Dear Sir,

We are the Catalan Agency of Certification (Agència Catalana de Certificació or CATCert). Our aim is to provide digital certification services and promote the usage of digital signature in order to make safer the communications within the Catalan government and the communications (within and for) the Catalan government.

According to the "Mozilla CA Certificate Policy" (MCACP), we are sending you this formal request attempting to fulfill all the requirements that are stated on your Policy:

1.- The certificate data: the names of every CA are listed below and the certificates contained in the attached file named "certificates.zip" and they can also be found on the URLs detailed:

1.1.- CA Acronym: "EC-ACC"

1.1.1.- Actual Name: "Entitat de Certificació de l'Agència Catalana de

Certificació"

1.1.2.- http://www.catcert.net/web/cat/descarrega/acc.crt

1.1.3.- CRL: http://epscd.catcert.net/crl/ec-acc.crl

1.2.- CA Name: "EC-GENCAT"

1.2.1.- Actual Name: "Entitat de Certificació de la Generalitat de Catalunva"

1.2.2.- http://www.catcert.net/web/cat/descarrega/gencat.crt

1.2.3.- CRL: http://epscd.catcert.net/crl/ec-gencat.crl

1.3.- CA Name: "EC-AL"

1.3.1.- Actual Name: "Entitat de Certificació de l'Administració Local"

- 1.3.2.- http://www.catcert.net/web/cat/descarrega/al csrs.crt
- 1.3.3.- CRL: http://epscd.catcert.net/crl/ec-al.crl

1.4.- CA Name: "EC-SAFP"

1.4.1.- Actual Name: "Entitat de Certificació de la Secretaria

d'Administració i Funció Pública"

1.4.2.- http://www.catcert.net/web/cat/descarrega/safs_csrs.crt

1.4.3.- CRL: http://epscd.catcert.net/crl/ec-safp.crl

1.5.- CA Name: "EC-PARLAMENT"

1.5.1.- Actual Name: "Entitat de Certificació del Parlament de Catalunya"

- 1.5.2.- http://www.catcert.net/web/cat/descarrega/parlament_csrs.crt
- 1.5.3.- CRL : http://epscd.catcert.net/crl/ec-parlament.crl
- 1.6.- CA Name: "EC-UR"

1.6.1.- Actual Name: "Entitat de Certificació d'Universitats i Recerca"

- 1.6.2.- http://www.catcert.net/web/cat/descarrega/ur_csrs.crt
- 1.6.3.- CRL : http://epscd.catcert.net/crl/ec-ur.crl

1.7.- CA Name: "EC-IDCAT"

- 1.7.1.- Actual Name: "Entitat de Certificació de idCAT"
 - 1.7.2.- https://www.idcat.net/public/ec-idcat.cer
 - 1.7.3.- CRL: http://epscd.catcert.net/crl/ec-idcat.crl

1.8.- CA Name: "EC-IDCAT"

1.8.1.- Actual Name: "Entitat de Certificació de la Universitat Rovira i

Virgili"

1.8.2.- http://www.catcert.net/web/cat/descarrega/urv_csrs.crt 1.8.3.- CRL: http://epscd.catcert.net/crl/ec-urv.crl

Information about the certification hierarchy of CATCert can be found here:

http://www.catcert.net/web/cat/serveis/cataleg_serveis_jerarquia.jsp

The OCSP service of CATCert can be found at the following URL:

http://ocsp.catcert.net/

2.- Purposes of the certificates issued by every CA:

| | SSL | DS/Enc | Code Signing |
|--------------------|-----|--------|--------------|
| 2.1 "EC-ACC" | YES | YES | YES |
| 2.2 "EC-GENCAT" | YES | YES | YES |
| 2.3 "EC-AL" | YES | YES | YES |
| 2.4 "EC-SAFP" | YES | YES | YES |
| 2.5 "EC-PARLAMENT" | YES | YES | YES |
| 2.6 "EC-UR" | YES | YES | YES |
| 2.7 "EC-IDCAT" | YES | YES | YES |
| 2.8 "EC-URV" | YES | YES | YES |

3.- A CP and CPS: The most updated documents of our CP and CPS are written in Catalan and can be found on our website at the following URL:

http://www.catcert.net/registre

This webpage provides information about both CP and CPS. The documents, though, can be addressed more directly by the URLs:

| http://www.catcert.net/web/cat/descarrega/dpc_catcert.pdf | (for the CPS) |
|---|---------------|
| http://www.catcert.net/web/cat/descarrega/pdc_catcert.pdf | (for the CP) |

We do have English versions of the documents, but they are under revision at the moment due to recent updates.

4.- (statement #8 & #9) Audits:

CATCert is preparing to obtain the following certifications:

- UNE-ISO/IEC 17799
- UNE 71502

CATCert is about to obtain (the certification is has been send and at the moment is being processed by AICPA/CICA since the report has been approved and emitted already by Ernst&Young): • Web Trust CA

Ja ha obtingut informe favorable de l'auditoria (by Ernst&Young): • ETSI TS 101 456

More information about this point can be found on the attached .pdf file "resum UNE.pdf" (in catalan).

5.- Concerning to the requirements that are followed on the certificate signing requests verification (statement #7). CATCert operates two different policies due to the concrete requirements of the two kinds of certificates that it issues:

5.1.- The first one (that is the one that applies to the bulk of certificates that CATCert issues) is based on a policy of trust delegation on different figures that take different roles on the certificate issuance cycle:

5.1.1.- The cycle starts on the figure of the Service Responsible: this is a figure on the end party (the party that requests the certification) and that assumes the responsibility of verifying and ensuring that the provided data for the certification corresponds to the real identity of the certificate subscriber. After verifying the identity of the subscribers, the SR fills up the forms that can be downloaded from our website with the information and sends them to the Registration Entiny (ER). This is an "out of band" proceeding.

5.1.2.- Once the forms arrive to the ER, the operator of the ER (Registration Entity), introduces the information into the system and, if everything is right, approves the request in order to pass it to the next step of the cycle that is the certificate generation process.

5.1.3.- Once the approval of the operator is given, the generation process is engaged from a remote (from the CA) and dedicated machine that generates the key-pair (either from a cryptographic card or software based), the PIN & the PUK, and, if the generation is based on a cryptographic card, part of the data is printed on it (CN, O and OU of the Subject's DN). This point may vary depending on the CA that the certificates are issued from.

5.1.4.- When the process is completed, the cards (or certificates) are sent to the SR that requested them together with a letter with the terms&conditions document and others and, separately, another letter with the PIN&PUK numbers.

5.2.- The second procedure, is the one that corresponds to a certain kind of certificates that are issued for the Catalan citizens. The certificate generation cycle differs from the one described above. The certificates following this procedure are issued only from the CA "EC-IDCat". This procedure came from the big amount of potential subscribers of such certificates that are the catalan citizens (around 6 milion). In this case, the resulting certificate is a software based certificate that is requested from a website. The user/subscriber fills up a web-based form, the key-pair is generated on the user machine and the public key and user data is sent to a server with approval-pending status. Afterwards, the user must go to a ERV (Virtual Registration Entity) to validate his data with the operator of the ERV. If the data is successfully validated, then the request is approved and the certificate generated but it remains stored on the server. Afterwards, the citizen can download it from the same computer where he requested it from and, as soon as he does so, the certificate is automatically installed on his webbrowser.

For more information about these procedures, please refer to the DPC.

Other points:

 Regarding to the statement #13 of the MCACP, we must point that every CA of our hierarchy may issue certificates with different profiles and purposes. As is stated on our CPS (Certification Practice Statement), we have certificates with different purposes (identificacion, signature, encypherment,..) and issued by using different levels of security that are Advanced Electronic Signature Certificates (software based certificates issued on .p12) and Qualified Electronic Signature Certificates (issued by using higher levels of security). Therefore, due to our hierarchy structure there is no way to decide about a certain purpose by the certificate of the CA that issued it only.

Hoping that the information above is going to be useful for the process, please do not hesitate to ask us about any detail that would result unclear or not considered in enough deep for us.

We will look forward to hear from you soon.

Yours sincerely.