Autoridad de Certificación de la Abogacía

Reference: **PDS_ACA.0**
Date: 06724/2016
Document status: **Published**

Consejo General de la Abogacía Española

PDS_ACA.0
PUBLIC KEY INFRASTRUCTURE (PKI) DISCLOSURE STATEMENT OF THE CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA CERTIFICATION AUTHORITY

(PDS_ACA.0)

PDS

PUBLIC KEY INFRASTRUCTURE DISCLOSURE STATEMENT OF THE CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA CERTIFICATION AUTHORITY

Administración ACABOGACÍA
Consejo General de la Abogacía Española
Paseo de Recoletos, 13
28004 Madrid

Changes

Date	Version	Changes
06/24/2016	PDS_ACA.0	Original version

THE MODEL OF THE PUBLIC KEY INFRASTRUCTURE'S DISCLOSURE STATEMENT OF THE CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA CERTIFICATION AUTHORITY (CA) IS HEREIN DEVELOPED. FOR ITS DEVELOPMENT IT HAS BEEN TAKEN INTO ACCOUNT THE STRUCTURE DETAILED IN THE EUROPEAN STANDARD ETSI EN 319 411-1. THIS STATEMENT IS CONSIDERED AS A COMPLEMENTARY INFORMATIVE DOCUMENT OF THE QUALIFIED TRUST SERVICE PROVIDER, BUT IT DOES NOT INTEND TO REPLACE THE CERTIFICATION PRACTICE STATEMENT AND SERVICE PROVIDER CERTIFICATED POLICY.

For more information, please consult our web site http://www.acabogacia.org or contact us via the e-mail address info@acabogacia.org.

Contents

1. Types of Statements

1.1. Service provider's contact information

Organization responsible:
Autoridad de Certificacion de la Abogacia (ACA).
Consejo General de la Abogacia Española (CGAE)

Contact person:
Administrator CA
Operations Department

E-mail:	info@acabogacia.org
Telephone:	Tel. +34902 41 11 41
Fax	+34915327836
Address:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

If the revocation of the qualified trust service provider's certificate is requested, the following communication mechanism would be enabled:

The revocation or suspension proceedings can be initiated on-site, by telephone or on-line by the website of CA.

On-site proceeding:

- Request by the subscriber. The subscriber shall be identified before an operator of its Registered Authority (RA), and manifest in writing their desire to suspend or revoke the certificate. The operator shall carry out the suspension or revocation and inform the subscriber when the process has been completed.

- Suspend by a third party. In the event is a third who presents the request, the operator will perform a series of questions so as to determine the cause of the request, the operator will receive the relevant documentation, and if it considers that the grounds established, it will effectuate the suspension, an interim pending further inquiries suspension. In addition, the operator will also send a message informing the subscriber on the circumstance.

On-line proceeding:

The subscriber of a /license to practice law (*Colegiado*) or employee certificate will have a website www.acabogacia.org from which he/she could request the certificate revocation. To that end, he/she would have to:

- Access to http://www.acabogacia.org
- Select: Users' area → Certificates' management → On-line revocation
- Introduce the Revocation Code given during the certificate generation process.

At the same time the certificate has been revoked, the subscriber would be notified, informing him/her on the reasons, date and hour in which the certificate will cease to have any effect.

The Service for the revocations' management would be available 24 hours per day, 7 days per week. In the event the system or any other element that is not under the control of CA fails, CA will do its best efforts to ensure that this service will not be unavailable for no longer than the maximum period of 24 hours.

The information concerning the status of the revocation will be available 24 hours a day, 7 days a week. In the event the system or any other factor that is not under the control of the CA fails, CA will do its best efforts to ensure that this service information will not be unavailable for no longer than the maximum period of 24 hours.

2. Types of certificates, validation procedures and use

2.1. Types of certificates

Autoridad de Certificacion de la Abogacia (ACA) can issue the following types of certificates:

1. BAR MEMBERSHIP QUALIFIED CERTIFICATE. These are Corporate certificates with a national level that are issued to end-entities natural persons belonging to a Bar Association, meaning, certificates issued with the intervention of their Bar Association acting as a Registrar with the exclusive capacity to certificate the quality of "membership" of a person identified as such in the certificate.

2. ADMINISTRATIVE PERSONNEL QUALIFIED CERTIFICATE. These are Corporate certificates that are issued to end-entities functionally related persons to the Bar Association, Regional Councils of Bar Associations and Consejo General de la Abogacia Española (Spanish National BAR) that act as Registrar or to institutions in connection therewith.

3. AUTHENTICATION OF WEBSITES QUALIFIED CERTIFICATE. These certificates allow to identify and link a certain URL to a certain entity; a Bar Association, Consejo General de la Abogacia Española or Regional Bar Council as well as any legal person related to the practice of law.

4. LEGAL ENTITIES' REPRESENTATIVES QUALIFIED CERTIFICATE. These are Corporate certificates issued to end-entities natural persons with capacity to act on behalf of a legal entity that have relation with Bar Association or with the Institutional Advocacy.

5. ELECTRONIC SEAL QUALIFIED CERTIFICATE. These are Corporate certificates issued to Bar Associations, Consejo General de la Abogacía Española, Bar Associations Councils and, in general, any legal person related in any way to these professions.

6. PROFESSIONAL ASSOCIATION PERSONNEL QUALIFIED CERTIFICATE. These certificates are issued to end-entities natural persons functionally related to a Council or Professional Association that act as Registrar or to institutions in connection therewith

7. EUROPEAN LAWYER QUALIFIED CERTIFICATE. These are Corporate certificates of European level issued to end-entities natural persons that belong to a Bar Association.

8. "THE LAW SOCIETY OF SCOTLAND QUALIFIED CERTIFICATES" QUALIFIED CERTIFICATE. These are certificates issued to end-entities natural persons that belong to "The Law Society of Scotland".

9. "AUTHORIZED" QUALIFIED CERTIFICATE. These are certificates issued to end-entities natural persons that have been authorized to request a digital certificate.

2.2. Validation Procedures

The information related to the suspension or revocation of a certificate is disseminated by *CA* throughout the validation systems enabled to such purpose, which entails the downloading of the CRLs and the online status query of the certificate.

2.3. Certificate´s use

Autoridad de Certificacion de la Abogacia (ACA) certificates may be used according to the terms established by the corresponding Certificate Policy.

BAR Membership Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.10.2.1)
Administrative Personnel Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.10.3.1)
Authentication of websites Qualified Certificate Policy (SSL) (OID 1.3.6.1.4.1.16533.40.1.1
Legal Entities' Representative Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.10.10.1)
Electronic Seal Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.20.3.1)
Professional Association Personnel Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.20.4.1)
European Lawyer Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.10.9.1)
“The Law Society of Scotland Qualified Certificates” Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.20.5.1)
"Authorized" Qualified Certificate Policy (OID 1.3.6.1.4.1.16533.20.6.1)

The use of certificates is prohibited in accordance with the Certification Practice Statement (CPS) and with the specific certification policy that corresponds.

It is prohibited the use for purposes against the Spanish and European Union legislations, the international covenants ratified by Spain, the morals and good habits and the public order. The use for purposes against the Certification Practice Statement (CPS) and the specific certification policy it is not permitted.

The certificates have not been designed, cannot be applied and cannot be used for resale as equipment for the control of dangerous situations nor used for purposes that require a fail-safe test such as the operation of nuclear installations, navigation or air communications systems, or a control arm systems where a system failure could involve death, personal injuries or severe environmental damages.

The end-entities certificates cannot be used to sign in the request system for the certificate´s emission, renovation, suspension or revocation, either for the signing of public-key certificates, nor for the signing of Certification Revocation lists (LRC o CRL).

The Certificates shall be used as it is provided by the AC and therefore, no modification on the Certificate is permitted.

AC does not create, store nor possess the qualified certificate subscriber's private key and therefore it is not possible to recover the encrypted data related to the public key in case of loss or deactivation of the private key or the device that stores it.

The Subscriber or User that decides to encrypt the information, will do it under his or her sole and exclusive responsibility and therefore AC will not have any responsibility concerning the encryption of information using the keys associated with the certificate.

3. Trust Limits

Information audit Logs will be stored for at least 15 years.

All data related to the certificate lifecycle will be kept for the time period established by current legislation. The certificates will be kept published in the repository for at least one year from its expiry date .

The Agreements with subscribers and any information related to the identification and authentication of the subscriber will be kept for at least 15 years or for the time period established by current legislation.

In addition, AC will register and make accessible for the maximum time period established by current legislation, even when the qualified or accredited service provider´s activities have ceased, the information relating to data issued and received by the qualified or accredited service provider so that it can serve for evidence in legal procedures and ensure the service continuity. This register activity can be carry out by electronic means.

Finally, the requirements concerning the log file and the audit logs foreseen in the paragraphs 6.4.5 and 6.4.6 of the European Standard ETSI EN 319 411-1 will be taken into account.

4. Subscribers' obligations

The subscriber of a certificate shall by obliged to comply with the applicable regulation in place, and also to:

- Guard his/her private key in a diligent manner.
- Use the certificate following this Certification Practice Statement (CPS) and the applicable Certificate Policies.
- Respect the documents signed by the RA.
- Inform without delay of the existence of any cause of suspension/revocation.
- Notify any amendments to the data provided for the creation of the certificate during its term of validity.
- Not use the private key nor the certificate after the moment he/her requests its suspension/revocation or after the CA or the RA notifies the same, or after the term of validity has expired.
- Nor those indicated under sections 6.3.5 a) to j) of the ETSI EN 319 411-1 European standard.

Finally, as established under the corresponding certificate policies, the service provider issues qualified certificates for electronic signature and provides electronic signature services based on these, and created using a qualified electronic signature creation device, in accordance with the applicable regulation.

5. Trust parties' obligation to verify the certificates status

The Users shall be obliged to comply with the applicable regulations, and also to:

- Verify the validity of the certificates when performing any operations which are based on such certificates.
- Know and comply with any applicable guarantees, limits and responsibilities when accepting and using the trusted certificates.
- Also with those indicated under sections 6.3.5 k) to m) of the ETSI EN 319 411-1 European standard.

Users who don't use the validation of certificates system made available to them to verify the validity of a certificate, shall consult the Registry of Certificates to trust these.
Any information on the issuance and status of the certificates will be available to the public under the terms established in the applicable regulation.
The CA will keep a safe storage and retrieval of certificates system and a Registry of Certificates and their status. The CA may delegate such functions on a third party. Access to the Registry of Certificates shall be via the website of Autoridad de Certificacion de la Abogacia (ACA) (www.acabogacia.org), or via any other means considered safe by the CA.

6. Discharge / Limitation of liability

The Consejo General de la Abogacia Española (CGAE), as qualified trust services provider, will be liable for any non compliance of the Policies or Statements of certification, and, where applicable, for any non compliance of Act 59/2003 on Electronic Signature, Regulation 910/2014 (eIDAS Regulation) or any regulation developing these.

In addition, the Consejo General de la Abogacia Española will hold any liability towards third parties for the actions of any people on who it delegates the performance of any of the functions required to provide the certification services.

Notwithstanding the above, the Consejo General de la Abogacia Española shall not guarantee the algorithms or cryptographic standards used, nor will it respond for any damages caused by external attacks which these might suffer, provided it had applied due diligence according to the state of the arts at the time, and it had proceeded according to the Policies and Statements of Certification, Act 59/2003, eIDAS Regulation and its developments regulations, where applicable.

Regarding the exclusion of liability (see section 6.8.8. of ETSI EN 319 411-1 European standard), the relationship between the CA and the RA will be subject to its specific contractual bond. The CA and the RA will discharge their liability under the terms established under the Certification Practice Statement and the certificate policies. In particular, the CA and the RA shall not liable in any case for any of the following circumstances:

i. For the use of the certificates, provided it exceeds that established under the applicable regulations and the Certification Practice Statement, in particular, for the use of a suspended or revoked certificate, or for relying on such certificate without having previously verified its status.
ii. For the misuse or fraudulent use of the certificates and certificate validation systems made available to that end.
iii. For the misuse of the information included in the certificate or in the certificate validation systems made available to that end.
iv. For any non compliance with the obligations set forth for the Subscriber or User under the applicable regulation, the Certification Practice Statement or the corresponding Certificate Policies.
v. For the content of the messages or documents signed or encrypted digitally.
vi. For the non retrieval of the documents encrypted with the public key of the Subscriber.
vii. For any fraud within the documents submitted by the solicitor.

In relation to the limit of liability in case of losses for operations, the Consejo General de la Abogacia Española, as Qualified Trust Service Provider, will hold the corresponding

liabilities in accordance with Act 59/2003 on Electronic Signature, the eIDAS Regulation and the rest of the applicable regulation.
The CA will be liable for any damages caused to the Subscriber o any other person who, in good faith, relies on the certificate, if there exists negligence or willful misconduct by the CA, with regards to:

- The accuracy of the information included in the certificate at the time of its issuance.
- The guarantee that, at the time of the delivery of the certificate, the Subscriber has his/her private key corresponding to the given public key or identified on the certificate.
- The guarantee that the public and the private key work together and in a complementary manner.
- The correspondence between the certificate requested and the certificate delivered.
- Any liability established by applicable regulations.

Finally, regarding the financial liability, the CA, as Qualified Trust Service Provider will keep sufficient economic resources to address the risk of liabilities for damages before the users of their services and before third parties, assuming liability over its activity as service provider, as established under the applicable regulation.
In particular, said guarantee is established by means of a civil liability insurance covering at least EUR 3.000.000.

7. Applicable agreements

The provision of trust services by the qualified services provider will be subject to the last version of the Certification Practice Statement and the Certificate Policies from Autoridad de Certificacion de la Abogacia (ACA), which may be found on the website http://www.acabogacia.org, or requesting information on the following email address: info@acabogacia.org.

Currently, according to the Certification Practice Statement, digital certificates can be issued to the following individuals / legal entities:

- BAR Membership Qualified Certificate: for individuals who are members of a BAR Association as a resident member.
- Administrative personnel's certificate: persons that belong to an Association or council of BAR Associations as employees, collaborators or any other associated to them or to an associated entity to such.
- Legal entities: BAR Associations and Councils or entities associated to the institutional legal scenario.
- European certificates: individuals who are members of a BAR Association or of a professional association, as lawyers, in accordance with article 2 of Directive 98/5/EC (OJ No L 77 of 14 March 1998).
- Certificates for authorized representatives of legal entities.

8. Privacy policy

The requirements mentioned in section 6.8.4 of ETSI EN 319 411-1 are generally applicable to the service provider.

On the other hand, the security measures implemented in relation to the personal data processing are mentioned in Annex I to the Certification Practice Statement (CPS).

Likewise, the *CA* will register all the relevant information related to the personal data issued and received by the qualified trust service provider and will keep it available for an appropriate period of time, even after the termination of the activities of the qualified trust service provider, doing so in order to have sufficient evidence in the context of a potential legal procedure and ensure the continuity of the service. This registration activity may be carried out electronically.

Lastly, the relevant requirements related to the retention of the registration information, which are mentioned in section 6.3.4 h) of ETSI EN 319 411-1, will be taken into account in accordance to what has been indicated regarding the retention periods of the Certification Practice Statement (CPS).

9. Return policy

No applicable stipulation according to what has been established in the Certification Practice Statement (CPS).

10. Applicable Law and dispute resolution procedures

10.1. Applicable Law

The following basic legislation is considered as applicable:

- Regulation (UE) No. 910/2014 of the European Parliament and Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter eIDAS) and repealing Directive 1999/93/CE.
- Directive 1999/93/CE of the European Parliament and Council of 13 December 1999 on a community framework for electronic signatures.
  (NOTE: This directive will be repealed when the vast majority of the articles of eIDAS are applicable, i.e. from 1 July 2016).
- Spanish Law 59/2003, of 19 December, on Electronic Signature (consolidated text, last modified 2 October 2015).
- Spanish Royal Legislative Decree 1/1996, of 12 April, approving the restated text of the law on Intellectual Property.
- Spanish Organic Law 15/1999, of 13 December, on Personal Data Protection, and its development Regulation, approved by Spanish Royal Decree 1720/2007, of 21 December.
- Law 11/2007, of 22 June, on electronic Access of citizens to public services (That law was repealed with effect from 2 October 2016, by the derogative disposition .2.b) of Law 39/2015, of 1 October).
- Spanish Law 39/2015, of October 1, on Common Administrative Procedure of the Public Administrations (effective: 2 October 2016).
- Spanish Law 9/2014, of 9 May, on General Telecommunications, which in its sixth final provision reported the amendment of Law 59/2003 of 19 December on Electronic Signature.
- Spanish Law 25/2015, of 28 July, on second chance mechanism, reducing the financial charge and other measures of social order, which in its fourth final disposition reported the modification of Law 59/2003 of 19 December on Electronic Signature.
- Spanish Royal Decree 3/2010 of 8 January, by which the National Insurance Scheme is regulated in the field of eGovernment.
- Spanish Royal Decree 951/2015, of 23 October, amending Royal Decree 3/2010 of 8 January, by which the National Insurance Scheme is regulated in the field of eGovernment.
- Spanish Law 40/2015, of 1 October, on the Legal Regime of the Public Sector (effective: 2 October 2016).

10.2. Dispute resolution procedures

Any controversy or claim arising out of or in relation with this document shall be definitely settled by one arbitrator in the context of the Spanish Arbitration Court, who will perform

the arbitration administration as well as the appointment of the relevant arbitrator/court of arbitration. The parties agree to comply with the rendered arbitration award.

11. Licenses, registered trademarks and audits

11.1. Licenses

The trusted service provider/ qualified trusted service provider Consejo General de la Abogacía Española ("CGAE"), with VAT number Q2863006I and commercial name "*Autoridad de Certificación de la Abogacía*" ("ACA"), is registered within the official list of trusted services, available at:
https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

11.2. Registered trademarks

CA does not undertake any specific commitment when issuing the relevant certificates with respect to the use of any registered trademarks by the subscribers. *CA* does not deliberately permit the use of a name the usage right for which have not been granted to the subscriber. However, *CA* is not obliged to look for evidence in relation to the possession of registered trademarks before the issuance of the relevant certificates.

11.3. Audits

In compliance with the Regulation 910/2014, the trusted service provider/ qualified trusted service provider will be subject to an audit, at least every 24 months.

In accordance to the Regulation 910/2014, the referred audits shall be conducted by the relevant conformity assessment body, and the auditors shall comply with the requirements referred in ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

Likewise, Webtrust audits may be performed by a first-level audit firm in accordance with the *WebTrust for Certification Authorities*' Criteria, which can be downloaded from *http://www.aicpa.org*, and which have been developed by the AICPA (American Institute of Certified Public Accountants, Inc.) and the CICA (Canadian Institute of Chartered Accountants).

The WebTrust Principles and Criteria are consistent with the standards developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).