Title:
Statoil Policy Disclosure Statement

Document no. :	Contract no.:	Project:

Classification:	Distribution:
Open	**Anyone**
Expiry date:	Status
2019-06-11	**Final**

Distribution date:	Rev. no.:	Copy no.:
2014-06-11	**2.1**	

Author(s)/Source(s):
PMA tasked Change Group
Subjects:
Statoil Policy Disclosure Statement
Remarks:
New version in connection with name change to Statoil

Valid from:	Updated:
2014-06-11	**2014-06-11**
Responsible publisher:	Authority to approve deviations:
Statoil PKI Policy Management Authority	**Statoil PKI Policy Management Authority**

Techn. responsible (Organisation	Techn. responsible (Name):	Date/Signature:
Statoil PKI Security Officer	**Kjetil Rønneberg Bustnes**	Kjetil Rønneberg Bustnes Digitally signed by Kjetil Rønneberg Bustnes DN: dc=com, dc=Statoil, c=NO, o=Statoil, serialNumber=9578-6000-00018274, cn=Kjetil Rønneberg Bustnes Date: 2014.06.27 12:18:14 +02'00'
Responsible (Organisation unit):	Responsible (Name):	Date/Signature:
Statoil PKI Security Officer	**Trond Bergill**	Trond Bergill Digitally signed by Trond Bergill DN: dc=com, dc=Statoil, c=NO, o=Statoil, cn=Trond Bergill, serialNumber=9578-6000-00027815 Date: 2014.07.01 13:18:00 +02'00'
Recommended (Organisation unit):	Recommended (Name):	Date/Signature:
LEG TPD	**Gaute Sletten**	Gaute Aleksej Sletten Digitally signed by Gaute Aleksej Sletten DN: dc=com, dc=statoil, c=no, o=Statoil, serialNumber=9578-6000-00236833, cn=Gaute Aleksej Sletten Date: 2014.09.16 11:58:59 +02'00'
Approved by (Organisation unit):	Approved by (Name):	Date/Signature:
CFO CIT IS	**Lars Idland**	Lars Idland Digitally signed by Lars Idland DN: dc=com, dc=Statoil, c=NO, o=Statoil, cn=Lars Idland, serialNumber=9578-6000-00060462 Date: 2014.07.01 15:19:30 +02'00'

Table of contents

1 Important Notice

Statoil issues certificates following four distinct certificate policies, namely:
- Statoil root certificate policy
- Statoil qualified certificate policy
- Statoil normal certificate policy
- Statoil light certificate policy

The Certificate Policies will only be available to parties with whom Statoil enters an agreement for use of digital certificates issued by a Statoil CA.
This document (PKI Disclosure Statement) does not substitute or replace the Certificate Policies but provides public information summarizing the key points of the Certificate Policies for the benefit of Subjects, Contractors and Relying Parties.

1.1 PDS history

This version replaces the former PDS with revision number 1.0.

2 Definitions and references

2.1 Definitions

Certificate:	Public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the Certification Authority which issued it.
Certificate Policy (CP):	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
Certification Authority (CA):	Authority trusted by one or more users to create and assign certificates
Certification Practice Statement (CPS):	Statement of the practices which a Certification Authority employs in issuing certificates
Contractor:	Entity contracting with a Statoil CA on behalf of one or more Subjects. For Machine Certificates the term Contractor also covers Line managers responsible for one or more Machines.
Electronic Signature:	Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data.
Relying Party:	Recipient (may be a computer system, an individual and/or an organization) of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Smartcard:	Device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Statoil:	Any organization controlled by Statoil ASA
Subject:	Entity identified in a certificate as the holder of the private key associated with the public key given in the Certificate.

2.2 References

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[2] EN 319 411-3 v1.1.1 (2013-01): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for certification authorities Trust Service Providers issuing public key certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates"

[3] EN 319 411-2 v1.1.1 (2013-01): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for certification authoritiesTrust Service Providers issuing qualified certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates"

[4] Norwegian Law; Lov 2001-06-15 nr. 81: "Lov om elektronisk signatur"

[5] Statoil CPS

[6] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

3 CA contact info

Statoil ASA

Forusbeen 50

4033 Stavanger

Att: Statoil Policy Management Authority.

Email: pma@Statoil.com

Tel: +47 51 99 00 00

Fax: +47 51 99 00 50

For user and usage information and support please search www.statoil.com , consult factsheets or submit a ticket to Statoil Servicedesk. For external users please submit the ticket through your contact in Statoil.

4 Certificate type, validation procedures and usage

The Statoil Digital Certification Services implement a closed hierarchical public key infrastructure consisting of one Root CA and 3 Subordinate CA. Statoil Digital Certification Services is only open to Subjects employed by Statoil or working with Statoil under contract and for Relying Parties who has entered an agreement with Statoil related to the use and acceptance of Statoil digital certificates.

Statoil or its representatives assumes no liability whatsoever in relation to the use of certificates or associated public/private key pairs issued under any of the Statoil Certificate Policies for any use other than in accordance with the Statoil Policy it is issued under and the express agreement entered between Statoil and a Relying Party only the written definitive agreement,

signed by the authorized representatives of Statoil, Contractor and/or Relying Party shall be binding upon the respective parties.

4.1 Statoil qualified certificate

Statoil Qualified Certificate Policy is based on EN 319 411-3 [3] and includes requirements for issuing qualified certificates (as required in Article 5.1 of the Electronic Signature Directive [1]) in accordance with Norwegian "Lov om elektronisk signatur" [4].
Statoil qualified certificates supports secure electronic identification of employees and/or employees of Contractors with whom Statoil have established an agreement. Only natural persons can be issued a Statoil qualified certificate. The registration procedures requires physical presence and the private signature keys are generated and stored on a personalized Smartcard complete with the persons picture, name and Statoil employee number.

As part of the registration, the RA/LRA shall on behalf of the CA, collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of Subjects to whom a Certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the Subject's identity shall be by appropriate means and in accordance with national law.

The Statoil Qualified CA has been cross certified with the GlobalSign "Trusted Root CA G2" and the GlobalSign "GlobalSign Primary SHA256 CA for Adobe".

The Statoil PKI adheres to Adobe Systems Incorporated "CDS Certificate Policy" (OID 1.2.840.113583.1.1.5)

The cross-certification certificates are shown in Appendix A

4.2 Statoil normal certificate

Statoil Certificate Policy Normal is based on EN 319 411-2 [2] and includes requirements for supporting the same level of quality as required by certification authorities issuing qualified certificates (as required in Article 5.1 of the Electronic Signature Directive [1]) but without the legal constraints as follows from issuing Qualified Certificates.

Statoil normal certificates supports secure email for Statoil employees and/or employees of Contractors with whom Statoil have established an agreement. Only natural persons can be issued a Statoil normal certificate, and the registration requires the use of a Statoil qualified certificate, registered as described above. Normal certificates and corresponding private keys are stored in software on the secured workstations of the subjects and is only accessible following authentication which as a minimum is in line with Statoil Authentication Policy.

4.3 Statoil light certificate

Statoil Certificate Policy Light is based on EN 319 411-2 [2] and includes requirements for issuing certificates to Statoil applications and computing devices running in or supporting Statoil infrastructure. These applications/computing devices may be operated by Statoil or by a third party on behalf of Statoil.

Statoil has no ambitions to issue certificates to the general public, nor to issue Publicly Trusted Certificates to servers and applications and will therefore not adhere to all requirements put forth in the PTC-BR[6]. Even so PTC-BR requirements will be implemented where appropriate.

Statoil light certificates and the corresponding private keys may be stored in software on the corresponding hardware, and the keys may be activated in an automated way by the hardware.

As part the registration process, the RA/LRA shall on behalf of the CA, verify that the Subject is operated on behalf of Statoil by checking Statoil asset lists or Statoil System Database.
The CA's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the Certificate.

4.4 Statoil root certificate

Statoil Qualified Certificate Policy includes requirements for issuing certificates to Statoil subordinate CAs.
Statoil Subordinate CAs shall, in order to be certified by Statoil Root CA, conform to the stipulations of the certificate policy definition and present a Certification Practice Statement that supports the certificate policy relevant to the policy under which the particular Subordinate CA issues its certificates.
The registration for sub certification under the Statoil root CA is performed directly by the Statoil Policy Management Authority.

4.5 Reliance limits

Statoil does not set reliance limits for certificates issued under this policy. Reliance limits may be set by other policies, application controls, and applicable law or by agreement. See Limitation of Liability, below.

5 Obligations of Subject and/or Contractor

It is the responsibility of the Subject and/or Contractor to:

a) submit accurate and complete information to Statoil CA in accordance with the requirements of the applicable Statoil Certificate Policy, particularly with regards to registration
b) the key pair is only used within and in accordance with the limitations set forth in the applicable Statoil Certificate Policy under which the Subject receives its certificate;
c) the Subject shall take necessary precautions to avoid unauthorized use of the Subject's private key;
d) take necessary precautions to avoid unauthorized use of the Subject's private key, in particular certify and agree that;
   - no unauthorized person and/or system has ever had access to the Subject's private signing key;
   - the Subject's private signing key shall be protected in accordance with the requirements set forth in the applicable Statoil Certificate Policy under which the Subject's certificate has been issued;
   - any compromise of the Subject's private signing key shall be immediately reported to the actual Statoil CA issuing the Subjects certificate;
e) without any reasonable delay, notify Statoil CA, if any of the following occur within the validity period of the certificate:
   - the Subject's private key has been lost, stolen, potentially compromised; or
   - control over the Subject's private key has been lost; or

- inaccuracy or changes to the certificate content;

f) In case of any events as described in e) above, the use of the Subject's private key shall immediately and permanently be discontinued.

g) only use the Subject's private key within a device conformant to the requirement set forth in the Statoil Certificate Policy under which the Subject receives its certificate;

h) if the Subject's keys are generated in the Smartcard under control of the Subject, and the private key is for creating Electronic Signatures and/or Authentication purposes, the Subject shall maintain control of the private key at all times once the private key is generated;

i) if Subject's keys are generated under control of the Contractor, private keys used for signing or Authentication in accordance with Statoil Qualified Certificate Policy shall only be generated within the Smartcard.

6 Certificate status checking obligations of relying parties

Relying Parties who has entered an agreement with Statoil related to the use and acceptance of Statoil digital certificates shall, in order to reasonable rely upon a certificate:

- Verify the validity, suspension or revocation of the certificate using current revocation status information
- Take account of any limitations on the usage of the certificate indicated to the Relying Party either in the certificate or the terms and conditions supplied as part of the agreement related to the use and acceptance of Statoil digital certificates; and
- Take any other precautions prescribed in agreements or elsewhere.

The Statoil PKI supports both X.509 v.2 revocation lists and OCSP status requests. The address of the revocation lists are given in the relevant certificates CRL distribution point extension while the OCSP address is given in the AIA extension.

7 Limited warranty and disclaimer/Limitation of liability

By signing a certificate containing a policy identifier which indicates the use of a Statoil certificate policy, the Statoil Issuing Authority certifies to all who reasonably rely on the information contained in the certificate, that the information in the certificate has been checked according to the procedures laid down in the relevant Statoil certificate policy.
The Statoil Issuing Authority assumes no liability whatsoever in relation to the use of certificates or associated public/private key pairs issued under the Statoil certificate policies for any use other than in accordance with these policies and a separate agreement between Statoil and any Relying Party related to the use and acceptance of Statoil digital certificates.
Statoil shall not be liable for any consequential, indirect or incidental damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, tort, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on, any Digital Certificate issued by any Statoil CA except only in the case of the Statoil CA's negligence, wilful misconduct, or where otherwise required by applicable law.
Nothing in the Statoil certificate policies excludes or restricts liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors.
Statoil excludes all liability of any kind in respect of any transaction into which a Subject may enter with any Relying Party unless liability is expressed as part of the separate agreement related to the use and acceptance of Statoil digital certificates.
Statoil is not liable to Subjects either in contract, tort (including negligence) or otherwise for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment.

Each provision of these policies, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

8 Certification Practice Statement

This document (PKI Disclosure Statement) can be found at:
http://pki.Statoil.com/pds/pds.pdf

The Certification Practice Statement is not normally made generally available, but under special circumstances and at the discretion of the Statoil Issuing Authority, the CPS may be obtained on application to the Issuing Authority as detailed above.

Registration and CA event log information is retained for ten years after establishment.

9 Privacy policy

Statoil shall ensure that the requirements of the applicable national data protection legislation are met.

The information that Subjects contribute to a Statoil CA shall be completely protected from disclosure unless Subjects with their agreement agree otherwise or the CA by court order or other legal requirement are required to disclose such information.

The user agrees to have the user information given in the certificates disclosed, according to the accessibility of the certificates to other users.

10 Signature policy

Statoil accepts that electronic signatures may be used as an alternative to written signatures, provided that the issuer of certificates for electronic signatures is on the “Trusted List” issued by the Norwegian Post and Telecommunications Authority or any equivalent trusted list issued by any similar authority within the European Economic Area.

Statoil will on a case by case basis at its own discretion accept an issuer of electronic certificates not on “Trusted Lists", after having been given access to the issuer’s certificate policy, certificate practice statement and an audit report verifying that the issuer is acting in accordance with such documents. If subsequently there has been a significant change to the issuers system for electronic signatures or if Statoil so reasonably requires, this mechanism shall be reapplied.

11 Applicable law, complaints and dispute resolution

The provision of Statoil Certification Services shall be governed by Norwegian law and all parties shall submit to the exclusive jurisdiction of the courts of Norway.

12 Audit

Audit is carried out on a bi-annual basis by an auditor chosen by Statoil.

Appendix A. Cross-certification certificates – Generation 0

Issuer: CN = GlobalSign Primary SHA256 CA for Adobe
OU = GlobalSign CDS
O = GlobalSign nv-sa
C = BE

-----BEGIN CERTIFICATE-----
MIIIgzCCB2ugAwIBAgIRdgWfFYGa7nsy6DLb/KSLiPYwDQYJKoZIhvcNAQELBQAw
cjELMAkGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExFzAVBgNV
BAsTDkdsb2JhbFNpZ24gQ0RTMS8wLQYDVQQDEyZHbG9iYWxTaWduIFByaW1hcnkg
U0hBMjU2IENBIGZvciBBZG9iZTAeFw0xMzA5MTcwMDAwMDBaFw0xOTEwMTMxNDA1
NTZaMHwxEzARBgoJkiaJk/IsZAEZFgNjb20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0
b2lsMQswCQYDVQQGEwJOTzEgMB4GA1UEChMXU3RhdG9pbCBBU0EgLSA5MjM2MDkw
MTYxHTAbBgNVBAMTFFN0YXRvaWwgUXVhbGlmaWVkIENBMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEAxcRB/NMeUdbNAy0s/HV/iXCfRsSjB7i6InZS2yti
1k/mV2bLsPVzh5MiPYa+mnOFJIAiT3Tc3EySmAXs6fsnNkQ2VcCBcVb20M3tT1sp
iyTyXD7nElIhX8QWhkBxaxuWberY7ov7RMRYMezrZWOP7xSLynIaE9eUqXsFod2F
9wCyhwXYsmjkXMjdgX62GV5QEnjkGPIt7DT53cgedbQe/d2i2kIa2vpi5lxBKXiZ
TjHZvgDobX5A8vR8KCliuJwKiiNDCKziKmqs/l/tAiVB9BnMN524wXjKprspRAwH
vKzH8a2LdWzSFfFefp4Q84I5xWt7H/EmSUzhoNCrgDtUd1NAOROCG8lmtqu4wcFN
cIAS/DUGJLSV/Im6rUqXCEP5MXDGUzfMekNtzpWsD/3Zxj9HKdoBUaVuIi1roDSz
8yr7ao9TNJ3G5lPwGYetz/lpkOiwtz9+t5Qp6goRsf9+w7N7mC8eveVq3u4A53pG
fm6e5rlbqdmf8QmCO3fhHlS8TR0a9+modaP6zX2kTRp+T3cfZ9RFxBuL/LHCDM7b
+aZQBHNj4ImPsoSFGHxhW8gjT92a3ZnhfFI5FvO4vgUiRYSfEWrySU24KHqbsl1d
XEPyuwX/UAHe17h7DCRiAKDnGeI+TeR5gV8xbKj45YQ2e6Kiuv1d2KLTbgARStH8
grcCAwEAAaOCBAgwggQEMA4GA1UdDwEB/wQEAwIBBjCCAfAGA1UdIASCAecwggHj
MIH5BgkqhkiG9y8BAgEwgeswMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkvMIG0BggrBgEFBQcCAjCBpwyBpFRoaXMgY2Vy
dGlmaWNhdGUgaGFzIGJlZW4gaXNzdWVkIGluIGFjY29yZGFuY2Ugd2l0aCB0aGUg
QWRvYmUgQ1AgYW5kIEdsb2JhbFNpZ24gQ1AvQ1BTIGxvY2F0ZWQgaW4gdGhlIEds
b2JhbFNpZ24gcmVwb3NpdG9yeTotIGh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29t
L3JlcG9zaXRvcnkvMIHkBghghEIBDgIBAjCB1zAuBggrBgEFBQcCARYiaHR0cDov
L3BraS5zdGF0b2lsLmNvbS9wZHMvcGRzLnBkZjCBpAYIKwYBBQUHAgIwgZcMgZRT
dGF0b2lsIGV4Y2x1ZGVzIGFsbCBsaWFiaWxpdHkgb2YgYW55IGtpbmQgcmVsYXRl
ZCB0byB0aGUgdXNlIGFuZCBhY2NlcHRhbmNlIG9mIFN0YXRvaWwgZGlnaXRhbCBj
ZXJ0aWZpY2F0ZXMgdW5sZXNzIGV4cHJlc3NlZCBpbiBzZXBhcmF0ZSBhY3JlZW1l
bnQuMBIGA1UdEwEB/wQIMAYBAf8CAQAwgcQGA1UdHgEB/wSBuTCBtqCBgTANggtz
dGF0b2lsLmNvbTANgQtzdGF0b2lsLmNvbTAOgQwuc3RhdG9pbC5jb20wUaRPME0x
EzARBgoJkiaJk/IsZAEZFgNjb20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0b2lsMQsw
CQYDVQQGEwJOTzEQMA4GA1UEChMHU3RhdG9pbKEwMAqHCAAAAAAAAAAAMCKHIAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMBQGA1UdJQQNMAsGCSqGSIb3
LwEBBTBABgNVHR8EOTA3MDWgM6Axhi9odHRwOi8vY3JsLmdsb2JhbHNpZ24uY29t
L2dzL2dzcHJtc2hhMmFkb2JlLmNybDCBigYIKwYBBQUHAQEEfjB8MDYGCCsGAQUF
BzABhipodHRwOi8vb2NzcDIuZ2xvYmFsc2lnbi5jb20vZ3Nwcm1zaGEyYWRvYmUw
QgYIKwYBBQUHMAKGNmh0dHA6Ly9zZWN1cmUuZ2xvYmFsc2lnbi5jb20vY2FjZXJ0
L2dzcHJtc2hhMmFkb2JlLmRlcjAdBgNVHQ4EFgQUjg9Y4Ic5Dl34c0uYJEaWdTvj
k1owHwYDVR0jBBgwFoAUWdgkws9rBkLUlXa1KVz12EErJF8wDQYJKoZIhvcNAQEL
BQADggEBAIW4PtYa//aaSYfAQWf7hi4SGPonm00LuTGxQ62B1Z+ip7kZsOYmleIr
/u8gUS5Nsi2QJp4ISP9+vd7mbLag8a/ZJazQzS0Mmz+bM7Twtt+Z+NtjI59CaGmM
pJuI8V2LZLYFpZ+6RUeNujsDrzcqoWtf8INiyptT3d4EJeOoU/jnSBnWhZSwSf2R
+5VIL2rOV08sVHULVALUAWtEIABNKm5GjZyrwKfExHUYU8EAN6VRsEcvW2b7frCj
+Tyi2u0WNdp7Op1gdiHvUiVknr1uHfLtAg4H72n7E+glwxfuCeCI8BeLgZFnbsC+
i0oueBNNPL7mXVPnE9GT6SZM0alqoS8=
-----END CERTIFICATE-----

Issuer: CN = Trusted Root CA G2
O = GlobalSign nv-sa
OU = Trusted Root
C = BE

-----BEGIN CERTIFICATE-----
MIIH/TCCBuWgAwIBAgIRRsHXt+G5QhTJ1bCt0DhLGTkwDQYJKoZIhvcNAQEFBQAw
XDELMAkGA1UEBhMCQkUxFTATBgNVBAsTDFRydXN0ZWQgUm9vdDEZMBcGA1UEChMQ
R2xvYmFsU2lnbiBudi1zYTEbMBkGA1UEAxMSVHJ1c3RlZCBSb290IENBIEcyMB4X
DTEzMDkxNzAwMDAwMFoXDTE5MTAxMzE0MDU1NlowfDETMBEGCgmSJomT8ixkARkW
A2NvbTEXMBUGCgmSJomT8ixkARkWB3N0YXRvaWwxCzAJBgNVBAYTAk5PMSAwHgYD
VQQKExdTdGF0b2lsIEFTQSAtIDkyMzYwOTAxNjEdMBsGA1UEAxMUU3RhdG9pbCBR
dWFsaWZpZWQgQ0EwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDFxEH8
0x5R1s0DLSz8dX+JcJ9GxKMHuLoidlLbK2LWT+ZXZsuw9XOHkyI9hr6ac4UkgCJP
dNzcTJKYBezp+yc2RDZVwIFxVvbQze1PWymLJPJcPucSUiFfxBaGQHFrG5Zt6tju
i/tExFgx7OtlY4/vFIvKchoT15SpewWh3YX3ALKHBdiyaORcyN2BfrYZXlASeOQY
8i3sNPndyB51tB793aLaQhra+mLmXEEpeJlOMdm+AOhtfkDy9HwoKWK4nAqKI0MI
rOIqaqz+X+0CJUH0Gcw3nbjBeMqmuylEDAe8rMfxrYt1bNIV8V5+nhDzgjnFa3sf
8SZJTOGg0KuAO1R3U0A5E4IbyWa2q7jBwU1wgBL8NQYktJX8ibqtSpcIQ/kxcMZT
N8x6Q23OlawP/dnGP0cp2gFRpW4iLWugNLPzKvtqj1M0ncbmU/AZh63P+WmQ6LC3
P363lCnqChGx/37Ds3uYLx695Wre7gDnekZ+bp7muVup2Z/xCYI7d+EeVLxNHRr3
6ah1o/rNfaRNGn5Pdx9n1EXEG4v8scIMztv5plAEc2PgiY+yhIUYfGFbyCNP3Zrd
meF8UjkW87i+BSJFhJ8RavJJTbgoepuyXV1cQ/K7Bf9QAd7XuHsMJGIAoOcZ4j5N
5HmBXzFsqPjlhDZ7oqK6/V3YotNuABFK0fyCtwIDAQABo4IDmDCCA5QwDgYDVR0P
AQH/BAQDAgEGMIIBNwYDVR0gBIIBLjCCASowgeQGCGCEQgEOAgECMIHXMC4GCCsG
AQUFBwIBFiJodHRwOi8vcGtpLnN0YXRvaWwuY29tL3Bkcy9wZHMucGRmMIGkBggr
BgEFBQcCAjCBlwyBlFN0YXRvaWwgZXhjbHVkZXMgYWxsIGxpYWJpbGl0eSBvZiBh
bnkga2luZCByZWxhdGVkIHRvIHRoZSB1c2UgYW5kIGFjY2VwdGFuY2Ugb2YgU3Rh
dG9pbCBkaWdpdGFsIGNlcnRpZmljYXRlcyB1bmxlc3MgZXhwcmVzc2VkIGluIHNl
cGFyYXRlIGFncmVlbWVudC4wQQYJKwYBBAGgMgE8MDQwMgYIKwYBBQUHAgEWJmh0
dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkvMBIGA1UdEwEB/wQI
MAYBAf8CAQAwgfUGA1UdHgSB7TCB6qCBtTANggtzdGF0b2lsLmNvbTANgQtzdGF0
b2lsLmNvbTAOgQwuc3RhdG9pbC5jb20wUaRPME0xEzARBgoJkiaJk/IsZAEZFgNj
b20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0b2lsMQswCQYDVQQGEwJOTzEQMA4GA1UE
ChMHU3RhdG9pbDAypDAwLjETMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT
8ixkARkWB3N0YXRvaWyhMDAKhwgAAAAAAAAAADAihyAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAADA1BgNVHSUELjAsBggrBgEFBQcDAgYIKwYBBQUHAwQG
CisGAQQBgjcUAgIGCisGAQQBgjcKAwwwPQYDVR0fBDYwNDAyoDCgLoYsaHR0cDov
L2NybC5nbG9iYWxzaWduLmNvbS9ncy90cnVzdHJvb3RnMi5jcmwwgYQGCCsGAQUF
BwEBBHgwdjAzBggrBgEFBQcwAYYnaHR0cDovL29jc3AyLmdsb2JhbHNpZ24uY29t
L3RydXN0cm9vdGcyMD8GCCsGAQUFBzAChjNodHRwOi8vc2VjdXJlLmdsb2JhbHNp
Z24uY29tL2NhY2VydC90cnVzdHJvb3RnMi5jcnQwHQYDVR0OBBYEFI4PWOCHOQ5d
+HNLmCRGlnU745NaMB8GA1UdIwQYMBaAFBT25YsxtkWASkxt/MKHico2w5BiMA0G
CSqGSIb3DQEBBQUAA4IBAQA9QV5pB5n6VIHs6Z1au9YFVSVDZh5rcGvEYBeF8u7g
/NRd1XXVJ//4eiCuN/Vj2j4tkOIGyNPENQNWMh5LjihCjWJhGiz0PEQ8jocXi35y
4ZN/JMAnEoVe1FYMlNiXMo65QrB8e0ZHgIibNLlfUpZKJje2sJgtt2FZ2tkM8RtE
kJnPFudBD12okNxu4dfQHfBmG3fpwja82Gro9V6Nc+RTQI1NxM2vmExYzwkU1v4L
MO7byMowe5qg7K/YHqrpauuQFk8Py2VYx7dPDurwgahNlNS2Qt45yRrqqFVW9D91
Odp1LUbos8zOOt8ykEnge6lYlpBPCh0At/nawu32Ow4G
-----END CERTIFICATE-----

Appendix B. Cross-certification certificates – Generation 1

Issuer: CN = GlobalSign Primary SHA256 CA for Adobe
OU = GlobalSign CDS
O = GlobalSign nv-sa
C = BE

-----BEGIN CERTIFICATE-----
MIIIgzCCB2ugAwIBAgIRZe0DyQyVq9ALGPKJABqApKwwDQYJKoZIhvcNAQELBQAw
cjELMAkGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExFzAVBgNV
BAsTDkdsb2JhbFNpZ24gQ0RTMS8wLQYDVQQDEyZHbG9iYWxTaWduIFByaW1hcnkg
U0hBMjU2IENBIGZvciBBZG9iZTAeFw0xNDA1MjgwMDAwMDBaFw0yMjA1MjQwMDAw
MDBaMHwxEzARBgoJkiaJk/IsZAEZFgNjb20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0
b2lsMQswCQYDVQQGEwJOTzEgMB4GA1UEChMXU3RhdG9pbCBBU0EgLSA5MjM2MDkw
MTYxHTAbBgNVBAMTFFN0YXRvaWwgUXVhbGlmaWVkIENBMIICIjANBgkqhkiG9w0B
AQEFAAOCAg8AMIICCgKCAgEA0wEswR8w0xNkkGZE8I+Y7VEaZ5u+QIclx9d6KO5O
DkCvkN95qlPOwoBPmFd2eghbtns1P9X/mHhN3BiIGK2PgYtoUVYekntkbZlqbMbj
L39jMPAeNwgdFipa+Grzf4UbTIVxDYvGgsjCFYfgQPHekwZY18iYy09mN5UzGNAN
DditUO4KQJCIcgqgydJD6n/p/y9cK5QGH8ZDfU7yqSJNv1M9dhl0w9+gintEez6q
sCx1RpzZqV6lG20ZWPg6wiVCQbC8bXvnMpNIh8WnrQbkUZ1A7ntOyYYPeXIO8FHS
zJHR+sW2eZ0S1Vl948btdokyPwLiotTCGKc+21O/ZdsLj2n3lxgfLwhHv8HVWyUV
KNFIyBSa0tjyh2sbdNxlytlRIB8/3VoslOXl/2t+qupSJZbKv0/3SzwFUCwSrxhH
rF936kOkKZTOSoayYDo0v4JNHS+eU+BKeIGTd/PdCNihuSTBLPUHDwgEm8dlFQ+6
bc/zjfgpkuiDGJwk8Yie4jRGc2bHcufjM3U5a7lwn/+GmhmELTL8Ydw0Lleoyehz
larWNWc8gXiQwgBfiPy4/kVe1ec4BcHKe8WbRvLoS0GDkA1WGxmm1l+Sb9zRjSCR
LuoPOBmvCUS/jOsXOYyIjoa4UzN/PKR9vrBShloQVmkyVZrbZY1sj3XJX6Q62+z8
V2cCAwEAAaOCBAgwggQEMA4GA1UdDwEB/wQEAwIBBjCCAfAGA1UdIASCAecwggHj
MIH5BgkqhkiG9y8BAgEwgeswMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkvMIG0BggrBgEFBQcCAjCBpwyBpFRoaXMgY2Vy
dGlmaWNhdGUgaGFzIGJlZW4gaXNzdWVkIGluIGFjY29yZGFuY2Ugd2l0aCB0aGUg
QWRvYmUgQ1AgYW5kIEdsb2JhbFNpZ24gQ1AvQ1BTIGxvY2F0ZWQgaW4gdGhlIEds
b2JhbFNpZ24gcmVwb3NpdG9yeTotIGh0dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29t
L3JlcG9zaXRvcnkvMIHkBghghEIBDgIBAjCB1zAuBggrBgEFBQcCARYiaHR0cDov
L3BraS5zdGF0b2lsLmNvbS9wZHMvcGRzLnBkZjCBpAYIKwYBBQUHAgIwgZcMgZRT
dGF0b2lsIGV4Y2x1ZGVzIGFsbCBsaWFiaWxpdHkgb2YgYW55IGtpbmQgcmVsYXRl
ZCB0byB0aGUgdXNlIGFuZCBhY2NlcHRhbmNlIG9mIFN0YXRvaWwgZGlnaXRhbCBj
ZXJ0aWZpY2F0ZXMgdW5sZXNzIGV4cHJlc3NlZCBpbiBzZXBhcmF0ZSBhZ3JlZW1l
bnQuMBIGA1UdEwEB/wQIMAYBAf8CAQAwgcQGA1UdHgEB/wSBuTCBtqCBgTANggtz
dGF0b2lsLmNvbTANgQtzdGF0b2lsLmNvbTAOgQwuc3RhdG9pbC5jb20wUaRPME0x
EzARBgoJkiaJk/IsZAEZFgNjb20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0b2lsMQsw
CQYDVQQGEwJOTzEQMA4GA1UEChMHU3RhdG9pbKEwMAqHCAAAAAAAAAAAMCKHIAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMBQGA1UdJQQNMAsGCSqGSIb3
LwEBBTBABgNVHR8EOTA3MDWgM6Axhi9odHRwOi8vY3JsLmdsb2JhbHNpZ24uY29t
L2dzL2dzcHJtc2hhMmFkb2JlLmNybDCBigYIKwYBBQUHAQEEfjB8MDYGCCsGAQUF
BzABhipodHRwOi8vb2NzcDIuZ2xvYmFsc2lnbi5jb20vZ3Nwcm1zaGEyYWRvYmUw
QgYIKwYBBQUHMAKGNmh0dHA6Ly9zZWN1cmUuZ2xvYmFsc2lnbi5jb20vY2FjZXJ0
L2dzcHJtc2hhMmFkb2JlLmRlcjAdBgNVHQ4EFgQU2nWZia7Mjd9CpahYqPyWuIat
xJowHwYDVR0jBBgwFoAUWdgkws9rBkLUlXa1KVz12EErJF8wDQYJKoZIhvcNAQEL
BQADggEBAD1915QhJafMrrpSLblxD7RE9b94oQzrW8rWfFNB94Rx7najakNzLLYJ
O5nVVUGzlIKMZyJBsFgpR31X1rKrOcCY23tDPlFJT33qgJXYAqKzFXHWrL5Mwz/Y
xh04mWI+/iWlQmxaSfZwanGguINWBhf0mFMHA1eEUpcFUshB/RAxqP0rxI5d+xbI
6UpBSMQ4UgdpQ58uSPq2LPMDpbHbEltmfR2+nb+39LLVghtVdfsFNljPWWMYVT3B
ZJtP4ecCiQvqMuwHEzjZpKAf8apYqKtg4PKtq1tRMeOFCWXUV6oFWaSDU6l580C/
0Ea+1aeicY1q0tgxiFcwV/L7rnsR5AA=
-----END CERTIFICATE-----

Issuer: CN = Trusted Root CA SHA256 G2
O = GlobalSign nv-sa
OU = Trusted Root
C = BE

-----BEGIN CERTIFICATE-----
MIIIETCCBvmgAwIBAgIRUNn9wgz3zyInBBgjY+GzhpswDQYJKoZIhvcNAQELBQAw
YzELMAkGA1UEBhMCQkUxFTATBgNVBAsTDFRydXN0ZWQgUm9vdDEZMBcGA1UEChMQ
R2xvYmFsU2lnbiBudi1zYTEiMCAGA1UEAxMZVHJ1c3RlZCBSb290IENBIFNIQTI1
NiBHMjAeFw0xNDA1MjgwMDAwMDBaFw0yMjA1MjgwMDAwMDBaMHwxEzARBgoJkiaJ
k/IsZAEZFgNjb20xFzAVBgoJkiaJk/IsZAEZFgdzdGF0b2lsMQswCQYDVQQGEwJO
TzEgMB4GA1UEChMXU3RhdG9pbCBBU0EgLSA5MjM2MDkwMTYxHTAbBgNVBAMTFFN0
YXRvaWwgUXVhbGlmaWVkIENBMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
AgEA0wEswR8w0xNkkGZE8I+Y7VEaZ5u+QIclx9d6KO5ODkCvkN95qlPOwoBPmFd2
eghbtns1P9X/mHhN3BiIGK2PgYtoUVYekntkbZlqbMbjL39jMPAeNwgdFipa+Grz
f4UbTIVxDYvGgsjCFYfgQPHekwZY18iYy09mN5UzGNANDditUO4KQJCIcgqgydJD
6n/p/y9cK5QGH8ZDfU7yqSJNv1M9dhl0w9+gintEez6qsCx1RpzZqV6lG20ZWPg6
wiVCQbC8bXvnMpNIh8WnrQbkUZ1A7ntOyYYPeXIO8FHSzJHR+sW2eZ0S1Vl948bt
dokyPwLiotTCGKc+21O/ZdsLj2n3lxgfLwhHv8HVWyUVKNFIyBSa0tjyh2sbdNxl
ytlRIB8/3VoslOXl/2t+qupSJZbKv0/3SzwFUCwSrxhHrF936kOkKZTOSoayYDo0
v4JNHS+eU+BKeIGTd/PdCNihuSTBLPUHDwgEm8dlFQ+6bc/zjfgpkuiDGJwk8Yie
4jRGc2bHcufjM3U5a7lwn/+GmhmELTL8Ydw0Lleoyehzlar WNWc8gXiQwgBfiPy4
/kVe1ec4BcHKe8WbRvLoS0GDkA1WGxmm1l+Sb9zRjSCRLuoPOBmvCUS/jOsXOYyI
joa4UzN/PKR9vrBShloQVmkyVZrbZY1sj3XJX6Q62+z8V2cCAwEAAaOCA6UwggOh
MA4GA1UdDwEB/wQEAwIBBjCCATcGA1UdIASCAS4wggEqMIHkBghghEIBDgIBAjCB
1zAuBggrBgEFBQcCARYiaHR0cDovL3BraS5zdGF0b2lsLmNvbS9wZHMvcGRzLnBk
ZjCBpAYIKwYBBQUHAgIwgZcMgZRTdGF0b2lsIGV4Y2x1ZGVzIGFsbCBsaWFiaWxp
dHkgb2YgYW55IGtpbmQgcmVsYXRlZCB0byB0aGUgdXNlIGFuZCBhY2NlcHRhbmNl
IG9mIFN0YXRvaWwgZGlnaXRhbCBjZXJ0aWZpY2F0ZXMgdW5sZXNzIGV4cHJlc3Nl
ZCBpbiBzZXBhcmF0ZSBhZ3JlZW1lbnQuMEEGCSsGAQQBoDIBPDA0MDIGCCsGAQUF
BwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5LzASBgNV
HRMBAf8ECDAGAQH/AgEAMIH1BgNVHR4Ege0wgeqggbUwDYILc3RhdG9pbC5jb20w
DYELc3RhdG9pbC5jb20wDoEMLnN0YXRvaWwuY29tMFGkTzBNMRMwEQYKCZImiZPy
LGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHc3RhdG9pbDELMAkGA1UEBhMCTk8x
EDAOBgNVBAoTB1N0YXRvaWwwMqQwMC4xEzARBgoJkiaJk/IsZAEZFgNjb20xFzAV
BgoJkiaJk/IsZAEZFgdzdGF0b2lsoTAwCocIAAAAAAAAAAAwIocgAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAwNQYDVR0lBC4wLAYIKwYBBQUHAwIGCCsG
AQUFBwMEBgorBgEEAYI3FAICBgorBgEEAYI3CgMMMEEGA1UdHwQ6MDgwNqA0oDKG
MGh0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvdHJ1c3Ryb290c2hhMmcyLmNy
bDCBjQYIKwYBBQUHAQEEgYAwfjA3BggrBgEFBQcwAYYraHR0cDovL29jc3AyLmds
b2JhbHNpZ24uY29tL3RydXN0cm9vdHNoYTJnMjBDBggrBgEFBQcwAoY3aHR0cDov
L3NlY3VyZS5nbG9iYWxzaWduLmNvbS9jYWNlcnQvdHJ1c3Ryb290c2hhMmcyLmNy
dDAdBgNVHQ4EFgQU2nWZia7Mjd9CpahYqPyWuIatxJowHwYDVR0jBBgwFoAUyGOb
CGlUwpjI2c3jM7dQXvjJAZswDQYJKoZIhvcNAQELBQADggEBAE01HkEnJGT/oqwn
T4y1G0GMMVxvTOeRa1Mz85y7V0qqy9RIHF425n0qtE2fiInmlx8BJ3vqcLOY+eCi
z/oSxB2aqh10PH0SApKL24MDL6R6ISdcWW47I+HEvZIKDdjhwCt+rHkUb1yrkXoC
KTj4BQe7V590rtjbfxZZYBTCxjygom17OfAwJDe1oaFPRJKsudtqzD2f6UP0STE7
1B/i8t8CtxBMKKbkW2YuVGzuT8mr7mSotxKdFxl89EwuTcZCEnEeH3p4vLO2IsPW
FsIYQ5pP47LTNy8BCLmz6n1U/DfUs+v9DeW0k/P8/1Su7rhhFCXYJ987/oCWkWmq
YxtFt/s=
-----END CERTIFICATE-----