<table>
<thead>
<tr>
<th>Title:</th>
<th>Statoil Policy Disclosure Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document no.:</td>
<td>Contract no.:</td>
</tr>
<tr>
<td>Classification:</td>
<td>Distribution:</td>
</tr>
<tr>
<td>Open</td>
<td>Anyone</td>
</tr>
<tr>
<td>Expiry date:</td>
<td>Status</td>
</tr>
<tr>
<td>2014-06-11</td>
<td>Final</td>
</tr>
<tr>
<td>Distribution date:</td>
<td>Rev. no.:</td>
</tr>
<tr>
<td>2014-06-11</td>
<td>2.1</td>
</tr>
</tbody>
</table>

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: 2014-06-11

Updated: 2014-06-11

Responsible publisher: Statoil PKI Policy Management Authority

Authority to approve deviations: Statoil PKI Policy Management Authority

Techn. responsible (Organisation unit): Statoil PKI Security Officer

Techn. responsible (Name): Kjetil Renneberg Bustnes

Date/Signature: 2014-06-11

Responsible (Organisation unit): Statoil PKI Security Officer

Responsible (Name): Trond Bergill

Date/Signature: 2014-06-11

Recommended (Organisation unit): LEG TPD

Recommended (Name): Gaute Sletten

Date/Signature: 2014-06-11

Approved by (Organisation unit): CFO CIT IS

Approved by (Name): Lars Idland

Date/Signature: 2014-06-11
Table of contents

1 Important Notice .............................................................................................................................. 3
  1.1 PDS history ............................................................................................................................ 3
2 Definitions and references .......................................................................................................... 3
  2.1 Definitions ............................................................................................................................. 3
  2.2 References ............................................................................................................................ 4
3 CA contact info ................................................................................................................................. 4
4 Certificate type, validation procedures and usage....................................................................... 4
  4.1 Statoil qualified certificate .................................................................................................... 5
  4.2 Statoil normal certificate ....................................................................................................... 5
  4.3 Statoil light certificate .......................................................................................................... 5
  4.4 Statoil root certificate .......................................................................................................... 6
  4.5 Reliance limits ....................................................................................................................... 6
5 Obligations of Subject and/or Contractor .................................................................................. 6
6 Certificate status checking obligations of relying parties......................................................... 7
7 Limited warranty and disclaimer/Limitation of liability ........................................................... 7
8 Certification Practice Statement ............................................................................................... 8
9 Privacy policy .............................................................................................................................. 8
10 Applicable law, complaints and dispute resolution................................................................. 8
11 Audit ........................................................................................................................................... 9
Appendix A. Cross-certification certificates .................................................................................. 10
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.
2.1 Classification: Internal (Restricted Distribution) Status: Final Expiry date: 2019-06-11 Page 4 of 13

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


[5] Statoil CPS


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
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 expressly stated 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:

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/KSL79blZiPywDQYJKoZIhvcNAQELBQAw
bWgMaQwFmkPn24gbYctzExFzVAvgNh
bA7Tdbkh2VhHWF5Pn224qQbRMS8sLQryDQYHZb91yWk/dMduIIFyA1hwncq
Uh90BMj212ZsnccvBiBB5g91l7Tae0Fx0Mr6AS5MctwcMADbFA0x0eTMXXMVNA1D
NT2aMhWxbz2RbgOkj1a1k/jk/KsAEZFGnJb20L2FVbVgoKjia1k/KsAECFzg3sG0
b21sMa2qMwQQVQDQQwEJOTuzIg9M641AUECXMUX3Rhd59pCBBU0QgLSAM5MJM2Dkw
MT1xkHATg6BVGAMTNFFloXTykmAVwVgb686MaKnVEKKNNiC1JABNbg5hhG159wOB
AQ7F4AOGCAg5AMIC5CkAcRBCP/NM3DhMAYaO/Q/HL/CFkKNBj7i6Inz2yti
k/w2VbLsPhtzvM1L_lifetime+mmOF3Jai1T3t3BYmAExf5nNKeV2CFb8Vb28M0t1p
iTyXfd7E61hXQWkhKbxaxwWe7v7r70YMRMezzZW0P7xSlyInIaE9eU9XSeeFd2F
9CyChy9wXsmyjKMDjxk62V5S6QnjkGP17dT35cgedeQe/d2lKia2v5i1f5KX1IZ
TjH7vzvOb5Xa8V8BcKljuWk1nNDCZki1Kmqa/l/aT1/AVB9nM5N24wXK5prspRAWb
V2Kha2DLDw3SF9F9PeN4BkI5Xw7H/EmS/3ZMsOnCqD6D/1/NAU0CG8lmtqu4cWP
CfAS/DGjJYXl/1s6vdqZ6ECP5H0QgUfMeKmNzcp2Sb3/3Xj9X96H2dS8V/4111o2d5S
8yr7ao/TMT3G5tPVtGyet/z/lpKOzTSz97t5g60aRaf9+w7N7mC9eweVq3u435pG
6m65t1bq0f8QMCoTzNi68475R0a9+mduh67z4x2tRzP+T3c299R9BhUL/L7CM7b
+a2Q8HNN4jMposSFGHxhWkxj792a3Zhhf515F0v4v0UYR5sFWrNYsSU24KhQba1d
XEPFykurU/AU3Te7B/7a7CDrlkOnT/feR5gVxbyKJ5y9Q6eKu1d4ZKtbg5RAt5th
grccWANeAAeCAAwQGM4A1UdEDwEB/wQEBwIBJBCF/AFAG1A1U1D1ACeawcggff7
MINbGtjkhkgy98dBgEwKsawH1fF5YVBBQHAGEnEm0b019bKzw83d2d26z2h
bHnpz24VY92t1j3L1c92aKxvBckv5MuG0b29gBrBuEBCQaCAjBwpwy8BF9xc3VY7Y
z1mlaMNH6ugFaFZal5TmZ4Wf9ZDwMVkJlUIGFJY29GZGF/2Ygd21CABUgDQ
QQRWYmuUQAGY5HYxKIDEs2bhnFnpz24G1aqV1BTgyXv2FQW2Qn4w4dh11Eds
b2JbnFnpz24G1aqV1BTgyXv2FQW2Qn4w4dh11Eds
JL3lC19a2vXvkmnCd2HhEB8a1BzuAvjBiXOQFCCFAR1AhQ0cD0v
L3bra5s2D9fB31m2nh39s9/3t9Vc3Rk2Jb3ZPbyYK1mNh9BQHAGEnEm0b019bKzw83d2
DrGFb21s1G9Y/1x12ZtVIsFbDrBsa1FawKdpK4gU3yY515tSbpmQcSmW3Xe
ZCBOby5U0GugD3CI56FmZ3d5c9tHb/besc11gh9meBFNYXxVQwNgj2Lh3xVRhBCB
ZXJoA4w2pZ2XMKgqEd5EnXNNvG4VHJC1C3ZCBpi1zZBxmcF0SBSr2z3J1w1
bnuM10B1GAIU6DeW9F/wQIMAYBFaRfg8CAQwGQA1UdEdQ/g/8swIfcTBcTbCqTANGtqz
DrGFb21s1G9Y/1x12ZtVIsFbDrBsa1FawKdpK4gU3yY515tSbpmQcSmW3Xe
QCD9QVQGQWEjO7ZmQ4A1UECXMUX3Rhd59pCBBU0QgLC4A0ZAMAAAAAAAACXHMAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EZAROBgjkc1jka/KsAEZFGnJb20L2FVbVgoKjia1k/KsAECFzg3sG0
-----END CERTIFICATE-----
Appendix B. Cross-certification certificates – Generation 1

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

-----BEGIN CERTIFICATE-----
MIIIgzCCB2ugAwIBAgIRZe0DyQyVq9yAGFJK3AqBmpKwvDQYJKoZlhwvzNNiAQELBQw
cEjLMKAaU1EHMCQCukUXGTAx8yNBvAoTEEdsab2JhbFNpZ24bnYt2ECZFArAVBhGV
BAA4dTkdsb2JhbfnZ24g5QsLwQYVDQQZeHZ891YxYxTaMDwEwYWaMhncing
U0BHh6JViZ2E1BHhGvziBB9g91I2AfeWfXsDA1Mjg7wMDAwMDAwFw0yMj1AMjQwMDAw
MDAwMDAwMDAwMEx2AGBgojKoZr20xFArAVBhGVoKjia姬/k/izM2E3Fzdgg2F0
b1ls1sMQwCQVdQQDQgEwzJzogE85+G4A1UECHM9X3r8dS9pCBBuEOgkLSA95H9ZM2Dk
MTYsMTAhBEgNBVAMTFNNYXVrA6qfDXhbGmawKVIENBHmR1cJANBkgqKIG9wQo
AQEEFAD0AcgBFMIICCQKgEAOwEwR80X0N8kKZs8bY7VEAae5u=+QI19cxdK6S0
DkCvKwN95qPlOwDBFmd3eqhntsn1P9x/mhH30I1G2PKgYtuUYVEelntkp2lbqMBj
L39j3PMAYqWVqFipa+Gzr4fUbTVXyDgsjCFYqFHeWk2zy1IYy09mN5uGQAN
DitUt04KJGCciggdYjDn/p/y9c5QH8ZDFu7qyJSJnW91U9d19U9+gintEe6q
sCkx1Pzq2dYIG62Z06Wf61v4QBC8XvKnMPH8Wr4QDquUI7enCyYIFE1B0F8NS
z3HR=s3w2Z0519Y84htdokyPIwI0cTCgCz210/2dILaj3ikLdLFh8VHvWvYV
KENPym8soA0tj2hsh2bDnXlyt1R18B/3Vos10X/2+qupJSzZjV0/3Z8wPUCwRxhrH
rF936okKZROsOay0Uv04VNNs6+eBKEEGTD/PdCNiuU5TBUPFVdEm8tdFt46+6
b/zJfkgkuliDgw8y8ie4RGRc2hbcfM3U5a71/wn/+-GmHMLETL8w501L0eYeoh
z1arLWNRc8gwXvRfoB1y4/k/Kele04BClHe8WBvLo0gDKAI1Wxmn11+SBz9rJSCR
LuoPBomVUS/sJo4XYyY1ojao4Zn/FPK9rVbShloQVMvXyzyBz1ay33KX6Q62+82
V2cCAwUAccAAACBGvagwQSM4A0lIdswEBw/QRawlBj/CSCAfAhA0lDAEAcwq5wy
M1H58gqkgkhiqG8yAPeswewqMyfIKyWSEgUHAGEnM90dHzhB1v83d3ld3s2b2h
HhNpZ24u4yU91C13ic9aAXrcvnkMI3GUG1gBgfFQCaJcRwy8BPrcaMyGvYy
gidMaiWnHdugQaFgF1G1JZm4x3mDvXNv5GIgF18YyGZFUy2U2qd10aCB0AguG
QWvRjYmUqA1gQ1Y5x1IE5dEsb2hJhWpZ24q50IqA1BTigxy2F6FfQwa4gDlH1Eds
b2JhbFNpZ24aLcVWBn3p43y4rJotlGh0dB0i18v3d3ld3s2bJbHnNpZ24y92t
L3J1CqcVncvMrHkHgHEIBDGBAJC12aBqgrgRBFvQCCyDIaHR0cDov
LB3aS3zdUGF0b2l1mLhNVSz3WheeG3tR3rN3IkVSB2APIkYRbQUHAg9wZC0g2RT
dGtoFb21i4VY2z110ZvG1scBamFwA9MiaXmpHdK9y2gYWS51GtpwVQQcyXRL
ZEBgA0Uyq0ZDQlg2yyl11KXs5wZXzn1Gv4CHc31N2CBpbiizBZBcmF0ZSBhZ3J1Z11
bnQwMBIGA1UDEwEB/wIQfIMABAaCCAAwqCQGfCAU1UDDgM5RA8xP0zewX7qyqoBwq
IC8mQFCSQ2QeW07ZnEQMA4lUeCMBH5Rdu9p8kbEwAgCtAAGAAAAAAAACMKH1A
AAAAAAAAAAAAAAAAAAAAAAAAAAAMABCQAgwDQJjBnmNAQ7G7C53Bt3
lWeBmMTBkRqWrfVZ0f3DM9wX9jz11o9drHORwI0V8yz3Jdsmdr2hjHnPZ24y92t
L2d2JaZC2thz2hmmFbk2J1mNybDCBC2YKlYBQHUAQEFeEFJ8MDYGCcGAGUfGB
AzAHipodHROiW18yvb2NoCtDlU2xyMFCvQ21b15j2b0Z3Wm12aGeyYwRvYmUw
QyGijYyWbTQWBMHMqODHA6Iy9zZWN1cmU2UxZvYFmfc21b15j2b0VYF2zXZ0
L2d2JaZC2thz2hmmFbk2J1mNybDCBC2YKlYBQHUAQEFeEFJ8MDYGCcGAGUfGB
AzAHipodHROiW18yvb2NoCtDlU2xyMFCvQ21b15j2b0Z3Wm12aGeyYwRvYmUw
QyGijYyWbTQWBMHMqODHA6Iy9zZWN1cmU2UxZvYFmfc21b15j2b0VYF2zXZ0
-----END CERTIFICATE-----