MINISTERIO DE TRABAJO
Y ECONOMÍA SOCIAL

SUBSECRETARÍA

S.G. DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIONES

Ministry Trust Service Provider
PKI Disclosure Statement

Version Control

Identifier	D006
Title	Ministry Trust Service Provider PKI Disclosure Statement
Version	06
Document status	Approved
Approval date	20200615

Change Control

Version	Date	Comment
01	20170406	English version.
02	20180710	The name of the Ministry has been updated. DIR3 code has been updated. Date format compliant with ISO8601: YYYYYMMDD. Limits of use updated with the expected life-time of public key certificates. Privacy policy updated. Supervisory Body name updated.
03	20190612	Expiration date removed. Supervisory body updated (generic). Added remark from Supervisory Body about signatories (subscribers) and electronic signature creation data custody in the introduction. Applicable law and complain section updated.
04	20190613	DIR3 Updated. Added LOPDGDD.
05	20191004	New section added with the terms and conditions for certificate revocation information.
06	20200615	The name of the Ministry has been updated. DIR3 code has been updated. TSPM term used in all the document instead of PSCM. CPS term used in all the document instead of DPCM. Section 6 about certificate revocation information updated and aligned with the CPS. Annex A added with the URLs.

Table of contents

1 Overview

This document is for information purposes only and under no circumstances replaces the Certification Practice Statement (hereinafter CPS, DPCM in Spanish) which users of the TSPM (Ministry Trust Service Provider) certificates are required to comply and be familiar with.

The CPS, available on URL http://ca.empleo.gob.es/meyss/DPCyPoliticas, is a public statement of the practices that the TSPM, as Trust Service Provider, CA employs in issuing, suspending, revoking and renewing certificates and other trusted services; and providing access to them, in accordance with specific requirements.

Article 3 of Regulation (EU) 910/2014 defines the signatory (subscriber of an electronic certificate) as "a natural person who creates an electronic signature", while its annex I indicates that qualified certificates shall include "at least the name of the signatory or a pseudonym".

Likewise, Regulation (EU) 910/2014 defines in its article 3.13) the "electronic signature creation data" as "unique data which is used by the signatory to create an electronic signature". For its part, article 24.1 of Law 59/2003 states that "the electronic signature creation data is the unique data, such as codes or private cryptographic keys, that the signatory uses to create the electronic signature".

In this sense, the liability of the Trust Service Providers is limited to the damages and losses caused, in case of negligence on the part of the signatory in the preservation of their electronic signature creation data, in the assurance of their confidentiality and in the protection of all access or revelation.

Consequently, electronic certificates are for personal and non-transferable use and all necessary precautions must be taken to avoid their improper use thereof. The possibility that the subscriber / signatory of an electronic certificate issued to its name transfers their possession and discloses their access codes to a third party, is not in accordance with current national and EU legislation in the area of trusted electronic services.

2 Trust Service Provider contact information

Subdirección General de Tecnologías de la Información y las Comunicaciones
Paseo de la Castellana 63
28071 Madrid
admin_ca@mtin.es / admin_ca@meyss.es
Phone number: 91 363 11 88/9 - Fax: 91 363 07 73

3 Certificate types

The TSPM issues, revokes and provider validation data about the following types of electronic certificates:

1. The Public Employee[1] Certificate for electronic signature as a means to electronically sign documents and proceedings. This certificate is issued on a smart card.
2. The Public Employee Certificate for authentication as a means to identify and authenticate a Public Employee in computer systems and applications. This certificate is issued on a smart card.
3. The Public Employee Certificate for authentication as a means to electronically sign documents and proceeding as well as to identify and authenticate a Public Employee in computer systems and applications. This certificate is issued and manage by a central HSM.

[1] Any Public Employee Certificate includes both the subscriber and the public entity in which the public employee works

4. The Electronic Seal Certificate for Public Administration, entity, public entity, or public law entity as a means to automated electronic administrative proceedings of the Public Administrations.

These electronic certificates are qualified[2] according to eIDAS[3] requirements.

The Inclusion in the list of trusted certification service providers (TSL) of Spain, can be verified through the electronic site of Spanish Supervisory Body on the URL https://sede.minetur.gob.es/

4 Limitations of use

The use of these certificates is limited to the different functions of the subscribing Public Administrations, acting through the public employees at their service as signatory, according to their title, employment and authorization conditions and powers.

The maximum expected life-time of public key certificates issued by the TSPM is 5 years.

5 Subscriber requirements

The subscriber (subject) for each type of certificate, according to policies and CPS, shall:

- Provide accurate data information for issuing the certificate and inform the TSPM about any modification.
- Know, accept, and comply with the limits of use of the certificates. The acceptance occurs after being properly authenticated and being able to generate the electronic certificate.
- Guarantee the custody of the private key linked to the certificate, avoiding loss, copy or non-authorised use.
- Request the certificate revocation as soon as possible if any of the information stored in the certificate has changed or there has been a loss of trust in the private key linked to the certificate.
- Not monitor, manipulate or perform reverse engineering operations on the certificate and its linked private key.
- Neither transfer nor delegate to a third party the requirements and obligations on the issued certificate.

6 Certificate status checking requirements for any relying party

The TSPM provides services to relying parties for checking the status of the certificates at any moment including status information beyond expiry or if it has been revoked. The certificate status information is reliable, publicly, automated, and internationally available at any moment, and free of charge. Both OCSP service and CRL are supported.

The TSPM ensures a level of service, ensuring the availability of all the certification services that offers, in special services related to certificate status information. The TSPM guarantees the integrity and authenticity of the certificate status information.

The service is available on-line 24 hours per day, 7 days a week. Upon system failure, the Business Continuity Plan shall be launched in order to solve the incident as soon as possible and ensure that the service is available.

In the case of expiration of any certificate from the TSPM CA or SubCA: in a period prior to the expiration time that will be set based on the certificate validity time issued by said CA:

- the issuance of new certificates will be stopped

[2] The Public Employee Certificate for authentication is the only one that is not qualified

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, concerning electronic identification and trust services for electronic transactions in the internal market.

- close to the expiration date, the existence of any active issued certificate will be reviewed, revoking when appropriate and a last CRL will be issued
- the OCSP service will continue to be offered by signing the responses with a certificate issued by a Certification Authority other than the expired one.

In the event of termination of the TSPM, the TSPM will issue a final CRL which will be published on the TSPM website indicated by the *cRLDistributionPoints* field. This website will be maintained for at least 15 years by the department that would replace the current Ministry. The new department will decide the feasibility of maintaining the OSCP service.

6.1 Revocation status service by CRL issuance

Each certificate issued specifies the address of the corresponding CRL, using the *cRLDistributionPoints* extension. The Certificate Revocation Lists (CRL) of the final entity are released at least every 24 hours, or when a revocation occurs and has a validation period of 24 hours. The location of the CRL is in Annex A: Links (URLs).

The state change of the validity of a certificate is indicated in a CRL in less than 5 minutes elapsed from the occurrence of such change. This means that the maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate is 5 minutes.

The TSPM does not remove certificates from revoked CRLs after they have expired and includes the X.509 *ExpiredCertsOnCRL* extension as defined in ETSI EN 319 411-1[4].

The last CRL exists as there are no more valid certificates in the scope of the CRL, when the certificate that signs the CRL expires, or when the private key of the certificate that electronically signs the CRL is out of order.

The TSPM will preserve the integrity and availability of the last CRL for 15 years as specified by the LFE preferably using long-term valid signatures in accordance with standard formats.

The TSPM will not issue a last CRL until all certificates within the CRL are expired or revoked.

6.2 OCSP revocation status service

The TSPM provides certificate status verification via OCSP, according to IETF RFC 6960[5] indicating that fact inside the certificates, using the extension *AuthorityInfoAccess* defined in technical specifications IETF RFC 6818[6] and RFC 6960, as follows:

- Access description is included, indicating the OID reserved for OCSP service access and the URL where the OSCP server is located.

The OCSP service returns in its response the *archiveCutOff* extension, as specified in IETF RFC 6960, with the *valid from* value of the Certification Authority certificate in the *archiveCutOff* date field.

The location of the OCSP service is in Annex A: Links (URLs).

The TSPM will offer the OCSP service once the root certificate has expired or its certification services have ended in accordance with what is specified by the LFE and the standard ETSI EN 319 411-1 from the location stated in the field of the certificates.

[4] ETSI Europe 319 411-1. Policy and security requirements for Trust Service Providers issuing certificates. Part 1: General requirements

[5] IETF RFC 6960: "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[6] IETF FRC 6818: “Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7 Revocation checking requirements for relying parties

Any relying party that relies on TSPM certificates shall:

- Determine that such certificate provides adequate assurances for its intended use as defined in CPS and Certificate Policies (CPs).
- Verify that the certificate validity by ensuring that the certificate has not expired.
- Ensure that the certificate has not been suspended nor revoked by accessing current revocation status information available at the location specified on the fields of the certificate to be relied upon.

The certificate status could be verified through the OCSP service provided by the TSPM, available at the URL specified on the fields of the certificate whose status is been checked.

8 Limitations of liability

The TSPM shall only be liable for the issue and delivery of certificates and, for key pairs and secure authentication devices (for authentication, electronic signature, and verification of electronic signatures).

The TSPM shall add a clause, in the contract agreement with the subscriber, which states that in no event shall the TSPM be held liable due to the issue and use of the certificate when:

- The subscriber provided false or wrong data information for the certificate.
- The subscriber was negligent in protecting the private key, in the use of a trusting service, or in maintaining right conditions to avoid the compromise, loss, dissemination, modification or non-authorised use of that key.
- The subscriber uses names (surnames, emails, or domain names), or any other certificate information against the intellectual or industrial property rights.

In no event shall the TSPM be held liable by any relying party when:

- Any relying party does not comply with the requirements.
- Any relying party trusted on the certificates under some not recommended circumstances.
- Any relying party trusted on the certificates, without any validation status to check if this was revoked or suspended.

The TSPM shall not be liable in the case of acts of fortuitous event, or force majeure.

In the event of termination of the activity as Trust Service Provider, the TSPM shall inform about this event, duly and sufficiently in advance, to the subscriber of the certificates, as well as the users of the affected services. The TSPM will transfer, with the express consent of the subscribers, those valid certificates on the effective date of the cessation of the activity, to another Trust Service Provider. If this transfer is not possible, the certificates will be revoked.

9 Privacy policy and data protection

According to article 14 in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), we inform you that the Subsecretary of the Ministry of Labour and Social Economy (Ministerio de Trabajo y Economía Social, in Spanish) is the controller for all personal data used for providing trusting services, that is, for the management of public employee and electronic seal public key certificates issued by the Ministry.

The Subsecretary, through its Trust Service Provider, carries out the data processing following the existing regulation on personal data protection, information security and its own activity regulation that allows the data processing, mainly the Public Employee Statute, the law 39/2015, and the law 40/2015, which regulate how the Public Administration and its public employees must operate.

In this sense, technical and organizational security measures have been adopted in order to guarantee the security of the personal data and avoid its unauthorized alteration, processing or access, responsible for causing material and immaterial damages. All the security measures have been adopted taking into account the current technology, the data categories and the degree of risks and are periodically reviewed in order to ensure that the measures are updated according to new risk scenarios.

As the main controller for all data subject and according to information requirements of article 14 in GDPR, the Subsecretary states the following basic information for data processing:

Data Controller	Subsecretaría del Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España (Spain) email: sgtic@meyss.es
DPO	Data Protection Officer (Delegado de Protección de Datos) Ministerio de Trabajo y Economía Social Paseo de la Castellana 63 Madrid 28071 España (Spain) email: dpd@meyss.es
Purpose and legal basis	Providing trusting services including the management of public employee and electronic seal public key certificates according to the Public Employee Basic Statute and 39/2015 and 40/2015 laws.
Data categories	Identification data: NIF/DNI, name and surnames, birth date, email, job description, entity. Other data: public and private key, certificate serial number, certificate request code.
Data origin	Database with the Ministry Public Employees SG de Recursos Humanos (Human Resources Area) Ministerio de Trabajo y Economía Social
Data transfer	Data transfer to police and justice bodies according to law. Certificate public data.
International data transfers	No international transfers outside EU are allowed.
Cancellation period	15 years according to regulation
Automated decision making	There is not any automated decision-making including profiling with the data subject

Subject rights: Subjects can exercise the right of access, the right to rectification, to erasure (to be forgotten), to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, in accordance with the provisions of articles 15 to 22 of the GDPR.

How to exercise these rights: by contacting the controller electronically, or through any Registry Office according to 39/2015 law.

Should you have any questions about your personal data or exercising your rights, please contact with the DPO (article 38.4 GDPR).

Right to lodge a complaint with a supervisory authority: please contact with Agencia Española de Protección de Datos (Spanish Data Protection Agency) at Jorge Juan 6 street. 28001. Madrid. España (Spain). (http://www.aepd.es).

10 Governing law, complaints and dispute resolution

The provision of trusted services of the TSPM will be governed by the provisions of the Laws of the Kingdom of Spain.

The law applicable to the provision of services, including the certification policies and certification practices, is the Spanish law, in particular:

- 39/2015 Law, October 1st, about Common Administrative Procedure of the Public Administrations.
- 40/2015 Law, October 1st, about Legal Framework of the Public Sector.
- The Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- 59/2003 Law, December 19th, about Electronic Signature.
- The Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR in short).
- 3/2018 Organic Law, December 5th, about Personal Data Protection and Digital Rights Guarantee (LOPDGDD).
- The Royal Decree 951/2005, July 29th, which establishes the general framework for the improvement of quality in the Spanish Central State Administration.

The procedure for submitting complaints and suggestions can be found on the following web page:

http://www.mitramiss.gob.es/es/contacto_ministerio/quejasysugerencias/quejas.htm

Annex A: Electronic Links (URLs)

Email Organization Data:

admin_ca@meyss.es

CPSM, Certificate Policies, PDS and Terms and Conditions:

http://ca.empleo.gob.es/meyss/DPCyPoliticas

https://ca.empleo.gob.es/en/CA_MEYSS/declaracion.htm (English version)

CA Root certificate, SubCA certificates and OCSP certificate:

http://ca.empleo.gob.es/meyss/certificados

OCSP Service Validation Status:

http://ca.empleo.gob.es/meyss/ocsp

CRL Root - AC RAIZ MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz

http://ca2.empleo.gob.es/meyss/crl/MEYSSAutoridadRaiz

CRL - SUBCA1 MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA1

http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA1

CRL - SUBCA2 MEYSS:

http://ca.empleo.gob.es/meyss/crl/MEYSSSubCA2

http://ca2.empleo.gob.es/meyss/crl/MEYSSSubCA2