



TCAB-002CA02-CAR-2018-411

Client Ivnosys Soluciones

Project TCAB-002CA02

Date 06/08/2018

Report TCAB-002CA02-CAR-2018-411

Version 2.0

Author Ana Andrés

Contents

1	CONFORMITY ASSESSMENT BODY INFORMATION	5
1.1	DATA OF THE CONFORMITY ASSESSMENT BODY	5
1.2	DATA OF THE ACCREDITATION BODY	6
1.3	ACCREDITATION CERTIFICATE.....	6
2	ASSESSMENT DATA	7
2.1	DATA OF THE ELECTRONIC TRUST SERVICES PROVIDER	8
3	AUDIT SUMMARY.....	9
3.1	ASSESSMENT SCOPE	9
3.2	ASSESSED CERTIFICATION SERVICES	10
3.2.1	<i>Certification Authority (CA)</i>	11
3.2.2	<i>Documentary Review</i>	12
3.2.3	<i>On-site Inspection</i>	12
3.3	CHANGES SINCE THE LAST ASSESSMENT	12
4	ASSESSMENT RESULTS	13
4.1	KINDS OF DISCOVERIES	13
4.2	DISCOVERIES	13
5	COMPLIANCE WITH ETSI EN 319 411-1	15
5.1	REQUIREMENTS FOR CERTIFICATION PRACTICE STATEMENTS	15
5.2	CERTIFICATE POLICY NAME AND IDENTIFICATION	16
5.3	PARTICIPANTS IN THE PKI	17
5.3.1	<i>Certification Authority (CA)</i>	17
5.3.2	<i>Subscriber and Subject</i>	18
5.3.3	<i>Others</i>	19
5.4	CERTIFICATE USAGE	19
6	TRUST SERVICE PROVIDERS PRACTICES	20
6.1	PUBLICATION AND REPOSITORY RESPONSIBILITIES	20
6.2	IDENTIFICATION AND AUTHENTICATION.....	21
6.2.1	<i>Naming</i>	21
6.2.2	<i>Initial Identity Validation</i>	22
6.2.3	<i>Identification and authentication for Re-key requests</i>	26
6.2.4	<i>Identification and authentication for revocation requests</i>	27
6.3	OPERATIONAL REQUIREMENTS OF THE CERTIFICATE LIFECYCLE	28
6.3.1	<i>Certificate Request</i>	28
6.3.2	<i>Processing of certificate applications</i>	29
6.3.3	<i>Certificate Issuance</i>	29
6.3.4	<i>Certificate Acceptance</i>	31
6.3.5	<i>Key pair and certificate usage</i>	33
6.3.6	<i>Certificate renewal</i>	34
6.3.7	<i>Certificate Re-key</i>	35
6.3.8	<i>Certificate modification</i>	35
6.3.9	<i>Certificate revocation and suspension</i>	36
6.3.10	<i>Certificate status services</i>	37
6.3.11	<i>End of subscription</i>	37
6.3.12	<i>Key escrow and recovery</i>	38
6.4	FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS.....	39

6.4.1	General	39
6.4.2	Physical security controls.....	40
6.4.3	Procedural controls.....	41
6.4.4	Personnel controls	42
6.4.5	Audit logging procedures	43
6.4.6	Records archival	44
6.4.7	Key changeover.....	44
6.4.8	Compromise and disaster recovery	45
6.4.9	Certification Authority or Registration Authority termination	46
6.5	TECHNICAL SAFETY CONTROLS	47
6.5.1	Key pair generation and installation	47
6.5.2	Private key protection and cryptographic module controls.....	49
6.5.3	Other aspects of key pair management	50
6.5.4	Activation Data.....	51
6.5.5	Computer security controls.....	52
6.5.6	Life cycle security controls	53
6.5.7	Network security controls.....	53
6.5.8	Timestamping	54
6.6	CERTIFICATE PROFILES, CRL AND OCSP.....	55
6.6.1	Certificate Profile	55
6.6.2	CRL Profile.....	56
6.6.3	OCSP Profile	57
6.7	COMPLIANCE AUDIT AND OTHER ASSESSMENT	58
6.8	OTHER ASPECTS AND LEGAL ISSUES.....	58
6.8.1	Fees.....	58
6.8.2	Financial responsibility	59
6.8.3	Confidentiality	59
6.8.4	Privacy of personal information	60
6.8.5	Intellectual property rights	60
6.8.6	Representations and warranties.....	61
6.8.7	Disclaimers of warranties	61
6.8.8	Limitations of liability	62
6.8.9	Indemnities	62
6.8.10	Term and termination	63
6.8.11	Individual notices and communications with participants.....	63
6.8.12	Amendments.....	63
6.8.13	Dispute resolution procedures	64
6.8.14	Applicable Laws.....	64
6.8.15	Compliance with applicable law.....	64
6.8.16	Miscellaneous provisions.....	65
6.9	OTHER PROVISIONS	65
6.9.1	Corporate.....	65
6.9.2	Additional testing	66
6.9.3	Disabilities	66
6.9.4	Terms and conditions	67
7	COMPLIANCE WITH ETSI EN 319 411-2	68
8	DOCUMENTS.....	73
8.1	TRUST SERVICE PROVIDER'S DOCUMENTS	73
8.2	GENERAL DOCUMENTS.....	74
8.2.1	Documents used in ETSI EN 319-411-1	75
8.3	OTHER DOCUMENTS	75



9	ABBREVIATIONS LIST	76
10	CERTIFICATE OF ACCREDITATION OF THE CONFORMITY ASSESSMENT BODY	78

1 Conformity Assessment Body information

1.1 Data of the Conformity Assessment Body

Name	Trust Conformity Assessment Body S.L..
VAT Number (VIES)	ES-B87459335
Registry	Company registered in the Mercantile Registry of Madrid, volume 34302, page 24, section 8, page M-617071
Address	Francisco Giralte, 2 28002, Madrid (España)
Main web page	http://tcab.eu/
Representative	Ainhoa Inza
Telephone	+34 91 782 48 55
Email	ainza@tcab.eu
Accreditation number	166/C-PR333
Accreditation date	20/07/2018
Certificate URL	https://www.enac.es/documents/7020/8b50f045-8ed2-4d1f-a6a2-31f6970e6316
Certificate URL (Technical Annex)	https://enac.es/documents/7020/6aa99e14-7f23-443c-92c5-1bb61512dc2c

1.2 Data of the Accreditation Body

Name	ENAC Entidad Nacional de Acreditación
VAT Number	G-78373214
Address	C/ Serrano 240, 3ª 28016 Madrid (España)
Main web page	http://www.enac.es
Telephone	+34 91 769 85 04
Email	operaciones@enac.es

This section complies with **REQ-ETAD-2**.

1.3 Accreditation Certificate

TCAB is nowadays accredited according to the criteria in the standard ETSI EN 419 403, UNE-EN ISO/IEC 17065 and RDE-16, published by ENAC, for the Certification activities defined in the Technical Annex No 166/C-PR333.

The accreditation certificate is included in section 10 "Certificate of accreditation of the conformity assessment body", complying with **REQ-ETAD-3**.

2 Assessment Data

The trust service was assessed in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2 relevant requirements. The fulfilment of these requirements has been verified by evaluating the corresponding documents of the TSP and by an on-site audit of the TSP location.

Project	TCAB-002CA02
Audit date/s and location	Documental review was performed on the 27 th , 30 th , 31 st July and 1 st August, 2018 On-site assessment took place on the 2 nd and 3 rd of August 2018 in Paterna (Valencia)
Audit length	6 days
Standard/s	EIDAS (Regulation UE 910/2014)
Kind of audit	Certification
Audited area – Scope	<i>Servicio de expedición de certificados electrónicos cualificados de firma electrónica.</i> Qualified electronic certificates for electronic signatures issuance service.
Audit team	
Lead Auditor	Ana Andrés (REQ-ETAD-4)
Auditor	Ainhua Inza
Report Date	06/08/2018

2.1 Data of the Electronic Trust Services Provider

Name	IVNOSYS SOLUCIONES S.L.
VAT number:	B98333362
Registry	Company registered in the Mercantile Registry of Valencia, volume 9306, Book: 6588 page 60, section 8, page V143049
Address	C/ Acceso Ademuz 12 – 1º – Of. 1., 46980 Paterna (Valencia).
Main web page	http://ivnosys.com/en/home/
Representatives	Alicia Jimenez Villa – Quality Manager
	Victor Alberto Tortosa Tortosa – Operations Manager
Telephone	+34 96 003 12 03
Email	info@ivnosys.com

3 Audit Summary

3.1 Assessment Scope

The certification assessment has been performed of the following trust service:

Qualified electronic certificates for electronic signatures issuance service (*Servicio de expedición de certificados electrónicos cualificados de firma electrónica*, as stated in the accreditation certificate).

Specifically, the qualified electronic certificates issuance included in this assessment scope are for QCP-n in accordance with the policy detailed below as defined in ETSI EN 319 411-1:

Qualified certificate type		OIDs
	I	IVNOSYS SOLUCIONES
	E	ETSI EN 319 411-2
Natural persons related to an organization (<i>Corporativo</i>)	I	1.3.6.1.4.1.47304.4.16.1.2.2
	E	0.4.0.194112.1.0
Natural persons acting as Legal representative (<i>De Representante con Poderes Generales de Representación</i>)	I	1.3.6.1.4.1.47304.4.16.1.3.1.2
<ul style="list-style-type: none"> Legal entity (De Persona Jurídica) Non-legal entity (De Entidad Sin Personalidad Jurídica) 	E	0.4.0.194112.1.0
Natural persons acting as Representative before Public Administration, aka Proxy to Civil Service (<i>De Representante para Trámites con las AAPP</i>)	I	1.3.6.1.4.1.47304.4.16.1.3.2.2
<ul style="list-style-type: none"> Legal entity (De Persona Jurídica) Non-legal entity (De Entidad Sin Personalidad Jurídica) 	E	0.4.0.194112.1.0
Natural persons acting as Representative of authorized persons (<i>De Representante para Apoderados</i>)	I	1.3.6.1.4.1.47304.4.16.1.3.3.2
<ul style="list-style-type: none"> Legal entity (De Persona Jurídica) Non-legal entity (De Entidad Sin Personalidad Jurídica) 	E	0.4.0.194112.1.0

These certificates are Qualified Certificates where the electronic signature creation data related to the electronic signature validation data is not located in a QSCD. These contain the QC statement for policy QCP-n as required by ETSI EN 319 412-5.

The assessment has been performed in accordance with the European standards and regulations, in particular:

- 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
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Certificates; Part 1: General Requirements.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

The following headquarters have been visited:

- Ivnosys Soluciones, S.L. - Acceso de Ademuz, 12 – Floor 1– Office 1. Paterna (Valencia).

3.2 Assessed Certification Services

The following certification services have been assessed:

- Registration service
- Certificate generation service
- Distribution/Dissemination service
- Revocation management service
- Revocation status service
- Provision of devices to the interested parties

Registration will be performed by the head office located in Paterna (Valencia), at public administrations or at companies acting as Enterprise RA. The services of data centre housing are carried out by AC Camerfirma (compliant with the eIDAS Regulation) and a third party acting as subcontractor for the non-critical processes.

All registration authorities will be operated under the same processes and security requirements, compliant with AC Camerfirma requirements as per its eIDAS certification.

In addition, the information security risk analysis and organizational reliability were considered during the assessment.

3.2.1 Certification Authority (CA)

The root CAs, the intermediate CAs and the certificates they issue have been evaluated. Its data, as downloaded from the **policy.ivsign.net** website, are:

The root CA is AC Camerfirma's 'CHAMBERS OF COMMERCE ROOT – 2016', belonging to external company AC Camerfirma, identified as follows:

Distinguished Name (DN)	CN = CHAMBERS OF COMMERCE ROOT – 2016 O = AC CAMERFIRMA S.A. 2.5.4.97 = VATES-A82743287 SERIALNUMBER = A82743287 OU = CHAMBERS OF COMMERCE ROOT – 2016 OU = see current address at www.camerfirma.com/address L = MADRID S = MADRID C = ES
Digital footprint	2D:E1:6A:56:77:BA:CA:39:E1:D6:8C:30:DC:B1:4A:BE:22:A6:17:9B
Certificate URL	http://www.camerfirma.com/certs/test_chambersofcommercero-2016.crt

This root certificate belongs to a company that is already EIDAS compliant and has been assessed by another Conformity Assessment Body. At the moment of performing the assessment, AC Camerfirma is certified, and this root certificate is included in the TSL (Trust Service Status List) managed by Ministry of Economy and Business (through its Secretary of Digital Progress).

The CA belonging to Ivnosys Soluciones, **IvSign CA**, used for the certificate emission is a subordinate CA (intermediate CA) of the previous root CA and is identified as follows:

Distinguished Name (DN)	CN = IvSign CA O = IVNOSYS SOLUCIONES S.L. 2.5.4.97 = VATES-B98333362 OU = see current address at https://psec.ivnosys.com/address L = PATERNA C = ES
Policy OID	2.23.140.1.2.2 Compliant with Baseline Requirements – Entity identity asserted
Area	Unión Europea
Digital footprint	FB:E1:29:07:2D:AC:2B:1A:AB:69:C3:B6:91:94:78:8D:EC:5D:BE:7B
Certificate URL	http://ca.ivsign.net/certs/IVSIGNCA.crt

This section complies with **REQ-ETAD-7**.

3.2.2 Documentary Review

The evaluation of CPS together with the service provider's documents listed in section 0 and the risk analysis assessment were performed by Ana Andrés.

This documentary review was performed on the on the 27th, 30th, 31st July and 1st of August 2018.

3.2.3 On-site Inspection

This inspection has been carried out in Paterna, Valencia and has included the collection of evidence by sampling of the correct operation of the technical and organizational processes related to the scope of the audit.

This inspection has been carried out by lead auditor Ana Andrés and auditor Ainhoa Inza on 2nd and 3rd of August, 2018. The participants belonging to the Trust Service Provider have been:

- Alicia Jimenez Villa – Quality Manager
- Victor Alberto Tortosa Tortosa – Operations Manager
- Rubén Curiel Vergara – IT Systems Manager
- Ester Cerveró Avellán – RA Operator

3.3 Changes since the last assessment

Previous assessment was carried out during TCAB's accreditation process, and, as TCAB was not yet accredited, it is not considered under the accreditation. However, there has been no organizational or technical relevant changes since then.

The scope for their ISO 27001 certification has changed to cover all operations and services, including specifically the trust services provided within eIDAS. Seen certification granted in the assessment body website.

4 Assessment Results

4.1 Kinds of Discoveries

- **Major Nonconformity (NC-M):** Systematic and critic breach against a certain Section of the reference Standard/s or a stablished procedure, in such a way that the safety or continuity of the services, processes or activities cannot be guaranteed. Its appearance entails the initial non-certification or the loss of the existing one. It requires immediate corrective actions.
- **Minor Nonconformity (NC-m):** Punctual (non-systematic) and non-critical breach of reference Standard (s) Section or an established procedure, so that even if it is a System failure, the security or continuity of the services, processes or activities can be guaranteed. Its appearance in an audit is a warning sign, but never implies the initial non-certification or the loss of the existing one. A large number of them may be an indicator of the precariousness of the system and constitute as a whole a very serious breach. It requires corrective actions.
- **Observations (OBS):** Not recommendable situations with deviation risk potential in a future that the auditor may have to reveal. They do not require Corrective Actions.
- **Improvement Opportunity (IO):** detected by the auditor to increase the efficiency of the System, processes or activities.

4.2 Discoveries

The documentary review and the on-site inspection have been performed for the following Policies:

- Política de Certificación de certificados de Persona Física
 - Reference (OID): 1.3.6.1.4.1.47304.4.
 - Available at: [http:// policy.ivsign.net](http://policy.ivsign.net)

As a summary, it has been identified:

Major Non-conformities: None

Minor Non-conformities: None

Observations:

- **OBS 01** Document control should be reinforced for the documentation related to the CPS. All evidences for eIDAS should be treated as the rest of documents.
- **OBS 02.** The use of the registration platform requires personal data transfer to **Deloitte**, but user acceptance of this personal data management is not collected at the moment.
- **OBS 03.** The identification of the person who requests the revocation of a certificate can be improved to avoid impersonation.
- **OBS 04.** Include further data verification in the RA operations such as DNI (Citizen ID

card) validity, that the mail address provided is a corporate one or one that requires identification before being supplied, and is not used by several persons.

- **OBS 05.** The security measures in **NixVal** to restrict access to equipment areas are correct but could be improved or have compensatory measures.
- **OBS 06.** The complete internal OID structure is documented but not formalized. It is within an internal wiki instead of the documented management system.
- **OBS 07.** It is not documented the non-discriminatory policy.
- **OBS 08.** It is recommended to add organizational measures to avoid fraud when technical measures are not feasible in cases when an operation needs further independence. For example, revocation, that can be performed by the same RA operator that issued the certificate.
- **OBS 09.** The web is not complying with accessibility recommendations.

Improvement Opportunities:

- **IO 01.** Since the legal person representative (proxy or Power of Attorney) certificate profile already complies with the specifications issued by the Finance and Public Administration Ministry (*General Secretariat of Digital Administration*) Certificate profile 2.0¹, it is recommended to mention it the policy.
- **IO 02** To evaluate the use of double factor authentication for the systems that store personal data and in the revocation process.

In the following sections, the results of the documentary review and on-site inspection carried out, together with the evidence gathered and the determined compliance status, are detailed.

This report shall be interpreted as a complementary item to the main Conformity Assessment Report, TCAB-002CA01-CAR-2018-E, and should never be considered as independent.

¹ https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

5 Compliance with ETSI EN 319 411-1

Compliance assessment in this report will be included in context with the standard requirement (framed text). Evaluation and evidence reviewed will indicate how the TSP complies with the framed requirement.

5.1 Requirements for Certification Practice Statements

ETSI 5.2 Certification Practice Statement requirements

The general requirements specified in ETSI EN 319 401 [8], clause 6.1 shall apply. In addition the following particular requirements apply:

NOTE 1: A TSP can document practices relating to specific CP requirements separate from the main CPS document.

a) The TSP CPS should be structured in accordance with IETF RFC 3647 [i.3].

b) The CPS shall include the complete CA hierarchy, including root and subordinate CA's.

c) The CPS shall include the signature algorithms and parameters employed.

d) The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.

NOTE 2: The TSP is not obliged to disclose any aspects containing sensitive information.

e) [PTC]: Clause 2.2 of BRG [5] and clause 8.3 of EVCG [4] shall apply.

f) [PTC]: Clause 2 of the BRG [5] and clause 8.2.1 of EVCG [4] shall apply.

g) The TSPs CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.

Documentary Review	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

The CPS is available in **policy.ivsign.net**, v0.1 dated 16/01/18, updated and according to specifications.

On-site inspection	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

Seen website with the information required.

5.2 Certificate Policy name and identification

ETSI 5.3 Certificate Policy name and identification

As described in IETF RFC 3647 [i.3], clause 3.3, certificates include a CP identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application. The identifiers for the certificate policies specified in the present document are:

- a) NCP: Normalized Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)
 - b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)
 - c) LCP: Lightweight Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)
 - d) EVCP: Extended Validation Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)
 - e) DVCP: Domain Validation Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)
 - f) OVCP: Organizational Validation Certificate Policy
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)
- If any changes are made to a CP as described in clause 4.2.5 which affects the applicability then the policy identifier should be changed.

Documentary Review	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

As stated in CPS section 1.1, the qualified certificates policy is **QCP-n**.

On-Site Inspection	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

Certificates are issued for natural persons and the organization is prepared to issue as well for legal persons.

The corporate OID 47304 is registered² on 01/03/2016 by José Biosca, personnel still present in Ivnosys Soluciones.

² <https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>

5.3 Participants in the PKI

5.3.1 Certification Authority (CA)

ETSI 5.4.1 Certification Authority

The authority trusted by the users of the certification services (i.e. subscribers as well as relying parties) to create and assign certificates is called the CA. The CA has overall responsibility for the provision of the certification services identified in clause 4.4. The CA is identified in the certificate as the issuer and its private key is used to sign certificates.

The CA may make use of other parties to provide parts of the certification service. However, the CA always maintains overall responsibility and ensures that the policy requirements identified in the present document are met.

EXAMPLE: A CA can sub-contract all the component services, including the certificate generation service (sometimes also called CA with the second meaning of CA as per definition above). However, the key used to sign the certificates is identified as belonging to the CA, and the CA maintains overall responsibility for meeting the requirements defined in the present document.

A CA is a type of Trust Service Provider (TSP), as defined in the Regulation (EU) No 910/2014 [i.14], and also a form of certification service provider as defined in the Electronic Signatures Directive 1999/93/EC [i.1], which issues public key certificates.

A TSP may include a hierarchy of CAs. Where a TSP includes a hierarchy of subordinate CAs up to a root CA the TSP is responsible for ensuring the subordinate-CAs comply with the applicable policy requirements. If the TSPs Trust

Anchor is signed by a Root CA outside the scope of the TSP policies then the Root CA requirements apply to the TSP's Trust Anchor.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The hierarchy is published in the web site and in the CPS, section *1.3.1 Autoridades de certificación*.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Checked the hierarchy documented in *3.2.1 Certification Authority (CA)*.

5.3.2 Subscriber and Subject

5.4.2 Subscriber and subject

In the framework of the present policies, the subject can be:

- a) a natural person;
- b) a natural person identified in association with a legal person;
- c) a legal person (that can be an Organization or a unit or a department identified in association with an Organization); or
- d) a device or system operated by or on behalf of a natural or legal person.

When a subscriber is the subject it will be held directly responsible if its obligations are not correctly fulfilled. When the subscriber is acting on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company), responsibilities of the subscriber and of the subject are addressed in clause 6.3.4 item e).

The link between the subscriber and the subject is one of the following:

- a) To request a certificate for natural person the subscriber is:

- i. the natural person itself;
- ii. a natural person mandated to represent the subject; or

NOTE: The local legal dispositions can address the handover of responsibility to a third person.

- iii. any entity with which the natural person is associated (such as the company employing the natural person or a non-profit legal person the natural person is member of).

- b) To request a certificate for legal person the subscriber is:

- i. any entity as allowed under the relevant legal system to represent the legal person; or
- ii. a legal representative of a legal person subscribing for its subsidiaries or units or departments.

- c) To request a certificate for a device or system operated by or on behalf of a natural or legal person the subscriber is:

- i. the natural or legal person operating the device or system;
- ii. any entity as allowed under the relevant legal system to represent the legal person; or
- iii. a legal representative of a legal person subscribing for its subsidiaries or units or departments.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Any legal or natural person is identified properly in the registration process.

Documented in the CPS section 3.2.2 *Autenticación de la Entidad y la vinculación de un individuo y*

3.2.3 *Autenticación de la identidad de un individuo.*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Subscribers can be persons or companies. In this second case, users will be the Company employees.

Interview with Noelia Rodrigo, chief RA operator.

Seen “*Documentación certificados cualificados*”, with the listing of documentation to be asked to subscribers/clients by the RA operator.

The main projects involve physical presence in company to register people.

5.3.3 Others

5.4.3 Others

Other participants, not covered by the present document, may be identified by the TSP.

Documentary Review	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable

On.site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

5.4 Certificate usage

5.5 Certificate usage

The policies NCP, NCP+ and LCP place no constraints on the user community and applicability of the certificate. The applicability of other certificates is as described below.

The specific purpose of EV Certificates is described in EVCG [4], clause 2. The purpose of PTC is described in BRG [5], clause 1.4.1.

Certificates issued under EVCG [4] or BRG [5] are for publicly trusted certificates used to identify web servers accessed via the TLS or SSL protocol as per IETF RFC 5246 [i.11].

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The usage for the different certificates is defined in CPS sections 1.4 y 4.5 *Uso de los certificados*.

On-site Inspection	Correct		NC-M		NC-m		OBS		IO	x
--------------------	---------	--	------	--	------	--	-----	--	----	---

Evidences

Seen permitted uses for the certificate issued as test during the audit. The uses are authentication and mail signing.

IO 01. Since the legal person representative (proxy or Power of Attorney) certificate profile already complies with the specifications issued by the Ministry for Finance and Public Administration Ministry (*General Secretariat of Digital Administration*) Certificate profile 2.0³, it is recommended to mention it the policy.

³ https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

6 Trust Service Providers Practices

6.1 Publication and repository responsibilities

ETSI 6.1 Publication and repository responsibilities

The TSP shall make certificates available to subscribers, subjects and relying parties.

In particular:

Dissemination

- a) Upon generation, the complete and accurate certificate shall be available to the subscriber or subject for whom the certificate is being issued.
- b) Certificates shall be available for retrieval in only those cases for which the subject's consent has been obtained. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subject.
- c) The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).
- d) The applicable terms and conditions shall be readily identifiable for a given certificate.
- e) [CONDITIONAL]:
 - i) [LCP]: the information identified in b) and c) above shall be available as specified in the TSP's CPS.
 - ii) [NCP]: the information identified in b) and c) above shall be available 24 hours per day, 7 days per week.

Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.
- f) [CONDITIONAL] If the TSP is not issuing publicly-trusted certificates, the information identified in c) above should be publicly and internationally available.
- g) [CONDITIONAL] If the TSP is issuing publicly-trusted certificates, the information identified in c) above shall be publicly and internationally available.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

As detailed in CPS sections *4.3.2 Notificación al suscriptor de la emisión del certificado* and *4.4.2 Publicación del certificado por la CA*.

The information is publicly available 24x7 in the web site as explained in CPS section *2.2 Publicación de información de los certificados*.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen mail with PIN for the user. The user can see, download and print the *Terms and Conditions* when the certificate request is validated. It is also published in the web.

All certificates are issued to be managed in two ways:

- Through a centralized platform which guarantees the user sole control of the private key
- Downloadable as a password protected certificate backup file (PKCS#12).

6.2 Identification and Authentication

6.2.1 Naming

6.2.1 Naming

NOTE: Requirements for naming in certificates are as specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412 [2], [9] and [10]. See clause 6.6.1 of the present document.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Certificate profiles comply with RFC 5280 and are issued according to X.509v3, RFC 3739 and ETSI EN 319 412, as stated in CPS section 7.1 *Perfil de Certificado*.

On-site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen 4000A - *Certificado Cualificado Corporativo (P12) [4000]_v1_00_firmado*.

Checked with Lapo.it⁴ tool:

- A corporate test certificate.
- A representative test certificate.

The certificates have the required fields and the OIDs are correct.

⁴ <http://lapo.it/asn1js/>

6.2.2 Initial Identity Validation

6.2.2 Initial identity validation

The TSP shall verify the identity of the subscriber and subject and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

NOTE 1: When registering, a subject is identified as a person with specific attributes. The specific attributes can indicate, for example, an association within an organization and possibly, a role within that organization.

In particular:

Registration

a) The TSP shall 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 (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

- [PTC]: The verification methods shall follow those specified in clause 11 of the EVCG [4] and clause 3.2 of BRG [5].

b) [CONDITIONAL] [NCP]: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

NOTE 2: An example of the required indirect evidence of identity is one or more registration documents electronically signed by a person trusted to have checked the persons' identity in line with the requirements of this clause. Some other examples can be found in annexes B and C of the EVCG [4].

a) The TSP shall 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 (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

- [PTC]: The verification methods shall follow those specified in clause 11 of the EVCG [4] and clause 3.2 of BRG [5].

b) [CONDITIONAL] [NCP]: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person

c) [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), evidence shall be provided of:

1) full name (including surname and given names consistent with the national identification practices); and

2) date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

The place of birth should be given in accordance to national or other applicable conventions for registering births.

d) [CONDITIONAL] [NCP]: If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence of the identity, in particular the ones listed in e), shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person

unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

e) [CONDITIONAL]: If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence shall be provided of:

1) full name (including surname and given names, consistently with the national or other applicable identification practices) of the subject;

- 2) date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which can be used to, as far as possible, distinguish the person from others with the same name;
 - 3) full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber);
 - 4) any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity identified in association with the legal person, consistent with the national or other applicable identification practices;
 - 5) affiliation of the natural person to the legal person consistent with national or other applicable identification practices;
 - 6) [CONDITIONAL]: when applicable, the association between the legal person and any organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices; and
 - 7) approval by the legal person and the natural person that the subject attributes also identify such organization.
- f) [CONDITIONAL] [NCP]: If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, in particular the ones listed in g), shall be checked against a duly mandated subscriber either directly, by physical presence of a person allowed to represent the legal person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.
- g) [CONDITIONAL]: If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided:
- 1) of full name of the organizational entity (private organization, government entity, business entity or noncommercial entity) consistent with the national or other applicable identification practices:
[PTC]: BRG [5], clause 3.2.2, shall apply.
[EVCP]: EVCG [4], clause 11.2, shall apply.
 - 2) [CONDITIONAL]: when applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.
- h) [CONDITIONAL] [NCP]: If the subject is a device or system operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, in particular the ones listed in i), shall be checked against a duly mandated subscriber either directly, by physical presence of a person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.
- i) [CONDITIONAL]: If the subject is a device or system operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person, evidence shall be provided of:
- 1) identifier of the device by which it can be referenced (e.g. Internet domain name);
 - 2) full name of the organizational entity:
[PTC]: clause 3.2.2 of BRG [5] shall apply;
[EVCP]: EVCG [4], clause 11.2.1, shall apply;
 - 3) any relevant existing registration information (e.g. company registration) of the legal person or other organizational entity identified in association with the legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices;
 - 4) a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the organizational entity from others with the same name; and
 - 5) [CONDITIONAL]: when applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the national or other applicable identification practices.
- j) [CONDITIONAL] [NCP]: If the subject is a device or system operated by a natural person, evidence of the identity, in particular the ones listed in k), shall be checked against either directly, by physical presence of the natural person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.
- k) [CONDITIONAL]: If the subject is a device or system operated by a natural person, evidence shall be provided of:

- 1) identifier of the device by which it can be referenced (e.g. Internet domain name);
- 2) a nationally recognized identity number, or other attributes which can be used to, as far as possible, distinguish the natural person from others with the same name;
- 3) [PTC]: clause 3.2.3 of BRG [5] shall apply.
- l) The TSP shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.
- m) [CONDITIONAL] If an entity other than the subject is subscribing to the TSP services (i.e. the subscriber and subject are separate entities - see clause 5.4.2) then evidence shall be provided that the subscriber is authorized to act for the subject as identified (e.g. is authorized for all members of the identified organization), in particular:
 - 1) full name (including surname and given names consistent with the national or other applicable identification practices) of the subscriber;
 - 2) when the subscriber represents a natural person (not associated with a legal person) an agreement to this representation; or
 - 3) when the subscriber represents a legal person (either for requesting a certificate for that legal person or to request a certificate for a natural person identified in association with the legal person), an agreement that the subscriber is allowed to represent the legal person and is entitled to request certificates for that legal person or its members are required. In particular, if the subscriber is not a natural person, it shall be represented by a natural person whose authorization to represent the subscriber shall be proved.
- n) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber shall be contacted.
- o) The TSP shall provide evidence of how they meet applicable data protection legislation within their registration process.
- p) The TSP's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.
- q) To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities. The only exception is the organization running all or part of the RA tasks subscribing a certificate for itself or persons identified

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The authentication method is correct as described in CPS sections 3.2.2 *Autenticación de la Entidad y la vinculación de un individuo* and 3.2.3 *Autenticación de la identidad de un individuo*.

On-Site Inspection

Correct		NC-M		NC-m		OBS	x		
---------	--	------	--	------	--	-----	---	--	--

Evidences

We jointly reproduced the process to obtain a certificate with the Chief RA Operator to identify and register a natural person for issuing a representative (proxy) certificate. It was issued and revoked with the certificate number 1c1598895A812.

The subscriber is directed to a web URL to request the certificate. There is a form to introduce data and receive information about the personal data protection law updated to the new GDPR.

It is required a personal mail, in which the user receives the mail stating that Ivnosys Soluciones has received the form and asking the subscriber to confirm the reception of

the mail. Once confirmed, the terms of use are presented to the subscriber along with the list of documents needed to proceed.

The RA operator will see the pre-request in the IVNOSYS adapted version of AC CAMERFIRMA STATUS platform.

The identification can be done on site or with the remote video on-boarding application (OBA, managed by Deloitte). It is a web interactive application that asks for contact data, then ask to present DNI to the camera to get a photo, shows the data collected after applying OCR to the photo from the DNI and allows the user to correct them. Then the app asks the user to show the face, move it or make any other gesture that it is easy to do spontaneously for a living person reacting to the instructions and show the DNI. If everything is OK all data goes to the app. The 90% of biometric similitude is considered OK for validity, the operator can call the user to the phone number registered in case of doubt. The data in the platform is encrypted, it is downloaded to Ivnosys Soluciones documentation management system and after 7 days, it is encrypted when the backup copy is done. Each RA operator has a file with restricted access.

If everything is OK, the information is validated. Then the video must be validated and the photo is compared with the DNI photo. Only more than 50% biometric similarity can be accepted upon RA operator criteria. There is a log in the platform with all the evidences of the tasks done.

OBS 02. The use of the registration platform requires personal data transfer to Deloitte, but user acceptance of personal data management is not collected at the moment.

In projects that includes physical presence of the natural person, the RA personnel will go to the client Company to perform the identification and collect the documentation needed to issue the certificates. This collection is always in person. The subscriber has to physically present the documents. The documents are scanned and archived.

Evidence: Seen documentation collected for CP Presidencial Buenavista (all documents are electronic).

The information collected about the subscriber is checked by the RA operators and signed by them if it is correct, so the request is validated. A mail is sent to the subscriber with the PIN needed for signing.

Evidence: Seen in the CertManager platform the issued certificate with the data that Noelia has introduced to check the process.

It is planned not to use any paper documents. Only electronic documents will be managed and stored, digitalizing any paper document received.

6.2.3 Identification and authentication for Re-key requests

6.2.3 Identification and authentication for Re-key requests

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes re-key following revocation or prior to expiration, or update due to change to the subject's attributes.

In particular:

Registration

a) i) The TSP shall check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid.

ii) [EVCP]: Clauses 9.4 and 11.3 of EVCG [4] shall apply.

iii) [OVCP] and [DVCP]: Clauses 6.3.2 and 3.3.1 of BRG [5] shall apply.

b) If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with clause 6.3.4, items a), b), c) and d).

c) Requirements of clause 6.2.2 shall apply.

NOTE: Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

No re-key process is available as detailed in CPS section 4.7 *Reemisión de Certificados*.

On-site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

6.2.4 Identification and authentication for revocation requests

6.2.4 Identification and authentication for revocation requests

The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

In particular:

Revocation management

a) The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

i) Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.

ii) How they can be submitted.

iii) Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

EXAMPLE 1: Confirmation can be required from the subscriber if a compromise is reported by a third party.

iv) Whether and for what reasons certificates can be suspended or revoked.

[PTC]: Clause 4.9 of the BRG [5] shall apply.

v) The mechanism used for distributing revocation status information.

vi) The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties. This shall be at most 24 hours.

NOTE: If the revocation or suspension request cannot be confirmed within 24 hours then the status need not be changed.

vii) 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 being made available to relying parties. This shall be at most 60 minutes.

With regard to vii), if the revocation request requires revocation in advance (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time according to the TSP policies.

With regard to vi) and vii), a TSP may give faster process times for certain revocation reasons.

viii) The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

b) Requests for revocation and reports of events relating to revocation shall be processed on receipt.

EXAMPLE 2: Compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations.

c) Requests for revocation and reports of events relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the TSP's practices.

Documentary Review

Correct

x

NC-M

NC-m

OBS

IO

Evidences

The method is documented in CPS sections *3.4 Revocación de la clave* and *4.9 Suspensión y revocación de certificados*

On-site Inspection

Correct

NC-M

NC-m

OBS

x

IO

Evidences

The revocation PIN is sent in the initial mail.

Certificates can be revoked from the STATUS platform, if the PIN is missing, the subscriber or the user can call the Call Center and ask for the initial mail to be sent again to the same mail address. If a company is the subscriber, it will present an authorization

to revoke the certificate.

Revocation can be done electronically only if the certificate data has not changed. The subscriber has the obligation to inform and a new certificate should be issued.

OBS 03. The identification of the person who requests the revocation of a certificate can be improved to avoid impersonation.

6.3 Operational requirements of the certificate lifecycle

6.3.1 Certificate Request

6.3.1 Certificate application

NOTE: See also clause 6.2.2 regarding identity validation.

In particular:

Registration

a) [CONDITIONAL] if the subject's key pair is not generated by the CA, the certificate request process shall check that the subject has possession or control of the private key associated with the public key presented for certification.

b) [EVCP]: For a dual control procedure in the validation process EVCG [4], clause 14.1.3, shall apply.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The rules to apply for a certificate are documented in CPS section *4.1 Solicitud de certificados*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen the STATUS platform, how it works and the activities carried out.

6.3.2 Processing of certificate applications

6.3.2 Certificate application processing

Application for certificates shall be from a trusted registration service.

NOTE: General requirements on the security of the TSP including human resources, operational security, and networks and privacy as specified in clauses 6.4.4, 6.5.6, 6.5.7 and 6.8.4 apply to external registration authorities.

In particular:

a) [CONDITIONAL] when external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The processing is always done with the STATUS platform provided by AC Camerfirma, as described in CPS *section 4 Requerimientos operacionales*.

On-site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen AC Camerfirma contract dated 09/03/2017 for sub-AC creation and maintenance. Seen AC Camerfirma obligations and responsibilities and the responsibility of Ivnosys Soluciones to comply with eIDAS as this subCA is included in its hierarchy. There are provisions for confidentiality, personal data protection and industrial property. Seen SLA in *Annex 2, Eidas certificate and ISO 27001 certificate*.

6.3.3 Certificate Issuance

6.3.3 Certificate issuance

The CA shall issue certificates securely to maintain their authenticity. The requirements for the use of the certificate profiles should be linked to a CP.

In particular:

Certificate generation

a) See clause 6.6.1 for certificate profiles.

b) The CA shall take measures against forgery of certificates, and in cases where the CA generates the subjects' key pair, guarantee confidentiality during the process of generating such data.

c) The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

d) [CONDITIONAL] If the CA generated the subject's key pair:

i) the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA;

ii) [LCP] and [NCP] the private key shall be securely passed to the registered subject; or to the TSP managing the subject's private key; and

iii) [NCP+] the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of the TSP managing the key on behalf of the subject, the TSP shall ensure that the subject has sole control (or if the subject is a legal person "control") over its signing key.

- e) Over the life time of the CA a distinguished name which has been used in a certificate by it shall never be re-assigned to another entity.
- f) [CONDITIONAL] If a certificate is issued to a natural person identified as being as associated with the legal person, then the subject attributes identifying the organization in the certificate should represent the legal person or sub-entity of that legal person and the subject identifier in the certificate shall be the natural person.
- g) Use of the policy identifier:
- [NCP]: The CP identifier shall be:
 - i) as specified in clause 5.3 item a); and/or
 - ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
 - [NCP+] The CP identifier shall be:
 - i) as specified in clause 5.3 item b); and/or
 - ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
 - [LCP] The CP identifier shall be:
 - i) as specified in clause 5.3 item c); and/or
 - ii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
 - [EVCP] The CP identifier shall be:
 - i) as specified in clause 5.3, item d);
 - ii) as specified in EVCG [4], clause 9.3.5; and/or
 - iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
 - [DVCP] The CP identifier shall be:
 - i) as specified in clause 5.3, item e);
 - ii) as specified in BRG [5], clause 7.1.6.1; and/or
 - iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
 - [OVCP] The CP identifier shall be:
 - i) as specified in clause 5.3 item f);
 - ii) as specified in BRG [5], clause 7.1.6.1; and/or
 - iii) an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Certificates are issued adequately as defined in CPS section 4.3 *Emisión de certificados*.
 Appropriate security measures are in place as defined in CPS section 5. *Controles de Seguridad Física, Procedimental y de Personal* and the use of Camerfirma Root AC.

On-site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Procedures as strictly followed by AC Camerfirma as stated.

Seen issuing process and results in the STATUS Platform for certificate serial number **1C15989954AF1C7A82**.

6.3.4 Certificate Acceptance

6.3.4 Certificate acceptance

The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

In particular:

Registration

a) Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 6.9.4.

b) [CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.

c) i) The TSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form.

ii) The terms and conditions may be transmitted electronically.

iii) The terms and conditions may use the model PKI disclosure statement given in annex A.

d) The TSP shall record the signed agreement with the subscriber (see clause 6.4.5 c)).

e) [CONDITIONAL]: Where the subscriber and subject are two separate entities and the subject is a natural person, the signed agreement shall be in 2 parts:

1) The first part shall be signed by the subscriber and shall include:

i) agreement to the subscriber's obligations (see clause 6.9.4) and the general terms and conditions as identified in clause 6.1;

ii) if required by the TSP, agreement by the subscriber to use a secure cryptographic device;

iii) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services;

iv) whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;

v) confirmation that the information held in the certificate is correct;

vi) obligations applicable to subjects (see clause 6.9.4);

vii) [PTC]: clause 9.6.3 of BRG [5] shall apply;

viii) [EVCG]: EVCG [4] clause 11.8 shall apply.

2) The second part shall be signed by the subject and shall include:

i) the agreement by the subject;

ii) obligations applicable to subjects (see clause 6.9.4);

iii) if required by the TSP, agreement by the subject to use a secure cryptographic device;

iv) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services.

f) [CONDITIONAL]: Where the subject and subscriber are the same entity the agreement shall be in one or two parts and shall include the part 1 and part 2 items listed above.

NOTE 1: The subscriber can agree to different aspects of this agreement during different stages of registration. For example, agreement that the information held in the certificate is correct can be carried out subsequent to other aspects of the agreement.

g) This agreement may be in electronic form.

h) The records identified above shall be retained for the period of time as indicated to the subscriber (see item c) above).

NOTE 2: See also clause 6.4.6 regarding retention of information.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Users must accept the terms and conditions as specified in CPS section 4.5.1 *Uso de la clave privada y del certificado por el suscriptor* and 9.16.1 *Marco legal*. Terms are documented in *eula1_IVNOSYS.txt*.

Data related to the certificates are kept for 15 years as stated in CPS section 5.5.2 *Periodo de retención para el archivo*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen contract model with conditions and terms of use, obligations of each part, etc.
No contract has been signed yet.

Seen Terms and Conditions in *eula1_IVNOSYS.txt*.

6.3.5 Key pair and certificate usage

6.3.5 Key pair and certificate usage

The subscriber's obligations (see clause 6.3.4) shall include items a) to j) below.

If the subject and subscriber are separate entities and the subject is a natural person, the subject's obligations shall include at least items b) c) e) f) h) i) and j) (as listed below):

- a) accurate and complete information is submitted to the TSP in accordance with the requirements of this policy, particularly with regards to registration;
- b) the key pair is only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person (see clause 6.9.4);
- c) unauthorized use of the subject's private key is avoided;
- d) [CONDITIONAL] if the subscriber or subject generates the subject's keys:
 - i) subject keys should be generated using an algorithm as specified in ETSI TS 119 312 [i.10] for the uses of the certified key as identified in the CP; and
 - ii) a key length and algorithm should be as specified in ETSI TS 119 312 [i.10] for the uses of the certified key as identified in the CP during the validity time of the certificate.
- NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.
- e) [CONDITIONAL] if the subscriber or subject generates the subject's keys and the private key is for creating digital signatures or seals the subject's private key can be maintained under the subject's sole control;
- f) [NCP+] only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;
- g) [NCP+] [CONDITIONAL] if the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the secure cryptographic device;
- h) notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
 - i) the subject's private key has been lost, stolen, potentially compromised;
 - ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or
 - iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.
- i) following compromise, the use of the subject's private key is immediately and permanently discontinued, except for key decipherment;
- j) in the case of being informed that the subject's certificate has been revoked, or the issuing CA has been compromised, ensure that the private key is not used by the subject.

NOTE 2: In the case of being informed that the subject's certificate has been compromised, the subject certificate is revoked, see clauses 6.2.4 and 6.3.9.

The notice to relying parties (see clause 6.9.4) shall recommend the relying party to:

- k) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 6.9.4);

NOTE 3: See clauses 6.2.4, 6.3.9 and 6.3.10 for requirements on certificate revocation and suspension.

- l) 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 required in clause 6.9.4; and
- m) take any other precautions prescribed in agreements or elsewhere:
 - i) Depending on CA's practices related to the problem reporting and response capability:
 - 1) [EVCP]: refer to clause 11.3 of EVCG [4].
 - 2) [OVCP] and [DVCP]: refer to clause 4.9.3 of BRG [5].

Documentary Review

Correct

x

NC-M

NC-m

OBS

IO

Evidences

Users must accept the terms and conditions as noted above.

Ivnosys Soluciones generates keys as detailed in CPS section 6.1 *Generación e instalación del par de claves*. The length of the CA key is 4.096 bits using sha256 with RSA encryption. Private keys are 2048 bits with RSA encryption.

On-site Inspection	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

Seen the model contract with the different obligations for the subscriber (the client company) and the user (the employee). This contract is reviewed by Camerfirma.

Checked in the certificate issued during the on-site inspection that the private keys are RSA 2048 and the signing algorithm is sha256.

6.3.6 Certificate renewal

6.3.6 Certificate renewal

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized.

EXAMPLE: The subscriber can, if the TSP offers this service, request a certificate renewal where relevant attributes presented in the certificate have not changed or when the certificate lifetime is nearing expiry. In particular:

Registration

- a) i) The TSP shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.
- ii) [EVCP]: Clauses 9.4 and 11.3 of EVCG [4] shall apply.
- iii) [OVCP] and [DVCP]: Clauses 6.3.2 and 3.3.1 of BRG [5] shall apply.
- b) If any of the TSP terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with clause 6.3.4, items a), b), c) and d).
- c) Requirements h) to l) of clause 6.2.2 shall apply.

NOTE 1: Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

Certificate generation

- d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

NOTE 2: See also clause 6.3.8.

Documentary Review	Correct	x	NC-M	NC-m	OBS	IO
--------------------	---------	---	------	------	-----	----

Evidences

It is not available the certificate renewal without a key renewal as stated in CPS section 4.6. *Renovación de certificados.*

On-site Inspection	Correct	NC-M	NC-m	OBS	x	IO
--------------------	---------	------	------	-----	---	----

Evidences

Seen the means provided to renew the certificates.

OBS 04. Include further data verification in the RA operations such as DNI (Citizen ID card) validity or that the mail address provided is a corporate one or one that requires identification before being supplied, and is not used by several persons.

6.3.7 Certificate Re-key

6.3.7 Certificate Re-key
NOTE: See clause 6.2.3.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

No re-key process is available as detailed in CPS section 4.7 *Reemisión de certificados*.

On-Site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

6.3.8 Certificate modification

6.3.8 Certificate modification

Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes certificate update due to change to the subject's attributes.

EXAMPLE: The subscriber can, if the TSP offers this service, request a certificate re-key where relevant attributes presented in the certificate have changed.

In particular:

Registration

a) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be verified, recorded, agreed to by the subscriber in accordance with clause 6.2.2.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

It is not possible to modify a certificate; a new request must be issued as detailed in CPS section 4.8 *Modificación de certificados*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

It is not possible to modify certificates. It has to be revoked and issued again.

6.3.9 Certificate revocation and suspension

6.3.9 Certificate revocation and suspension

The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

In particular:

a) The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of the certificate.

b) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

c) [CONDITIONAL]: Where Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours; and:

i) every CRL shall state a time for next scheduled CRL issue;

ii) a new CRL may be published before the stated time of the next CRL issue;

iii) the CRL shall be signed by the CA or an entity designated by the TSP.

NOTE: See clause 6.6.2 regarding CRL profile requirements.

d) [OVCP] and [DVCP]: The TSP shall operate and maintain its certificate status information. Clause 4.10.2 of BRG [5] shall apply.

e) [EVCP]: TSP shall comply with EVCG [4], clause 13.

f) [CONDITIONAL]: Where CARL is used a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date. In any case, a new CARL shall be generated once a CA certificate has been revoked.

g) In the case of any cross-certificates issued by the CA, the CARL should be issued at least every 31 days.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Certificate revocation follows the process define in CPS section 4.9. *Suspensión y revocación de certificados.*

The CRL is published at least every day, as detailed in CPS section 4.9.7 *Frecuencia de emisión de CRLs.*

On-site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen certificate serial number **1C15989954AF1C7A82** revoked in the RA platform.

The CRL address in in the certificate and published in **policy.ivsign.net**. Checked the date of the CRL (date 6/3/18 time 8:41). The CRL is automatically updated, at most 24 hrs. and latency is 48 hrs.

6.3.10 Certificate status services

6.3.10 Certificate status services

The TSP shall provide services for checking the status of the certificates.

In particular:

Revocation status

a) Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best endeavors to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

b) The integrity and authenticity of the status information shall be protected.

c) Revocation status information shall include information on the status of certificates at least until the certificate expires.

d) OCSP shall be supported.

NOTE 1: See clause 6.6.3 for profile requirements of OCSP.

e) CRL should be supported.

NOTE 2: See clause 6.6.2 for profile requirements of CRL.

f) [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, any updates to revocation status shall be available for all methods, and the information provided by all services shall be consistent over time taking into account different delays in updating the status information for all the methods.

g) The revocation status information shall be publicly and internationally available.

Documentary Review

Correct

x

NC-M

NC-m

OBS

IO

Evidences

The revocation status information is available 24x7 through the AC Camerfirma CA and their own OCSP, and measures are in place to avoid that it is unavailable for more than 24 hours. Described in CPS section 4.9.9 *Disponibilidad de comprobación on-line de la revocación*

On-Site Inspection

Correct

x

NC-M

NC-m

OBS

IO

Evidences

Seen the CRL signed for integrity.

The OCSP is available on the date of the audit, and it has been checked with a set of test certificates that it is working properly. TEST_REVOKED_4000 and TEST_VALID_4000

6.3.11 End of subscription

6.3.11 End of subscription

No policy requirement.

Documentary Review

Correct

x

NC-M

NC-m

OBS

IO

Evidences

The end of the subscription occurs when the certificate expires or the subscriber requests it as stated in CPS section 9.10 *Duración y resolución*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

It is included in the contracts with clients.

6.3.12 Key escrow and recovery

6.3.12 Key escrow and recovery

- The security of any duplicated subject's private keys shall be at the same level as for the original subject's private keys.
- The number of any duplicated subject's private keys shall not exceed the minimum needed to ensure continuity of the service.
- [CONDITIONAL]: If the subject's private key is to be used for digital signatures, then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow), and results in its use not being under the sole control of the signer or owner.
NOTE: This does not preclude the TSP generating and managing the key on behalf of the user provided that the key is kept under the sole control of the user.
- [CONDITIONAL]: If the subject's private key is to be used for authentication, then the CA should not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow), and results in its use not being under the sole control of the signer or owner.
- [CONDITIONAL]: If the subject's private key is to be used for decryption, then the CA may back it up.
- [CONDITIONAL]: If the CA requires a subject private key used for decryption to be escrowed by the CA or a designated entity, then this private key shall not have other key usages.
- [CONDITIONAL]: If a copy of the subject's key is kept by the CA for escrow then the CA shall keep secret the private key and only make it available to appropriately authorized persons.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

There is no provision to escrow keys.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The CPS section 4.12 states that they don't keep any key and rely in AC Camerfirma for the necessary backups.

6.4 Facilities, management and operational controls

6.4.1 General

6.4.1 General

The requirements identified in ETSI EN 319 401 [8], clauses 5, 6.3 and 7.3, shall apply.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

As part of the ISMS, there is a risk analysis, a security policy and the assets are documented in an inventory, as detailed in CPS section 6.5 *Controles de seguridad informática*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen *SGSI Identificación de Activos y Valoración de Riesgos_ALI_v2.xls*. with assets belonging to Servicio IvSign CA. Only *Information Destruction* for this service has a risk above 3 which has been defined as acceptable level. The actions defined are to review the documental procedure to clarify it and training.

They plan to install Jira (a bug-tracking, issue-tracking and project-management software application) for daily operations management, so the incidents are expected to be reduced.

Seen *MA01 Manual de Calidad y Seguridad de la Información v2* del 16/01/17.

Seen *Política de uso aceptable de los activos v1* del 10/03/16.

Seen *Política de Calidad y Seguridad de Ivnosys, v1* del 15/12/15.

6.4.2 Physical security controls

6.4.2 Physical security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.6, shall apply. In addition the following particular requirements apply:

Certificate generation and revocation management

a) The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

b) Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.

c) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.

d) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

e) Controls shall be implemented to protect against equipment, information, media and software relating to the TSP services being taken off-site without authorization.

f) Other functions relating to TSP operations may be supported within the same secured area provided that the access is limited to authorized personnel.

g) Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

As part of the ISMS, there is sufficient and efficient physical security controls, as recorded in CPS sections 5 and 6.

On-Site Inspection

Correct		NC-M		NC-m		OBS	x	IO	
---------	--	------	--	------	--	-----	---	----	--

Evidences

Seen MA01 Manual de Calidad y Seguridad de la Información v2 del 16/01/17.

Seen PS04 Seguridad física y del ambiente v1 del 12/12/16.

In the office premises there is only a storage server for backup copies and internal operations such as the documentation management system. In the visual inspection, this internal CPD is correct.

The main CPD is hosted by Nixval contractor.

OBS 05. The security measures in Nixval to restrict access to equipment areas are correct but could be improved or have compensatory measures.

6.4.3 Procedural controls

6.4.3 Procedural controls

The requirements identified in ETSI EN 319 401 [8], clause 7.4, items b), c), d) and e) shall apply.

In addition the following particular requirements apply:

NOTE: With regards general to requirement "Sensitive data shall be protected" [8], Sensitive data includes registration information.

Certificate generation

a) Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

- [PTC]: BRG [5], clause 4.3 shall apply.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Access to the CA systems is controlled and secured, as defined in CPS section 6
Controles de seguridad técnica.

Critical activities that require dual control have been documented such as the certificate issuance by the subCA or the installation of new equipment. IVSIGN HSM DUAL CONTROL IVS-PR-241-2O dated 29/06/2018.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Ticket OTRS ID 180625034 dated 25/06/18 to prepare the HSM in Fips mode.

Tasks carried out to install new HSM, Alta HSMIVS3 with video evidences:

- "video_inicialización_02.mp4" containing the firmware loading for FIPS mode with the manufacturer tool (CAT). Default passwords were changed for the root and the clsagent.
- "video_inicialización_03.mp4" Creation of 4 new users, using their own USBs to introduce their keys created in the HSM. Deletion of the admin user.
- "video_inicialización_04.mp4". Master key generation for backup.
- "video_inicialización_05.mp4", to end the HSM configuration, the cryptographic user and operator are created.

6.4.4 Personnel controls

6.4.4 Personnel controls

The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply:

- a) In addition to the trusted roles identified in ETSI EN 319 401 [8], 7.2 item i), the trusted roles, of the registration and revocation officers responsibilities as defined in CEN TS 419 261 [i.9] shall be supported.
- b) [PTC]: the role of validation specialist shall be included as specified in BRG [5] and EVCG [4].

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The critical roles are defined as well as their responsibilities, as defined in CPS section 5.2. *Controles de procedimiento* y 5.3 *Controles de seguridad de personal*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen “*Requisitos del puesto Administrador de Sistemas*”. Seen *Ficha de Personal de Rubén Curiel* that comply with requirements.

Checked “*Ficha de alta del personal interno autorizado para desarrollar las labores de operador de RA*”, signed by Jaime Castelló, dated 22/02/18, to authorise a person identified with initials ECA to carry out the training for RA operators. The course was finished by ECA on 02/03/18 and has passed the test. There is as well a test on Security and IT.

The “*Declaración Responsable del Operador de RA*” is not yet signed, it is pending AC Camerfirma validation of the training process.

Seen contract for RA dependent on the RA Ivnosys Soluciones.

6.4.5 Audit logging procedures

6.4.5 Audit logging procedures

The requirements identified in ETSI EN 319 401 [8], clause 7.10, shall apply. In addition the following particular requirements apply:

NOTE: ETSI TS 101 533-1 [i.13] suggests provisions on how to preserve digital data objects.

a) All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

Registration

b) All events related to registration including requests for certificate re-key or renewal shall be logged.

c) All registration information including the following shall be recorded:

i) type of document(s) presented by the applicant to support registration;

ii) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;

iii) storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 6.3.4, item d));

iv) any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 6.3.4, item d);

v) identity of entity accepting the application;

vi) method used to validate identification documents, if any; and

vii) name of receiving TSP and/or submitting Registration Authority, if applicable.

d) The TSP shall maintain the privacy of subject information.

Certificate generation

e) The TSP shall log all events relating to the life-cycle of CA keys.

f) The TSP shall log all events relating to the life-cycle of certificates.

g) The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

Revocation management

h) The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Logs are registered and stored as defined in CPS sections 5.5.6 *Sistema de recogida de información de auditoría*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen internal systems access logs.

Seen user logs.

Logs managed by STATUS (registration management) platform provided by AC Camerfirma are not directly accessed by the provider. AC Camerfirma sends logs files daily according to a procedure. Seen logs dated 04/07/18 for the test certificates,

6.4.6 Records archival

6.4.6 Records archival

The following particular requirements apply:

NOTE: [i.13] suggests provisions on how to preserve digital data objects.

a) The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

i) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA (see clause 6.4.5, item g));

ii) documentation as identified in clause 6.3.4.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Records are appropriately archived and protected as described in CPS section 5.5
Archivo de registros

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Information stored in the AC Camerfirma platforms are subject to their backup policies.

IT systems have an architecture that provides high availability. Backup copies are done daily, and two sets are stored, one in Nixval hosted Data Center and another in the offices. Complete weekly copies are done in two hard disks stores off premises.

6.4.7 Key changeover

6.4.7 Key changeover

No policy requirement.

Documentary Review

Correct		NC-M		NC-m		OBS		IO	
---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable

On-Site Inspection

Correct		NC-M		NC-m		OBS		IO	
---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable

6.4.8 Compromise and disaster recovery

6.4.8 Compromise and disaster recovery

The requirements identified in ETSI EN 319 401 [8], clauses 7.9 and 7.11, shall apply. In addition the following particular requirements apply:

TSP systems data backup and recovery

- a) TSP systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.
- b) In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly. Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.
- c) Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.
- d) [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

CA key compromise

- e) The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster and the planned processes shall be in place. NOTE: It is suggested that the plan include a requirement that all subject keys are revoked.
- f) Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.
- g) In the case of compromise the TSP shall as a minimum:
 - i) inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs. In addition, this information shall be made available to other relying parties;
 - ii) indicate that certificates and revocation status information issued using this CA key may no longer be valid; and
 - iii) revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.

Algorithm compromise

- h) Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall:
 - i) inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, this information shall be made available to other relying parties; and
 - ii) schedule a revocation of any affected certificate.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Ivnosys Soluciones is ready to act upon disasters to maintain continuity as described in CPS section 5.7 *Recuperación ante desastres*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The Recovery Plan depends on AC Camerfirma and relies on their continuity plans. There is a continuity strategy "*PS09 Continuidad.*"

Seen "*Procedimiento restauración*" with actions in case of disaster, AC key compromise and IvSign key compromise.

Critical systems recovery tests have been carried out and non-critical systems recovery tests are scheduled to be completed before September.

6.4.9 Certification Authority or Registration Authority termination

6.4.9 Certification Authority or Registration Authority termination

The requirements identified in ETSI EN 319 401 [8], clause 7.12, shall apply. In addition the following particular requirements apply:

- a) Regarding the requirement of bullet b) iii) of clause 7.12 of ETSI EN 319 401 [8], this shall apply to registration information (see clauses 6.2.2, 6.3.1 and 6.3.4), revocation status information (see clause 6.3.10) and event log archives (see clauses 6.4.5 and 6.4.6) for their respective period of time as indicated to the subscriber and relying party (see clause 6.8.10).
- b) Regarding the requirement d) of clause 7.12 of ETSI EN 319 401 [8], this shall also include the handling of the revocation status for unexpired certificates that have been issued.
- c) When another cross certified TSP stops all operations, including handling revocation (see clause 6.4.9 b), all cross certificates to that TSP shall be revoked.

NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [8], clause 7.12 d) i), include cross certified TSP.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Ivnosys Soluciones is ready to act upon termination as described in CPS section 5.7.3 *Procedimientos ante el compromiso de una clave privada de entidad* and 5.8 *Cese de CA*, and document *PS.CA09 Plan de cese de la autoridad de certificación IVSIGN CA* dated 03/01/2018.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Seen *PS.CA09 Plan de cese de la autoridad de certificación IVSIGN CA* and *contract with AC Camerfirma*, stating termination provisions for service continuity.

Seen *RA standard contract*, with termination provisions, not in use for now as they have not started to provide the service.

6.5 Technical safety controls

6.5.1 Key pair generation and installation

6.5.1 Key pair generation and installation

The requirements identified in ETSI EN 319 401 [8], clause 7.5, shall apply.

In addition the following particular requirements apply:

Certificate generation

The CA shall generate keys securely and the private key shall be secret.

a) CA key pair generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

b) CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

NOTE 1: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

c) The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

NOTE 2: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

d) Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate for signing subject key pairs and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate. The new CA certificate shall also be generated and distributed in accordance with this policy.

e) These operations should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.

f) The TSP shall have a documented procedure for conducting CA key pair generation for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users. This procedure shall indicate, at least, the following:

i) roles participating in the ceremony (internal and external from the organization);

ii) functions to be performed by every role and in which phases;

iii) responsibilities during and after the ceremony; and

iv) requirements of evidence to be collected of the ceremony.

g) The TSP shall produce a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. This report shall be signed:

i) For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

ii) For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

iii) [PTC]: clause 6.1.1.1 of the BRG [5] shall apply.

Certificate generation and dissemination

h) CA signature verification (public) keys shall be available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

NOTE 3: For example, CA public keys can be distributed in self-signed certificates, along with a declaration that the key authenticates the CA, or issued by another CA. By itself a self-signed certificate cannot be known to come from the CA. Additional measures, such as checking the fingerprint of the

certificate against information provided by a trusted source, is needed to give assurance of the correctness of this certificate.

Certificate generation / subject device provision

[CONDITIONAL] If the CA generates the subject's keys:

- i) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the uses identified in the CP during the validity time of the certificate.
- j) CA-generated subject keys should be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [i.10] for the purposes stated in the CP during the validity time of the certificate.

NOTE 4: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.10] can be superseded by national recommendations.

- k) CA-generated subject keys shall be generated and stored securely whilst held by the TSP.

Subject device provision

- l) The subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised. If the TSP or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key.
- m) The CA shall delete all copies of a subject private key after delivery of the private key to the subject, except for conditions as described in clause 6.3.12.
- n) [NCP+]: The TSP shall secure the issuance of a secure cryptographic device to the subject. In particular:
 - i) Secure cryptographic device preparation shall be done securely.
 - ii) Secure cryptographic device shall be securely stored and distributed.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The key pair generation is done is a HSM which is certified according to FIPS 140- 2 level 3, as describe in CPS section 6.1. *Generación e instalación del par de claves.*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Certificates are issued through Registration "STATUS" Platform hosted by AC Camerfirma and the AC Camerfirma HSM. Ivnosys Soluciones subCA is hosted in AC Camerfirma.

6.5.2 Private key protection and cryptographic module controls

6.5.2 Private key protection and cryptographic module engineering controls

Certificate generation

In addition to requirements in clause 6.5.1 the following particular requirements apply:

- a) CA key pair generation shall be carried out within a secure cryptographic device which:
 - i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or
NOTE 1: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 [1], are currently under development within CEN as CEN TS 419 221-2 [i.16], CEN TS 419 221-3 [i.17], CEN TS 419 221-4 [i.18], or CEN EN 419 221-5 [i.19].
 - ii) meets the requirements identified in ISO/IEC 19790 [3] or FIPS PUB 140-2 [12] level 3.

The secure cryptographic device should be as per i).

NOTE 2: With the general availability of devices which meet ISO/IEC 15408 [1], it is expected that ISO/IEC 19790 [3] or FIPS 140-2 [12] level 3 will no longer be acceptable.

NOTE 3: This applies also to key generation even if carried out in a separate system.

- b) The CA private signing key shall be held and used within a secure cryptographic device as indicated in a) above.

- c) [CONDITIONAL]: When outside the secure cryptographic device (see item b) above) the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

- d) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

- e) Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

- f) [CONDITIONAL]: Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

- g) The secure cryptographic device shall not be tampered with during shipment.

- h) The secure cryptographic device shall not be tampered with while stored.

- i) The secure cryptographic device shall be functioning correctly.

- j) The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

NOTE 4: This destruction does not necessarily affect all copies of the private key. Only the physical instance of the key stored in the secure cryptographic device under consideration will be destroyed.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The HSM is FIPS certified according to FIPS 140- 2 level 3, as described in CPS section 6.1. *Generación e instalación del par de claves.*

Key protection is described in CPS section 6.2. *Protección de la clave privada.*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The private key for the sub-Ca is hosted by AC Camerfirma. Seen the “Acta de Generación de certificado de Ivsign CA y su OCSP Responder” cod **INTJAM2017020 v1** dated 05/10/2017.

6.5.3 Other aspects of key pair management

6.5.3 Other aspects of key pair management

The TSP shall use appropriately the CA private signing keys and shall not use them beyond the end of their life cycle.

In particular:

Certificate generation

- CA signing key(s) used for generating certificates as defined in clause 6.3.3, and/or issuing revocation status information, shall not be used for any other purpose.
- The certificate signing keys shall only be used within physically secure premises.
- The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in clause 6.5.1, item c).
- All copies of the CA private signing keys shall be destroyed at the end of their life cycle.
- [CONDITIONAL]: If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [6] and aligned with point c).

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Key management is correct as defined in CPS section 6.1 *Generación e instalación del par de claves*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Key management depends heavily on AC Camerfirma procedures. Seen Minutes for CA key generation ceremony "Acta de Generación de certificado de Ivsign CA y su OCSP Responder" cod INTJAM2017020 v1 dated 05/10/2017 and its audit report. It is considered correct.

6.5.4 Activation Data

6.5.4 Activation data

The following particular requirements apply:

Certificate generation

a) The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.

Subject device provision

[CONDITIONAL]: In particular, if the TSP issues a secure cryptographic device:

b) Secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

c) Where the secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.

NOTE: Separation can be achieved by ensuring distribution of activation data and delivery of secure user device at different times, or via a different channel.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

There is dual control for installation for certificates PKCS#12, as described in CPS section 6.1.1 *Generación del par de claves*, since it is done following AC Camerfirma CA procedures.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The private key for the subCa is hosted by AC Camerfirma. Seen the "*Acta de Generación de certificado de Ivsign CA y su OCSP Responder*" cod INTJAM2017020 v1 dated 05/10/2017.

6.5.5 Computer security controls

6.5.5 Computer security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.4, items a) and f), shall apply.

NOTE: Requirements for the trustworthy systems can be ensured using, for example, systems conforming to CEN TS 419 261 [i.9] or to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [1].

In addition the following particular requirements apply:

Certificate generation

a) Local network components (e.g. routers) shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified by the TSP.

b) The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

Dissemination

c) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

Certificate Revocation status

d) Revocation status application shall enforce access control on attempts to modify revocation status information.

Certificate generation and revocation management

e) Continuous monitoring and alarm facilities shall be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

EXAMPLE: This can use an intrusion detection system, access control monitoring and alarm facilities.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

IT systems are protected as defined in CPS section 6.5. *Controles de seguridad informática and 6.7 Controles de seguridad de red*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

AC Camerfirma is EIDAS certified, so the Root-CA certificate is available through MINECO (Secretary of State for the Digital Progress) managed TSL and by other means. Ivsign Sub-CA certificate is available in **policy.ivsign.net**.

6.5.6 Life cycle security controls

6.5.6 Life cycle security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.7 shall apply for all service components. In addition the following particular requirements apply:

System planning

a) [NCP]: capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.

b) [PTC]: clause 5 of the BRG [5] shall apply.

Certificate generation and revocation management

c) See clause 6.5.5, item e).

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

IT systems are protected as defined in CPS section 6.5. *Controles de seguridad informática and 6.7 Controles de seguridad de red.*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The IT systems architecture provides high availability and is monitored for capacity and incidents.

Systems are maintained, and changes are controlled.

6.5.7 Network security controls

6.5.7 Network security controls

The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.

In addition the following particular requirements apply:

a) The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

b) The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

c) The TSP shall grant access to secure zones and high security zones to only trusted roles.

d) The Root CA system shall be in a high security zone.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

AC Camerfirma and Ivnosys Soluciones have security programs and certifications, both parties are certified according to ISO 27001 and the cryptographic modules are within secured areas.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen AC Camerfirma certificates at

<http://www.camerfirma.com/camerfirma/acreditaciones/>

Checked certification scope to ensure it is included. Seen access control procedures

communicated to Ivnosys Soluciones. As it specifically included in their ISO 27001 annual audit, it is considered correct.

6.5.8 Timestamping

6.5.8 Timestamping

NOTE: Not in the scope of the present document. See ETSI EN 319 421 [i.15] for policy requirements for TSPs issuing time-stamps.

Timestamping	Correct		NC-M		NC-m		OBS		IO	
--------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable

On-Site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

6.6 Certificate Profiles, CRL and OCSP

6.6.1 Certificate Profile

6.6.1 Certificate profile

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

The certificate shall be issued according to the relevant certificate profile as identified below:

- i) [LCP, NCP and NCP+] for issuance of certificates to natural persons (excluding for web site certificates): ETSI EN 319 412-2 [9].
- ii) [LCP, NCP and NCP+] for issuance of certificates to legal persons (excluding for web site certificates): ETSI EN 319 412-3 [10].
- iii) [PTC] for issuance of certificates for web sites or devices: ETSI EN 319 412-4 [2].

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

The certificates meet the applicable standards (X.509 version 3, RFC 5280, EN 319 412 and EN 319 411) as detailed in CPS section 7.1 *Perfiles de Certificado*

They also meet country specific profile definitions according MPTFP requirements⁵.

NOTE Sub-CA certificate does not include SERIAL NUMBER field in the SUBJECT section.

According RFC 3739:

The serialNumber attribute type SHALL, **when present**, be used to differentiate between names where the subject field would otherwise be identical. This attribute has no defined semantics beyond ensuring uniqueness of subject names. It MAY contain a number or code assigned by the CA or an identifier assigned by a government or civil authority. It is the CA's responsibility to ensure that the serialNumber is sufficient to resolve any subject name collisions.

NOTE: Sub-CA certificate states a policy of Extended Validation in Certificate Policies field with OID 2.23.140.1.2.2 which implies this meaning: CA-Browser Forum, Certificate Policy, Extended Validation Baseline Requirements, Organization Validated. For the kind of validation provided by Ivnosys Soluciones there is also the option to adopt OID 2.23.140.1.2.3 (CA-Browser Forum, Certificate Policy, Extended Validation Baseline Requirements, Individual Validated) or 2.5.29.32.0 {joint-iso-itu-t(2) ds(5) certificateExtension(29) certificatePolicies(32) anyPolicy(0)}

⁵ https://administracionelectronica.gob.es/pae_Home/dam/jcr:474ae40a-fe06-45fa-aa8f-113049e9c889/2016_Perfiles_de_certificados_1-ed.pdf

On-Site Inspection	Correct		NC-M		NC-m		OBS	x		IO	
--------------------	---------	--	------	--	------	--	-----	---	--	----	--

Evidences

Seen 4000A - *Certificado Cualificado Corporativo (P12) [4000]_v1_00_firmado*.

Checked with Lapo.it⁶ tool:

- A corporate (natural person belonging to a corporation or civil service body) test certificate.
- A representative (proxy, Power of Attorney) test certificate.

The certificates have the required fields and the OIDs are correct.

OBS 06. The complete internal OID structure is documented but not formalized. It is within an internal wiki instead of the documented management system.

6.6.2 CRL Profile

6.6.2 CRL profile

The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

Documentary Review	Correct	x	NC-M		NC-m		OBS			IO	
--------------------	---------	---	------	--	------	--	-----	--	--	----	--

Evidences

This profile is according to the Certification Policies, as detailed in CPS section 7.2 *Perfil de CRL*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS			IO	
--------------------	---------	---	------	--	------	--	-----	--	--	----	--

Evidences

Checked profile with MS parser (tool installed in Windows OS), it contains the fields and data required.

⁶ <http://lapo.it/asn1js/>

6.6.3 OCSF Profile

6.6.3 OCSF profile

The OCSF shall be as defined in IETF RFC 6960 [11].

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

The OCSF complies with RFC 6960, as documented in CPS section 7.3 *Perfil OCSF*

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Checked OCSF certificate.

The OCSF is available and free of charge on the date of the audit, and it has been checked with a set of test certificates that it is working properly.

TEST_REVOKED_4000 and TEST_VALID_4000.

6.7 Compliance audit and other assessment

6.7 Compliance audit and other assessment

NOTE: See ETSI EN 319 403 [i.2].

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Ivnosys Soluciones is subject to various audits annually.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Seen certificates for ISO 9001 (issued by **Cámara Certifica**), ISO 27001 (issued by **Aenor**) and the report for the penetration test. It is planned to start implementation for ISO 14001, ISO 20000-1 and ENS.

The ISO 27001 certificate seen during the on-site audit is not updated to the actual scope. Seen updated scope and the certification granted status in AENOR website (Certificate No SI-0010/2016).

The eIDAS assessment is taking place as TCAB-002CA01-CAR-2018-E report reflects.

6.8 Other aspects and legal issues

6.8.1 Fees

6.8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP services.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Fees are detailed in 9.1 *Tarifas*.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

The company plans to issue certificates in project-oriented actions. So, in every every project will have a bid or offer, detailing prices. Ivnosys Soluciones is working on a standard list of prices.

6.8.2 Financial responsibility

6.8.2 Financial responsibility

The requirements identified in ETSI EN 319 401 [8], clause 7.1.1, item c) shall apply.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Ivnosys Soluciones holds an insurance policy as detailed in CPS section 9.2
Responsabilidad financiera.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen insurance policy provided by insurance company **Liberty Mutual Insurance Europe Ltd.** with a limit of 3.500.000€. Seen **Conditions Particulares** signed with Insurance Broker **Aon** on 02/03/2018.

6.8.3 Confidentiality

6.8.3 Confidentiality of business information

No policy requirement.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The rules for preserving confidentiality are documented in CPS section 9.3
Confidencialidad.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The information for the creation of certificates are stored in AC Camerfirma premises.
All information is considered confidential unless it's public. Access is restricted according to the roles of each employee.

6.8.4 Privacy of personal information

6.8.4 Privacy of personal information

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item c) shall apply. In addition the following particular requirements apply:

- a) The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP system components.
- b) Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

NOTE: Data protection issues specific to these policy requirements are addressed in:

- i) registration (see clause 6.2.2);
- ii) confidentiality of records (clauses 6.3.2, item a) and 6.4.5, item d));
- iii) protecting access to personal information;
- iv) user consent (see clause 6.3.4, item d)).

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

All personal data is protected according to the law, as documented in CPS 9.4 *Política de privacidad*.

Documents related to personal data has been updated to RGPD.

Contracts have been signed with critical suppliers as AC Camerfirma, Deloitte and Nixval.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen contracts signed with:

Nixval. dated 16/07/18 code 20180713125406_edt with provisions for security, confidentiality and personal data protection.

Deloitte, Registration Support Application (Video onboarding) signed 16/07/18.

6.8.5 Intellectual property rights

6.8.5 Intellectual property rights

No policy requirement.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

This aspect is documented in CPS section 9.5 *Propiedad Intelectual*

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen provisions for intellectual property in the contract with AC Camerfirma.

6.8.6 Representations and warranties

6.8.6 Representations and warranties

The requirements identified in ETSI EN 319 401 [8] clause 6.3, item b and clause 6.4 of the present document shall apply. TSP has the responsibility for conformance with the procedures prescribed in this policy, even when the TSP functionality is undertaken by outsourcers.

In addition the following particular requirements apply:

- a) The TSP shall provide all its certification services consistent with its CPS.
- b) [PTC]: the TSP shall comply with BRG [5], clause 9.6.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Ivnosys Soluciones has detailed this aspect in CPS section 9.6 *Representación y garantías*.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Procedures are correctly followed.

6.8.7 Disclaimers of warranties

6.8.7 Disclaimers of warranties

See clause 6.8.6.

NOTE: See also clause A.2 for additional information.

Documentary Review	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

On-Site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

6.8.8 Limitations of liability

6.8.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

NOTE: For TSP operating in EU, see article 13 of the Regulation (EU) No 910/2014 [i.14] and ETSI EN 319 401 [8], clause 7.12, item d).

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

This aspect is documented in CPS section 9.8 *Limitaciones de responsabilidad*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen **Terms and Conditions EULA_IvSignCA-v2** with the different responsibilities.

6.8.9 Indemnities

6.8.9 Indemnities

No policy requirement.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

This aspect is documented in CPS section 9.9 *Indemnizaciones*

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

There has been no claims or controversies up to now.

6.8.10 Term and termination

6.8.10 Term and termination
No policy requirement.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.10 *Duración y resolución*

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

No evidence is available since services are not yet in production.

6.8.11 Individual notices and communications with participants

6.8.11 Individual notices and communications with participants
No policy requirement.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.11 *Notificaciones y comunicaciones en tre los participantes* and SG - Plan de comunicación Rev. 1

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Seen document “*Plan de notificación de incidentes de acuerdo con el artículo 19 del Reglamento eIDAS*”.

6.8.12 Amendments

6.8.12 Amendments
No policy requirement.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.12 *Modificaciones*.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Services and documentation are subject to annual reviews or when changes occur.

6.8.13 Dispute resolution procedures

6.8.13 Dispute resolution procedures

The requirements identified in ETSI EN 319 401 [8], clauses 6.2, item i) and 7.1.1, item e) shall apply.

NOTE: See clause A.2 for additional information.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.13 *Procedimiento de resolución de disputas* and procedure P.Disputas v7 04/07/18.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This is included in contracts, conflicts will be treated by arbitration.

No disputes have arisen yet.

6.8.14 Applicable Laws

6.8.14 Governing law

Not in the scope of the present document.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.16.1 *Marco legal*

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

The current legal framework in Spain and the European Union is included in contracts.

6.8.15 Compliance with applicable law

6.8.15 Compliance with applicable law

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item a) shall apply.

Documentary Review	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

This aspect is documented in CPS section 9.16.1 *Marco legal*.

On-Site Inspection	Correct	<input checked="" type="checkbox"/>	NC-M	<input type="checkbox"/>	NC-m	<input type="checkbox"/>	OBS	<input type="checkbox"/>	IO	<input type="checkbox"/>
--------------------	---------	-------------------------------------	------	--------------------------	------	--------------------------	-----	--------------------------	----	--------------------------

Evidences

Seen "*Documento de Seguridad*", the current eIDAS audit and the information made public in the web site.

6.8.16 Miscellaneous provisions

6.8.16 Miscellaneous provisions
No policy requirement.

Documentary Review	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

On-Site Inspection	Correct		NC-M		NC-m		OBS		IO	
--------------------	---------	--	------	--	------	--	-----	--	----	--

Evidences

Not applicable.

6.9 Other provisions

6.9.1 Corporate

6.9.1 Organizational

The requirements identified in ETSI EN 319 401 [8], clause 7.1 shall apply. In addition the following particular requirements apply:

Certificate generation and revocation management

a) The parts of the TSP concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

NOTE: The TSP may need to take into account privacy requirements.

b) The parts of the TSP concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

The critical roles, persons required per task and roles requiring independence are defined in CPS section 5.2 *Controles de procedimiento*. To avoid conflicts of interest the recruitment has several requirements defined in CPS section 5.3.1 *Requerimientos de antecedentes, calificación, experiencia, y acreditación*.

On-Site Inspection	Correct		NC-M		NC-m		OBS	x	IO	
--------------------	---------	--	------	--	------	--	-----	---	----	--

Evidences

OBS 07. It is not documented the non-discriminatory policy.

OBS 08. It is recommended to add organizational measures to avoid fraud when technical measures are not feasible in cases when an operation needs further independence. For example, revocation, that can be performed by the same RA operator that issued the certificate.

6.9.2 Additional testing

6.9.2 Additional testing

a) The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

EXAMPLE: Publishing PKCS#12 certificates in its web site.

b) Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

c) [PTC]: BRG [5], clause 2.2 shall apply.

d) For cross certificates, clause 3.2.6 of BRG [5] shall apply.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

There are provisions to issue test certificate.

On-Site Inspection

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

Test certificates are available upon demand. We have used two test certificates for validating requirements in this audit.

6.9.3 Disabilities

6.9.3 Disabilities

The requirements identified in ETSI EN 319 401 [8], clause 7.13, item b) shall apply.

Documentary Review

Correct	x	NC-M		NC-m		OBS		IO	
---------	---	------	--	------	--	-----	--	----	--

Evidences

There is no specific provision focused on accessibility but a clause on the website with contact information for people with disabilities in order to facilitate their access to the services.

On-Site Inspection

Correct		NC-M		NC-m		OBS	x	IO	
---------	--	------	--	------	--	-----	---	----	--

Evidences

There are procedures in place for people with disabilities to access the services, but this procedures are not formally documented.

OBS 09 The web is not complying with total accessibility recommendations, and the planned provisions are not documented.

6.9.4 Terms and conditions

6.9.4 Terms and conditions

The requirements identified in ETSI EN 319 401 [8], clause 6.2 shall apply.

In addition the following particular requirements apply:

- a) The terms and conditions shall include a notice as specified in clause 6.3.4.
- b) [PTC]: Clause 9.8 of BRG [5] shall apply with the exception indicated in EVCG [5], clause 18.

Documentary Review	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Terms and Conditions are available to subscribers.

On-Site Inspection	Correct	x	NC-M		NC-m		OBS		IO	
--------------------	---------	---	------	--	------	--	-----	--	----	--

Evidences

Seen Terms and Conditions in website.

7 Compliance with ETSI EN 319 411-2

As per its complementary and brief nature, and in order to increase the readability of this report, assessment according to ETSI EN 319 411-2 will be documented with no extensive quotation of the standard.

Most of norm EN 319 411-2 controls refer to EN 319 411-1, whose assessment has been included previously. ETSI EN 319 411-2 assessment has been performed reviewing the CPS, CP, certificates' profiles and set of test certificates.

- Certificates generated in PKCS#12 comply with EU qualified certificate issued to natural persons (QCP-n).

5.1 General requirements	Correct
5.2 Certification Practice Statement Requirements	Correct
5.3 Certificate Policy name and identification	Correct
6.2.2 Initial Identity Validation Registration a) [QCP-n] and [QCP-n-qscd] the identity of the natural person and, if applicable, any specific attributes of the person, shall be verified: i) by the physical presence of the natural person; or ii) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence;	Correct
6.3.5 Pair and Certificate Usage a) [QCP-n], [QCP-n-qscd], [QCP-l] and [QCP-l-qscd]: the subject's private key shall be maintained under the subject's sole control. b) [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: i) If the subscriber holds the QSCD, then the subscriber's obligation (see clause 6.3.4) shall require that digital signatures are only be created by such a device. ii)) If a QTSP manages the QSCD for the subject, the private key shall not be used for signing except within a QSCD. c) [QCP-n], [QCP-n-qscd], [QCP-l] and [QCP-l-qscd]: the subject's private key shall only be used to create digital signatures.	Correct

<p>6.3.10 Certificate Status Services</p> <p>NOTE 1: Regulation (EU) No 910/2014 requires this service to be provided free of charge.</p> <p>Revocation status</p> <p>a) Revocation status information shall be made available beyond the validity period of the certificate.</p> <p>NOTE 2: The obligation from ETSI EN 319 411-1 [2] to support OCSP is not applicable after the certificate expiry.</p> <p>b) The TSP shall document precisely in its practices statements and in its terms and conditions how requirement a) is met, including TSP termination (see clause 6.4.9).</p>	<p>Correct</p>
<p>6.4.5 Audit Logging Procedures</p> <p>Subject device provision</p> <p>a) [QCP-n-qscd] and [QCP-l-qscd]: the TSP shall log all events relating to the preparation of QSCDs.</p> <p>General</p> <p>b) The TSP shall record all relevant information concerning data issued and received and shall log all events relating to the EU qualified certificate registration, generation, dissemination, and when applicable, revocation management and device preparation.</p> <p>c) The information shall be maintained as necessary to meet legal requirements beyond the termination of the TSP (see clause 6.4.9).</p> <p>d) The TSP shall document how this information is accessible.</p> <p>e) The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.</p> <p>NOTE: Regulation (EU) No 910/2014 article 24.2 (h) requires a qualified TSP to <i>"record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically"</i>.</p>	<p>Correct</p>
<p>6.5.1 Pair Generation and Installation</p> <p>Subject device provision</p> <p>a) [QCP-n-qscd] and [QCP-l-qscd]: the TSP shall verify that the device is meeting the appropriate requirements in terms of qualification and is certified.</p> <p>NOTE 1: Regulation (EU) N° 910/2014 [i.1] requires the QSCD to be certified as meeting the requirements of annex II through a certificate following the rules expressed in sections 4 and 5 of this Regulation.</p>	<p>Correct</p>

6.5.2 Private Key Protection and Cryptographic Module Engineering Controls

Subject device provision

- a) [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]:
 - i) if the device is not prepared by the TSP, the TSP shall verify that the device is a QSCD at the moment of the registration;
 - ii) if the subject's key pair is not generated by the TSP, the certificate request process shall ensure that the public key to be certified is from a key pair effectively generated by a QSCD;
 - iii) if the subject's key pair is managed by a TSP which is not the TSP issuing the certificate itself, the TSP issuing the certificate shall verify that this TSP is qualified.
- b) [QCP-n-qscd] and [QCP-l-qscd]: the TSP shall monitor QSCD certification statuses until the end of the validity period of the certificate and take appropriate measures in case of modification of this status. Such measures shall be documented in the TSP's CPS.
NOTE: When the TSP's CPS or CP requires the revocation of certificates when a certified data is modified, the measures above need to be considered accordingly.

Correct

6.6.1 Certificate Profile

Certificate generation


- a) The certificate shall be issued according to the certificate profile ETSI EN 319 412-5 [4].
- b) [QCP-n-qscd] and [QCP-l-qscd]: the certificate shall include the qcStatement for QSCD (esi4-qcStatement-4) defined in ETSI EN 319 412-5 [4].
- c) [QCP-n-qscd] and [QCP-l-qscd]: the qcStatement for QSCD (esi4-qcStatement-4) shall not be included in certificates that are not issued according to [QCP-n-qscd] or [QCP-l-qscd] requirements.
- d) [QCP-n] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 a); and/or
 - ii)) an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- e) [QCP-l] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 b); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- f) [QCP-n-qscd] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 c); and/or
 - ii) a OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- g) [QCP-l-qscd] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 d); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- h) [QCP-w] the certificate shall include at least one of the following policy identifier:
 - i) the policy identifier defined in clause 5.3 e); and/or
 - ii) a OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- i) [QCP-w]: the policy identifier as specified in EVCG [3] may be included in addition to the identifier(s) required in h).
- j) [CONDITIONAL] if the certificate contains only an OID allocated by the TSP, the referred certificate policy shall be built according to clause 7. In particular it shall clearly identify which of the certificate policy defined in the present document it adopts as the basis.

Correct

<p>6.9.4 Terms and conditions</p> <p>In addition, the following particular requirements apply:</p> <ul style="list-style-type: none">a) the certificate policy shall include a clear statement indicating that the policy is for EU qualified certificates and whether the policy requires use of a QSCD;b) a PKI disclosure statement shall be supported;c) the PKI disclosure statement should be structured according to annex A in ETSI EN 319 411-1 [2].	<p>Correct</p>
---	----------------

8 Documents

8.1 Trust Service Provider's Documents

CPS	<p>Certification Practice Statement</p> <p>DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN IVSIGN CA</p> <p>1.3.6.1.4.1.47304.4.1</p> <p>v0.1 16/01/2018</p>
CPS-2	<p>Additionally, as reference, AC Camerfirma SA's CPS: DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CERTIFICADOS DIGITALES AC CAMERFIRMA SA EIDAS-2016 CHAMBERS OF COMMERCE ROOT - 2016 y GLOBAL CHAMBERSIGN ROOT - 2016. V. V1.2.2,</p> <p>OID 1.3.6.1.4.1.17326.10.1</p> <p>https://policy.camerfirma.com/</p>
CertPro	<p>Certificate profile</p> <p>4000A - Certificado Cualificado Corporativo (P12)</p> <p>[4000]_v1_00_firmado 19/12/2107 JUANÁNGEL MARTÍN GÓMEZ <martin_ja@camerfirma.com>.</p>
CP	<p>Certificate Policy</p> <p>OID 1.3.6.1.4.1.47304.4.16.1.2.2</p>
PDS	<p>PDS.ES IVSIGN CA PKI DISCLOSURE STATEMENT</p> <p>v0</p>
Insurance	<p>Liability Insurance</p> <p>Liberty Mutual Insurance Europe Ltd. Policy with a limit of 3.500.000€.</p> <p>Aon <i>Condiciones Particulares</i> signed on 02/03/2018.</p>
ISO27001_cert	<p>ISO 27001 – Certification – Certificate No SI-0010/2016</p>  <p>Updated scope available at AENOR certificate directory (at their website).</p>
KeyGenScript	<p>Minutes for CA key generation ceremony</p> <p>“Acta de Generación de certificado de Ivsign CA y su OCSP Responder” cod INTJAM2017020 v1 dated 05/10/2017.</p>

RiskAnalysis	PS01 – Análisis de riesgos SGSI Identificación de Activos y Valoración de Riesgos_ALI_v3.xls
TP	Termination Plan, as documented in <i>PS.CA09 Plan de cese de la Autoridad de Certificación IvSign CA</i>
Roles	Role Concept Version x as of y
SC	Subscriber Model Contract
ToU	Terms of Use eula1_IVNOSYS.txt.
NotificationPlan	“PS.CA02 Plan de notificación de incidentes de acuerdo con el artículo 19 del Reglamento (UE) 910/2014 (EIDAS)”
FO001	Listado de documentos en vigor
QCDOC	Documentación certificados cualificados
MA01	Manual de Calidad y Seguridad de la Información, version 2, dated of 16 th January, 2017.
	Política de uso aceptable de los activos, version 1, dated of 10 th March, 2016.
	Política de Calidad y Seguridad de Ivnosys, version 1, dated of 15 th December, 2015.

8.2 General Documents

BRG	CA/Browser Forum – Baseline Requirements Guidelines Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
EIDAS	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
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

8.2.1 Documents used in ETSI EN 319-411-1

The following documents are mentioned in the ETSI Standard with reference [nn]:

[1]	ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
[2]	ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".
[3]	ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[4]	EVCG - CA/Browser Forum (V1.5.5): "Guidelines for The Issuance and Management of Extended Validation Certificates".
[5]	BRG - CA/Browser Forum (V1.3.0): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".
[6]	ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
[7]	IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
[8]	ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; General Policy Requirements for Trust Service Providers".
[9]	ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
[10]	ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
[11]	IETF RFC 6960: "X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP".
[12]	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

8.3 Other documents

TCAB-002CA01-CAR-2018-E	Conformity Assessment Report Initial Certification Version 2 as of 6 th August 2018
-------------------------	--


9 Abbreviations list

AC	Autoridad de Certificación (Certification Authority)
ARL	Authority Certificate Revocation List
BRG	Baseline Requirements Guidelines for the Issuance and Management of Publicly-Trusted Certificates issued by CAB Forum
CA	Certification Authority
CAB	Conformity Assessment Body
CABF	Certificate Authority/Browser Forum. Also “CAB Forum” can be used instead
CC	Common Criteria
CM	Cryptographic Module
CN	Common Name
CP	Certificate Policy
CPD	Centro de Proceso de datos (Data Center)
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider. CSP is used synonymously with CA
DVC	Domain Validation Certificate
DVCP	Domain Validation Certification Policy
DNI	Documento Nacional de Identidad. Citizen ID card.
EAL	Evaluation Assurance Level
EN	European Norm
ENAC	Entidad Nacional de Acreditación
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
EVCP+	Enhanced Extended Validation Certificate Policy (with SUD)
HSM	Hardware Security Module
ICT	Information and Communications Technology ID Identity
IS	Information Security
ISO	International Organization for Standardization
ISMS	Information Security Management System

ITSEC	Information Technology Security Evaluation Criteria
LCP	Lightweight Certificate Policy
MINCOTUR	Ministry of industry, trade and tourism, transitionally hosting the informational website for TSP.Ministry of Economy and Business
MINECO	Ministry of Economy and Business
MPTFP	Finance and Public Administration Ministry
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy (with SUD) NetSec-CAB Network Security Requirements- CA/Browser Forum
NIST	National Institute of Standards and Technology (USA)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy PDCA Plan Do Check Act
PTC	Publicly-Trusted Certificate. PTC is used synonymously with DVC and OVC.
PTC-BR	Publicly-Trusted Certificate Policy-Baseline Requirements. PTC-BR is used synonymously with DVCP and OVCP.
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
SGAD	General Secretariat of Digital Administration
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer (see also TLS)
SUD	Secure User Device
TCAB	Trust Conformity Assessment Body
TLS	Transport Layer Security
TSA	Time-Stamp Authority
TSL	Trust Service Status List
TSP	Trust Service Provider. TSP is used synonymously with CA, when issuing certificates.

10 Certificate of accreditation of the conformity assessment body

Acreditación



Otorga la presente / Grants this

ACREDITACIÓN
166/C-PR333


a

TRUST CONFORMITY ASSESSMENT BODY, S.L.

Según criterios recogidos en la norma UNE-EN ISO/IEC 17065, para las actividades de CERTIFICACIÓN definidas en el ANEXO TÉCNICO nº 166/C-PR333.

According to the criteria in the standard UNE-EN ISO/IEC 17065 for the Certification activities defined in the Technical Annex No 166/C-PR333.

Fecha de entrada en vigor / Coming into effect: 20/07/2018


D. José Manuel Prieto Barrio
Presidente

La acreditación mantiene su vigencia hasta notificación en contra. Este documento no tiene validez sin su correspondiente anexo técnico. La presente acreditación y su anexo técnico están sujetos a modificaciones, suspensiones temporales y retirada. Su vigencia puede confirmarse en www.enac.es.

The accreditation maintains its validity unless otherwise stated. The present accreditation is not valid without its corresponding technical annex. This accreditation and its technical annex could be reduced, temporarily suspended and withdrawn. The state of validity of it can be confirmed at www.enac.es.

ENAC es firmante de los Acuerdos de Reconocimiento Mutuo establecidos en el seno de la European co-operation for Accreditation (EA) y de las organizaciones internacionales de organismos de acreditación, ILAC e IAF (www.enac.es)

ENAC is signatory of the Multilateral Recognition Agreements established by the European co-operation for Accreditation (EA) and the International organizations of accreditation bodies, ILAC and IAF (www.enac.es)

Ref.: CPR/9957 Fecha de emisión 20/07/2018

Código Validación Electrónica: QK27809AH17310n39

La vigencia de la acreditación y del presente certificado puede confirmarse en <http://www.enac.es/web/enac/validacion-electronica> o haciendo clic aquí

This section complies with **REQ-ETAD-3**.