTCCR1jMrPoIVDaGezq1
BE3wMBIGA1UdEwEB/wQIMAYBAf8CAQMwDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3
DQEBBQUAA4IBAQCFDF2O5G9RaEIFoN27TyclhAO992T9Ldcw46QQF+vaKSm2eT92
9hkTI7gQCvlYpNRhcL0EYWoSihfVCr3FvDB81ukMJY2GQE/szKN+OMY3EU/t3Wgx
jkzSswF07r51XgdIGn9w/xZchMB5hbgF/X++ZRGjD8ACtPhSNzkE1akxehi/oCr0
Epn3o0WC4zxe9Z2etciefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----
```


9.2.1.1.12. C=BE, CN=Belgium Root CA6

=> serial number : 71:8b:57:ff:6b:69:3e:5a:1c:23:5e:d8:87:a3:ef:51:f4:01:0f:26

=> Issuer=Subject : C=BE, CN=Belgium Root CA6


```
-----BEGIN CERTIFICATE-----
MIIDaDCCAu2gAwIBAgIUcYtX/2tpPlocI17Yh6PvUfQBDyYwCgYIKoZIzj0EAwMw
geAxCzAJBgNVBAYTAkJFMREwDwYDVQQHDAhCcnVzc2VsczEwMC4GA1UECgwnS2lu
Z2RvbSBvZiBCZWxnaXVtIC0gRmVkZXJhbCBHb3lcm5tZW50MTYwNAYDVQQLDC1G
UFMgSG9tZSBBZmZhaXJzIC0gQklLLUdDSSAoTlRSQkUtMDM2MjQ3NTUzOCkxOTA3
BgNVBAsMMEZQUyBQb2xpY3kgYW5kIFN1cHBvcnQgLSBCT1NBIChOVFJCRS0wNjcx
NTE2NjQ3KTEZMBcGA1UEAwwQQmVsZ2lbSBSb290IENBNjAeFw0yMDA2MDMxMDAx
MzFaFw00MDA2MDMxMDAxMzFaMIHgMQswCQYDVQQGEwJCRTERMA8GA1UEBwwIQnJ1
c3NlbHMxMDAuBgNVBAoMJ0tpbmdkb20gb2YgQmVsZ2l1bSAtIEZlZGVyYWwgR292
ZXJubWVudDE2MDQGA1UECwwtRlBTIEhvbWUgQWZmYWlycyAtIEJJSy1HQ0kgKE5U
UkJFLTAzNjI0NzU1MzgpMTkwNwYDVQQLDDBGUFMgUG9saWN5IGFuZCBTdXBwb3J0
IC0gQk9TQSAoTlRSQkUtMDY3MTUxNjY0NykxGTAXBgNVBAMMEEJlbGdpdW0gUm9v
dCBDQTYwdjAQBgcqhkjOPQIBBgUrgQOAIgNiAAR532ARaLVsPSf5Pz9+b5ExaxpC
e8iGGkDgkbUlGM0ulbr0YqbKva7EoOAY+YL5ZJs8S0KIsuQNc0f2vgI8xcyPQHge
CaLcw0OzvmfCHf/OMOIozEKgKaAK6pHvaBXP0tijZjBkMBIGA1UdEwEB/wQIMAYB
Af8CAQEwHwYDVR0jBBgwFoAULqCIsAsNYonsHT/Un8ySRI5IaUYwHQYDVR0OBBYE
FC6giLALDWKJ7B0/1J/MkkSOSGlGMA4GA1UdDwEB/wQEAwIBBjAKBggqhkjOPQQD
AwNpADBmAjEAt2e2vVG4/aMjIokbQQuCnvI8so8rZl/IbKupMCJitfFi7oVlHllY
FDdYMDTKWLZgAjEAsa2wuz3Ew6/68XXtIT+51snqkl2KLlaVgKXYlpTh2zqQBIBd
KO1nMO/rQRfuZ701
-----END CERTIFICATE-----
```


9.2.1.2 Certificat(s) B : Timestamping

les mêmes que ArchiveTimestamping

9.2.1.3 Certificat(s) C : ArchiveTimestamping

- Cfr .http://repository.eid.belgium.be/ , http://repository.pki.belgium.be/ & https://repository.eidpki.belgium.be
- Les Timestamps doivent contenir le certpath entier.
- Les mêmes que “Certificat(s) A” auxquels s'ajoute les suivants

9.2.1.3.1. OU = GlobalSign Root CA - R6, O = GlobalSign, CN = GlobalSign

=> serial number : 45:e6:bb:03:83:33:c3:85:65:48:e6:ff:45:51

=> Issuer=Subject : OU = GlobalSign Root CA - R6, O = GlobalSign, CN = GlobalSign


```
-----BEGIN CERTIFICATE-----
MIIFgzCCA2ugAwIBAgIORea7A4Mzw4VlSOb/RVEwDQYJKoZIhvcNAQEMBQAwTDEg
MB4GA1UECxMXR2xvYmFsU2lnbiBSb290IENBIC0gUjYxEzARBgNVBAoTCkdsb2Jh
bFNpZ24xEzARBgNVBAMTCkdsb2JhbFNpZ24wHhcNMTQxMjEwMDAwMDAwWhcNMzQx
MjEwMDAwMDAwWjBMMSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSNjET
MBEGA1UEChMKR2xvYmFsU2lnbjETMBEGA1UEAxMKR2xvYmFsU2lnbjCCAiIwDQYJ
```

```
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAJUH6HPKZvnsFMp7PPcNCPG0RQssgrRI
xutbPK6DuEGSMxSkb3/pKszGsIhrxbaJ0cay/xTOURQh7ErdG1rG1ofuTToVBu1k
ZguSgMpE3nOUTvOniX9PeGMIyBJQbUJmL025eShNUhqKGoC3GYEOfsSKvGRMIRxD
aNc9PIrFsmbVkJq3MQbFvuJtMgamHvm566qjuL++gmNQ0PAYid/kD3n16qIfKtJw
LnvnvJO7bVPiSHyMEAc4/2ayd2F+4OqMPKq0pPbzlUoSB239jLKJz9CgYXfIWHSw
1CM69106yqLbnQneXUQtkPGBzVeS+n68UARjNN9rkxi+azayOeSsJDa38O+2HBNX
k7besvjihbdzorg1qkXy4J02oW9UivFyVm4uiMVRQkQVlO6jxTiWm05OWgtH8wY2
SXcwvHE35absIQh1/OZhFj931dmRl4QKbNQCTXTAFO39OfuD8l4UoQSwC+n+7o/h
bguyCLNhZglqsQY6ZZZZwPA1/cnaKI0aEYdwgQqomnUdnjqGBQCe24DWJfncBZ4n
WUx2OVvq+aWh2IMP0f/fMBH5hc8zSPXKbWQULHpYT9NLCEnFlWQaYw55PfWzjMpY
rZxCRXluDocZXFSxZba/jJvcE+kNb7gu3GduyYsRtYQUigAZcIN5kZeR1Bonvzce
MgfYFGM8KEyvAgMBAAGjYzBhMA4GA1UdDwEB/wQEAwIBBjAPBgNVHRMBAf8EBTAD
AQH/MB0GA1UdDgQWBBSubAWjkxPioufi1xzWx/B/yGdToDAfBgNVHSMEGDAWgBSu
bAWjkxPioufi1xzWx/B/yGdToDANBgkqhkiG9w0BAQwFAAOCAgEAgyXt6NH9lVLN
nsAEoJFp5lzQhN7craJP6Ed41mWYqVuoPId8AorRbrcWc+ZfwFSY1XS+wc3iEZGt
Ixg93eFyRJa0lV7Ae46ZeBZDE1ZXs6KzO7V33EByrKPrmzU+sQghoefEQzd5Mr61
55wsTLxDKZmOMNOsIeDjHfrYBzN2VAAiKrlNIC5waNrlU/yDXNOd8v9EDERm8tLj
vUYAGm0CuiVdjaExUd1URhxN25mW7xocBFymFe944Hn+Xds+qkxV/ZoVqW/hpvvf
cDDpw+5CRu3CkwWJ+n1jez/QcYF8AOiYrg54NMMl+68KnyBr3TsTjxKM4kEaSHpz
oHdpx7Zcf4LIHv5YGygrqGytXm3ABdJ7t+uA/iU3/gKbaKxCXcPu9czc8FB10jZp
nOZ7BN9uBmm23goJSFmH63sUYHpkqmlD75HHTOwY3WzvUy2MmeFe8nI+z1TIvWfs
pA9MRf/TuTAjB0yPEL+GltmZWrSZVxykzLsViVO6LAUP5MSeGbEYNNVMnbrt9x+v
JJUEeKgDu+6B5dpffItKoZB0JaezPkvILFa9x8jvOOJckvB595yEunQtYQEgfn7R
8k8HWV+LLUNS60YMlOH1Zkd5d9VUWx+tJDfLRVpOoERIyNiwmcUVhAn21klJwGW4
5hpxbqCo8YLoRT5s1gLXCmeDBVrJpBA=
-----END CERTIFICATE-----
```


9.3 Règles complémentaires

9.3.1 Liste des algorithmes de signature acceptés : (<SignatureMethod Algorithm=)

http://www.w3.org/2001/04/xmldsig-more#rsa-sha512 (1.2.840.113549.1.1.13)
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512 (1.2.840.10045.4.3.4)

9.3.2 Nombre de signatures par document déposé :

plusieurs « Detached » signatures dans un xml.

9.3.3 Mime-types acceptés :

Document type 1 :

Id="D*" MimeType="pdf" – pdf/A-1 (ISO 19005-1:2005) ou pdf/A supérieur en accord avec le service ICT SPF Justice.

Filename : IMG-fr.pdf, TXT-fr.pdf, IMG-nl.pdf, TXT-nl.pdf, IMG-de.pdf ou TXT-de.pdf,

Document type 2 (Optional) :

Id="D*" Filename="AnnexeRefs.xml" MimeType="xml"

conforme à l'xml suivant http://signinfo.eda.just.fgov.be/XSignInfo/2020/07/annexes_metadata, obligatoire si il y des annexes.

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:annexe="http://signinfo.eda.just.fgov.be/XSignInfo/2020/07/annexes_metadata"
           targetNamespace="http://signinfo.eda.just.fgov.be/XSignInfo/2020/07/annexes_metadata"
            elementFormDefault="qualified" attributeFormDefault="unqualified">

<xs:element name="annexes">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="nb" type="xs:integer"             minOccurs="1" maxOccurs="1"/>        <!-- number of annexes -->
    <xs:element name="annexe"  type="annexe:annexeType" minOccurs="0" maxOccurs="unbounded">
    </xs:element>
   </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="annexe" type="annexe:annexeType"/>

    <!-- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -->
      <xs:complexType name="annexeType" >
       <xs:sequence>
        <xs:element name="uuid"    type="annexe:UUIDType" minOccurs="1" maxOccurs="1"/>    <!-- uuid of annexe -->
        <xs:element name="sha256"  type="xs:hexBinary"    minOccurs="1" maxOccurs="1"/>    <!-- sha256 of annexe -->
       </xs:sequence>
      </xs:complexType>
    <!-- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -->

<xs:element name="UUIDType" type="annexe:UUIDType"/>

    <!-- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -->
      <xs:simpleType name="UUIDType">
          <xs:restriction base="xs:string">
              <xs:pattern
                  value="[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}">
              </xs:pattern>
          </xs:restriction>
      </xs:simpleType>
    <!-- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -->

</xs:schema>
```

9.3.4 Nombre maximal de documents signés

2 à 6 documents type 1 et 1 document type 2 ("AnnexeRefs" temporairement optionnel, mais obligatoire si il y des annexes)

9.3.5 Information de révocation

Elle doit être ajoutée par le Service d'encadrement ICT du SPF Justice sous la forme d'une réponse OCSP.

9.3.6 Type signataire

Le signataire doit être une eID Belge.

9.3.7 Liste des algorithmes acceptables pour les certificats.

Sha1 (1 3 14 3 2 26)
Sha256 (2 16 840 1 101 3 4 2 1)
Sha512 (2 16 840 1 101 3 4 2 3)
Ripemd160 (1 3 36 3 2 1)
Sha1withRSAEncryption (1 2 840 113549 1 1 5)
Sha256withRSAEncryption (1 2 840 113549 1 1 11)
Sha512withRSAEncryption (1 2 840 113549 1 1 13)
ecdsa-with-Sha1 (1 2 840 10045 4 1)
RsaSignatureWithripemd160 (1 3 36 3 3 1 2)
ecPublicKey (1 2 840 10045 2 1) Length >= 160
RsaEncryption (1 2 840 113549 1 1 1) Length >= 1020
ecdsa-with-Sha256 (1.2.840.10045.4.3.2)
ecdsa-with-Sha384 (1.2.840.10045.4.3.3)
ecdsa-with-Sha512 (1.2.840.10045.4.3.4)

References

[1] :ETSI TR 102 041 (v1.1.1):"Signature policy report"

Citizen CA : Énoncé des pratiques de Certification

(OID: 2.16.56.1.1.1.2 , 2.16.56.1.1.1.2.1 , 2.16.56.1.1.1.2.2 , 2.16.56.9.1.1.2 , 2.16.56.9.1.1.2.1 , 2.16.56.9.1.1.2.2)

En même temps que ce CPS, d'autres documents liés au processus de certification dans le contexte de la carte d'identité électronique belge peuvent avoir été pris en compte. Ces documents seront disponibles par le biais du répertoire du CSP à l'adresse: http://repository.eid.belgium.be & https://repository.eidpki.belgium.be.