CERTIFICATION PRACTICE STATEMENT

Version:	2.0
Date:	08/10/2025
Created by:	Compliance Department
Approved by:	Jorge Guillamet (Country Manager)

Document Control and Follow up

Version	Date	Creation	Revision	Approval
1.0.	02/27/2020	Cristina Romera Soto (Legal Department)	Carlos Sáez Quintero	Iván Nabalón Barrientos CEO
1.1.	05/29/2020	Cristina Romera Soto (Legal Department) Albert Borrás	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.2.	25.05.2021	Cristina Romera Soto (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.3	15.10.2021	Francisco J. Ferrándiz (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.4	21.10.2021	Francisco J. Ferrándiz (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.5	22.10.2021	Francisco J. Ferrándiz (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos(CEO)
1.6.	03.12.2021	Cristina Romera Soto (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.7.	04.04.2022	Cristina Romera Soto Carlos Sáez Quintero Francisco Ferrándiz (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.8	20.12.2022	Cristina Romera Soto (Legal Department)	Iván Nabalón Barrientos (CEO)	Iván Nabalón Barrientos (CEO)
1.9	17.07.2023	Cristina Romera Soto Carlos Sáez Quintero Francisco Ferrándiz (Legal Department)	Jorge Guillamet (Country Manager)	Jorge Guillamet (Country Manager)
1.10	14/11/2023	Cristina Romera Soto Carlos Sáez Quintero Francisco Ferrándiz (Legal Department)	Jorge Guillamet (Country Manager)	Jorge Guillamet (Country Manager)

1.11	22/01/2024	Cristina Romera Soto Carlos Sáez Quintero Francisco Ferrándiz (Legal Department)	Jorge Guillamet (Country Manager)	Jorge Guillamet (Country Manager)
1.12	28/05/2024	Cristina Romera Soto Carlos Sáez Quintero Francisco Ferrándiz (Legal Department)	Jorge Guillamet (Country Manager)	Jorge Guillamet (Country Manager)
2.0	08/10/2025	Albert Borrás (Compliance Department)	Jorge Guillamet (Country Manager)	Jorge Guillamet (Country Manager)

Latest changes

Version	Date	Change	Description of change
2.0.	08/10/2025	General	- Description of third-party obligations. - Contact information. - Clarification regarding test certificates and self-issued certificates. - Review and expansion of information related to the certificate lifecycle processes, including revocation and suspension. - Extension and further detail of log-related concepts as well as the retention period. - Inclusion of sections concerning incident notification. - Expansion of information regarding CA key management and detailed specifications of certificate profiles. - Annual review of the document, including general wording adjustments and correction of minor errors.

INFORMATION NOTE REGARDING THE CHANGE OF THE COMPANY NAME OF ELECTRONIC IDENTIFICATION S.L. TO SIGNICAT S.L.U.
Electronic Identificacion S.L., with the date of registration in the commercial register on 24 May 2023, has changed its corporate name to SIGNICAT S.L.U. and is currently in the internal process of notification and documentary modification. For clarification purposes, any reference in this Certification Practice Statement and documentation associated with this document or the services provided in which a reference is made to "ELECTRONIC IDENTIFICATION S.L.", "ELECTRONIC ID" or "EID" will be understood to be made by SIGNICAT S.L.U.

Content

1 Introduction

1.1 Presentation

This document contains the reference framework for developing the Statement on Certification Practices and describes each of the paragraphs to be completed, in accordance with RFC 3647.

SIGNICAT SLU, formerly known as, ELECTRONIC IDENTIFICATION, S.L, protected by the Community Denominational Trademark (MC), is a company registered in the Trade and Companies Register of Madrid since March 13th, 2013, holder of the TIN number B86681533 and Registration Data: Volume: 30920, Book: 0, Folio: 146, Section: 8, Page: M556508, dated April 3rd, 2013.

1.2 Document name and identification

This document consists of the SIGNICAT SLU Statement on Certification Practices.

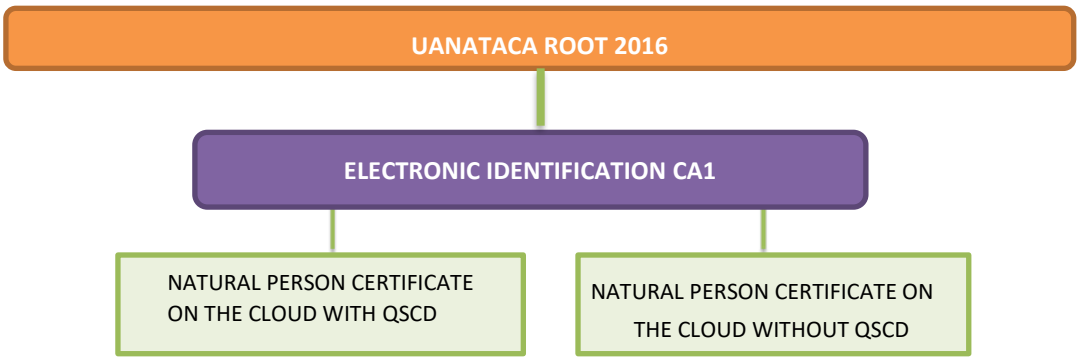
1.3 Participants in certification services

1.3.1 Certification services provider

The electronic certification services provider is the person, natural or legal, who issues and manages certificates for end entities through a Certification Entity, or provides other services associated with the electronic signature.

SIGNICAT SLU (formerly Electronic ID) is a trust electronic service provider, which acts in accordance with the provisions of Regulation (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND COUNCIL, dated July 23rd, 2014, relating to electronic identification and trust services with regard to electronic transactions within the internal market, thus derogating Directive 1999/93 / EC, as well as the technical regulations of ETSI, applicable to the issue and management of qualified certificates, mainly EN 319 411-1 and EN 319 411-2, in order to facilitate compliance with legal prerequisites and international recognition of its services.

For the purposes of providing certification services, SIGNICAT SLU has established a hierarchy of certification entities:



UANATACA ROOT 2016

This is the original certification entity of the hierarchy which issues certificates to other certification entities and whose public key certificate has been automatically signed.

Identification data:

- CN: UANATACA ROOT 2016
- Digital print: 2e69a72bcbf9df1f560be51388d636703d5927ed
- Valid from: Friday, March 11th, 2016
- Valid until: Monday, March 11th, 2041
- RSA key length: 4.096 bytes
- URL: https://web.uanataca.com/common/project/pdf/autoridad-certificacion/01_raizca-2016.cer


```
-----BEGIN CERTIFICATE-----
MIIHAzCCBOugAwIBAgIITWOS6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTEwOTEz
NTNaFw00MTAzMTEwOTEzNTNaMIG5MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEbMBkGA1UEAwwSVUFOQVRBQ0EgUk9PVCAyMDE2MRgwFgYDVQRhDA9W
QVRFUy1BNjY3MjE0OTkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
d5rtQey704cMzz7A1vuB4HLs0Y8YlH7BXKFAuxwzst1GOl7TzZzOeDEjGZMSjI00
JRUdmZ/lmG927tES5dDlrfDrNvKu3mof9j6Wjch4HmNqT6I30TXnhBNbtKEYHWxC
cIvQ0OKaFUUBEt+NzS6smyDAzbwyFUPSPid8JoGaGUMy7hhah38cLN408ffigCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtrLcRbpQ8usMbwJSO1aoi71Lu
ISeBGJjqaszMPOty923PGHemImxHl5mHT13k5ha98EK4ZXMFfjxSVrypvpHgjThU
V3s4ZeaSpSbWkFxl6Tl++OTciMLOp66jwZV3I4DqeRmNXJkiRebs5u8bDDZxxeSP
RusoFI1cLm9cqCNy51hd2LNv8QECUNQ/RPon0sh+BSoSedppYXq6TFqpabE/FTnt
JBU7CMJV3EFJ/jSvXf6qj7JjInUQXajSxDdt0WrmDW8aQCRKCZ0Ml/Iwb8yk83/y
ZDt6E+Ez63V/x7sA2ZygG61zf4wOT95FNA4Z1atfOEcp/2uc5HXKrUTXTMDJJZfD
WMo30Ae1Rei94TRd/9XRqPdEk0B/VL5/991SlEX6Ol0NwKRPm6HNNZoWbdnmLEc+
CGnX1yj01R51Y4UTOalJ/W7oiNxmpZQAdAc9NN/gkwIDAQABo4IBCzCCAQcwHQYD
VR0OBBYEFFUs8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBmAYEVR0gADCBjzAzBggrBgEFBQcCARYnaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMFgGCCsGAQUFBwICMEwMSkNlcnRp
ZmljYWRvIHJhw616IGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFj
YS5jb20vcHVibGljL3BraS9kcGMvMA4GA1UdDwEB/wQEAwIBBjAcBgNVHREEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEATAyOSKmK/yj6
JFb/RaHMmor8knkwQWVi3lFASKyfLQc6FfHoVjEgihu6HekIlMS7WBzetQVomaTR
TDu6eJeyo/+7CB+VGGHOYYjSdc8F8WI1HFN3f6ztKuM6zlVz3Xyj9BHhg1H4gqNL
Yxe99kq14xQEOR/fm0p7rVgVeeHhG8m1S5UGyyJ1ukeiB0d0PqwVWlG1np+i/nhf
```

nrxGSTnbRJyHzx6tuaLuQyHQU+Dg0TS8k65a8URioVkQ0CWb7yIyJ5bEBmPR2yqX
Owt6nYR8/3blrU99+wp67pmQttSggX3sB2a9WfY94Y5uIPB7JisOUBmqH23RjakE
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzkzSl/i4G+Zxya8oQb2cIqF
HnvyCVXDOd4/CWNBLZQCTyGRUKOocvu1kKXgmVY6hTQGhM8Tr5yg/XT21gaAv3/7
th5ib2iGgq8Q8E3AW3ND+8N/qMjZ2aIkBKQYUFmLWiZt6n6ni73E2LQQEs+0uh9+
1xTPcI7AfDv+p0m6HDP0pq0t7BX0DQbh5QwPpiHBkB8atzE5gmQxnkt4/g0S2av5
Lc+U7ufZ5/ao7tLL1qkTX2r87jN7T8+lZOSHBbQan2QosyBfZWXgxaFYTspoy5tP
n4RMcCgXqHSYlArUKaQ8OWmT42AKLdY= -----END CERTIFICATE-----

ELECTRONIC IDENTIFICATION CA1

This is the certification entity that issues certificates to end entities within the hierarchy and whose public key certificate has been digitally signed by UANATACA ROOT 2016.

Identification data:

- CN: ELECTRONIC IDENTIFICATION CA1
- Digital print: 2e69a72bcbf9df1f560be51388d636703d5927ed
- Valid from: Tuesday 02.25.2020
- Valid until: Thursday 02.24.2033
- RSA key length: 4.096 bytes
- URL:https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIO NCA1. pem.cer

-----BEGIN CERTIFICATE-----
MIIIdTCCBl2gAwIBAgIINsAgN1d7Z1EwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0yMDAyMjUxMDU3
MTNaFw0zMzAyMjQxMDU3MTNaMIGbMQswCQYDVQQGEwJFUzEPMA0GA1UEBwwGTUFE
UklEMScwJQYDVQQKDB5FbGVjdHJvbmljIElkZW50aWZpY2F0aW9uIFMuTC4xEDAO
BgNVBAsMB1BTQy1FSUQxJjAkBgNVBAMMHUVMRUNUUk9OSUMgSURFTlRJRklDQVRJ
T04gQ0ExMRgwFgYDVQRhDA9WQVRFUy1CODY2ODE1MzMwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDAFOTSwnEBJSAM6h9FT5ETiVHAtI1K885qGC6Bd+5i
UMhUmHUek5m1PZxJzUsMUNndPBfaRIi2os4upOnwrwNsk0bOfdTKh6qwmN5Uqstb
L9QH2W3eLYeUZHH11dY/be3PZSUICrMZZRUT/YP5GBhhJR+uy69AYJ8VzeLwjMtl
guse840QBRALuPRP7Q4U2P//hfFvw2vlZAEpnAFeO4pK6Ey9dzXciZpPteL/9CYf
1Cl48fNpFs85Pjsl/2xKycrRIYc0dCTe6yCTlzFPbZX5xsKicMzvFdsN//6BFckb
/1f8hW7ywZkgBHUfuvNkLrL7LfDdvYdGM8vzfS5Ozz7j+nXFs1MYc0g4iIumynhp
tmpkR1n/+JDMNf3uTFWlXUZO9dy4cfr7zqLm+Y+a+6ARud8K8aKRCHUFqOEMWKJB
4T7C1a1+/omPvXeAHjB8nt1Eqw4tACQQhbB3AHbdd5bnwp4mxu/o97kvfI0TCE5c
+IqacLZWW8SXDmRHv2hQTkCA1Gte5qJLnC/M0aWbyd0XFkYj9Xjzoa4k0oYSRI+0
wbKrhTlYQu8t14dLvOxujfRlOx1ZZfQwVEqPvIJjN8t5K97POI2kyaoOcFG5iwAo
06bvLfxEgq7kDU05OZ0UxZut5Q7SUB9f9lkA9bFkeg+9RQtBSNUdj7BCosvJmaOQ
0wIDAQABo4ICmzCCApcwfgYIKwYBBQUHAQEEcjBwMDYGCCsGAQUFBzABhipodHRw

Oi8vb2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUH
MAGGKmh0dHA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAd
BgNVHQ4EFgQUhRVkzZsHSJ335ppEB5x5Coyhlj8wEgYDVR0TAQH/BAgwBgEB/wIB
ADAfBgNVHSMEGDAWgBRVLPG8oV657qAviFcQW/yW95GaLDAcBgNVHRIEFTATgRFp
bmZvQHVhbmF0YWNhLmNvbTCB4wYDVR0gBIHbMIHYMIHVBgRVHSAAMIHMME0GCCsG
AQUFBwIBFkFodHRwczovL3d3dy5lbGVjdHJvbmljaWQuZXUvY2VydGlmaWNhdGlv
bi1wcmFjdGljZS1zdGF0ZW1lbnQtY3BkLzB7BggrBgEFBQcCAjBvDG1DZXJ0aWZp
Y2FkbyBkZSBsYSBBdXRvcmlkYWQgZGUgQ2VydGlmaWNhY2nDs24gU3Vib3JkaW5h
ZGEgZGUgRWxlY3Ryb25pYyBJRGVudGlmaWNhdGlvbi4gLSB3d3cuZWxlY3Ryb25p
Y2lkLmV1MIGLBgNVHR8EgYMwgYAwPqA8oDqGOGh0dHA6Ly9jcmwxLnVhbmF0YWNh
LmNvbS9wdWJsaWMvcGtpL2NybC9hcmxfdWFuYXRhY2EuY3JsMD6gPKA6hjhodHRw
Oi8vY3JsMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvYXJsX3VhbmF0YWNh
LmNybDAOBgNVHQ8BAf8EBAMCAQYwHwYDVR0RBBgwFoEUaW5mb0BlbGVjdHJvbmlj
aWQuZXUwDQYJKoZIhvcNAQELBQADggIBABd3oBLIIp7Saspm9DWVMudT79NCJ02h
00t8P1PZR0zz3KAkdrO4G1hg92vKqzhjgJsHMYt2zV8XYQ487T2S/pKbIMTTDFHR
wSNyU5S4z8p4gufCF8kkrZlRim0SKBtiaYnKLqmtiyiLjnPvegwpq3gVcg8afKI5
qxnShchNH+lveNx/QC7MePku0FAZY9naFEPmcdSs3mGiVHZbuv5eWsqm4/BMx+4X
PBmHO8Vjj2HzUdfCcavkXkocDA8+7WB+aQHZ3gHZQvC0pFKSwO6YSdo8d/IfICzU
J7yADUkVvDW4DMox6GwnXc8b9WQkjWHPXSHLMs93kzLtE3Lws9C//I1lMbf4o7U4
wkt55M3nYO2mt7AEwS9oKSDr3hQsN6IA/IMwoYj4oML9U6ytcYTNUQINRWShyLdf
WMwtOZmhlQXbbYqlXHhwVqL1hjlQ6bPOARKOo186ol5cP0LEV4ehDDVQoHZFgRje
MPD/UEQp83v9Q4swHZjzTlsBhlRhZH5g+TWXTYBPOs94quaJRI9QVlVk7ICEsQA6
11F1XG4tkX7CuvuOdPjv1VBrJPM4oREsU1YXxNzew3+NH1IJ4SS/RpwiwctUpepR
vRyrQlKf4bHqMTXh04CsE19fE8RLjxy7VnCDTbrYo7TCAoQQMbQwK9nEOIOOeTs2
d3QXqGqKXRth -----END CERTIFICATE-----

1.3.2 Registration Authorities

A Registration Authority may consist of a natural or legal person acting in accordance with this Statement on Certification Practices and, where applicable, by means of an agreement signed with a concrete CA, exercising the functions of requests management, identification and registration of certificate applicants, as well as those provided for in the specific Certification Policies. RAs are delegated authorities of the CA, although the latter is ultimately responsible for the service.

An SIGNICAT SLU Registration Authority is the entity responsible for:

- Processing certificates requests.
- Identify the applicant and check that he meets the prerequisites necessary for applying for the certificate.
- Validate the personal circumstances of the person who will appear as signatory on the certificate.
- Manage key generation and certificate issuance.
- Issue the certificate to the subscriber or reveal the means of its generation.

- Protect the documentation relating to the identification and registration of signatories and / or subscribers, as well as the life cycle management of certificates.

Who can act as SIGNICAT SLU RA?

- Any entity authorized by SIGNICAT SLU
- SIGNICAT SLU directly.

SIGNICAT SLU will contractually formalize the relationship between itself and each of the entities acting as SIGNICAT SLU Registration Authorities.

The entity acting as the SIGNICAT SLU Registration Authority may authorize one or more persons as the RA Operator, to operate the SIGNICAT SLU certificates issuance system on behalf of the Registration Authority.

The Registration Authority may delegate the functions of identifying subscribers and / or signatories, subject to prior collaboration agreement where the delegation of these functions is accepted. SIGNICAT SLU must expressly authorize this collaboration agreement.

The Registration Authorities subject to this Statement on Certification Practices may also consist of units designated for the purposes of this function by the subscribers of certificates, such as a human resources department, since it has authentic records relating to the link between the signatories and the subscriber.

1.3.3 Subscribers

The certification service subscribers are:

- Enterprises, entities, corporations and companies that acquire from SIGNICAT SLU (either directly or through a third party), for use within their professional corporate domain, and are identified on the certificates.

- The natural persons who acquire the certificates for their own use, and are identified as such on the certificates.

The subscriber of the certification service acquires a license to use the certificate, for own use - electronic seal certificates - or, for the purpose of facilitating the certification of the identity of a specific person and duly authorized to act within the subscriber's organizational structure - electronic signature certificates. In the latter case, this person is identified on the certificate.

The subscriber of the electronic trust service is, therefore, the client of the certification service provider, in compliance with private legislation, and has the rights and obligations defined by the certification service provider, which are additional and considered without prejudice to rights and obligations of signatories, as authorized and governed by European technical regulations applicable to the issue of qualified electronic certificates, ETSI EN 319 411 in particular, sections 5.4.2 and 6.3.4. e).

1.3.4 Trust parties

This SCP considers as a User Party or User, the person who receives an electronic transaction carried out via a certificate issued by any of the CAs of SIGNICAT SLU and who voluntarily entrusts the Certificate issued by it.

1.3.5 Other participants

Public Key Infrastructure Services Provider

SIGNICAT SLU and UANATACA, S.A. have entered into a technology service provision contract pursuant to which UANATACA will provide the public key infrastructure (PKI) in support of the SIGNICAT SLU trust services. Likewise, UANATACA provides SIGNICAT SLU with the technical staff necessary for the correct performance of reliable functions specific to a Trust Services Provider.

That said, UANATACA is the provider of infrastructure services relating to certification services, lends its technological services to SIGNICAT SLU in order that it can fulfill the services inherent to a Trust Service Provider, ensuring services continuity at all times under the conditions and in accordance with the prerequisites required by the regulations.

Likewise, UANATACA is a Trust Service Provider certified under the provisions of European Regulation No. 910/2014 of the European Parliament and Council, dated July 23rd, 2014, relating to electronic identification and trust services with regard to electronic transactions on the internal market, thus derogating Directive 1999/93 / EC (EIDAS Regulation).

UANATACA's PKI is subject to annual audits in order to assess the compliance of qualified trust service providers, in accordance with applicable regulations, under ISO / IEC 17065: 2012, ETSI EN 319 403 V2.2.2., ETSI EN 319 421 v1.1.1, ETSI EN 319 401 v2.1.1, ETSI EN 319 411-2 v 2.1.1 and ETSI EN 319 411-1 v 1.1.1.

The Public Key Infrastructure service provider undertakes to provide SIGNICAT SLU with the necessary technological services for the delivery of certification services. In this regard:

- The provider shall have the appropriate hardware and software resources to ensure that the services are delivered in compliance with the security levels required by the applicable regulations.
- The provider shall be responsible for the custody and hosting of these systems in a Data Processing Center that meets internationally recognized standards for both logical and physical security.
- The provider shall carry out all necessary maintenance activities—preventive, corrective, adaptive, and reactive—to ensure the continuity and quality of the technological services.
- The provider shall deliver third-level technical support, i.e., support that exceeds SIGNICAT SLU internal management capabilities and is directly related to technical issues or failures in the infrastructure.

- The provider shall make available the qualified technical personnel required for the operation of the PKI infrastructure, including trusted roles responsible for system administration and operation.

1.4 Use of certificates

1.4.1 Certificates permitted uses

Qualified Natural Person Certificate on the CLOUD without QSCD

This document has OID 1.3.6.1.4.1.55193.1.1.1. certification. This is a qualified certificate, issued for the purposes of advanced electronic signature and authentication, in accordance with the QCP-n certification policy, with OID 0.4.0.194112.1.0. The natural person certificates on the CLOUD consist of certificates which qualify under the provisions of Articles 24 and 28 of Regulation (EU) 910/2014.

They guarantee the identity of the subscriber and of the person appearing in the certificate and allow the generation of the "advanced electronic signature, based on a qualified electronic certificate".

Certificates can be used in the following applications:

a) Authentication in access control systems.

b) Email secure signature.

c) Other electronic signature applications, in accordance with the agreements between the parties or the legal regulations applicable in each case.

The usage information in the certificate profile indicates the following:

The "key usage" field is enabled and thus allows performance of the following functions:

a. Digital signature in order to perform the authentication function.

b. Content Commitment in order carry out the electronic signature function.

c. Key Encipherment

Qualified Natural Person Certificate on the CLOUD with QSCD

This document has OID 1.3.6.1.4.1.55193.1.1.2. certification. This is a qualified certificate, issued for the purposes of advanced electronic signatures and their authentication, in accordance with the QCPn-qscd certification policy, with OID 0.4.0.194112.1.2. This certificate is issued in a centralized QSCD and it consists of a qualified certificate in accordance with the provisions set out under Article 28 of Regulation (EU) 910/2014.

It operates using qualified signature creation devices (QSCD), in accordance with Articles 29 and 51 of Regulation (EU) 910/2014 and complies with the provisions of the technical regulations of the European Telecommunications Standards Institute, identified by the reference number ETSI EN 319 411-2.

It guarantees the identity of the signatory and his link with the subscriber of the trust electronic service, by allowing the generation of the "qualified electronic signature", that is to say, the advanced signature, based on a qualified certificate, which has been generated by means of a qualified device, thus equaling the handwritten signature for legal effects and purposes, without the need to comply with any other additional prerequisites.

It can also be used by other applications that do not require the electronic signature as an equivalent to the handwritten signature, such as in the applications described below:

a) Email secure signature.

b) Other email applications.

The usage information in the certificate profile indicates the following:

The « key usage » field is enabled and thus allows performance of the following functions:

a. Digital signature in order to perform the authentication function

b. Content Commitment in order carry out the electronic signature function

c. Key Encipherment

1.4.2 Limits and prohibitions on the use of certificates

Certificates are used in accordance with their own functions and for the purposes established, and cannot be used for other functions and other purposes.

Likewise, certificates must be used exclusively in accordance with applicable regulations, taking particular account of import and export restrictions at all times.

Certificates cannot be used to sign any certificate whose key is public, or to sign certificate revocation lists (CRL).

The certificates were not designed, nor can they be intended, nor their use or resale as equipment for the control of dangerous situations be authorized and neither can they be permitted in cases where uses require faultless interventions, such as in the operation of nuclear installations, navigation or air communications systems, or weapon control systems where an error can directly result in death, personal injury or serious environmental damage.

The use of digital certificates in transactions that contravene this Statement on Certification Practices, in the legal documents related to each certificate or the contracts with registration entities or with their signatories / subscribers, should be considered as an undue use for all

relevant legal effects and purposes, SIGNICAT SLU therefore being hold harmless in accordance with the legislation in force from any liability due to inappropriate use of the certificates, made by the signatory or by any third party.

SIGNICAT SLU does not have access to data to which the use of a certificate may be applied. Consequently, and because of the technical impossibility of having this access to the content of the message, SIGNICAT SLU cannot evaluate this content, the subscriber, the signatory or the person responsible for the protection must therefore assume all responsibility arising from the content and related to certificate usage.

Likewise, the subscriber, the signatory, or the person responsible for the protection will have to assume any responsibility likely to result from the use of this outside the limits and conditions of use appearing in this Statement on Certification Practices, the legal documents related to each certificate or the contracts or agreements with the registration entities or with their subscribers, as well as any other improper use thereof, derived from this paragraph or likely to be interpreted as such under the legislation in force.

1.5 Policy management

1.5.1 Company managing the document

SIGNICAT, S.L.U.: B-86681533
Avenida Ciudad de Barcelona, 81. 4ª Planta
28007 Madrid (Spain)

1.5.2 Contact data

SIGNICAT, S.L.U.: B-86681533
Avenida Ciudad de Barcelona, 81. 4ª Planta
28007 Madrid (Spain)
eIDLegal@signicat.com

1.5.3 Document management procedures

The SIGNICAT SLU documentary and organizational system guarantees the proper management of this document and the specifications of the service associated with it, thanks to the existence and application of the corresponding procedures.

1.5.4 1.5.4. SIGNICAT SLU OID Arc

The IANA, in its PEN (Private Enterprise Numbers) registry, has assigned SIGNICAT SLU (formerly Electronic ID) the following OID: 55193. Accordingly, its OID arc starts as 1.3.6.1.4.1.55193

1.5.5 Primary Certificates Policy OIDs

This SCP considers the following meanings of OID

CERTIFICATE	**OID Identifier**
Qualified Natural Person Certificate on the CLOUD without QSCD	1.3.6.1.4.1.55193.1.1.1
Qualified Natural Person Certificate with QSCD managed by the User	1.3.6.1.4.1.55193.1.1.2

2 Publication of information and deposit of certificates

2.1 Directory

SIGNICAT SLU has a certificates Directory where information about certification services is published.

This service is available 24/7 and, in the event of a system failure for a cause not attributable to SIGNICAT SLU, the latter will strive to ensure that the service is available again within the time limit set out in section 5.7.4 of this Statement on Certification Practices.

SIGNICAT SLU requests the prior authorization of the holder to publish the certificate.

2.2 Publication of the information of the electronic certification services provider

SIGNICAT SLU publishes the following information in its Directory:

- Issued certificates.
- Lists of revoked certificates and other information relating to the certificate revocation status.
- Applicable certification policies.
- The Statement on Certification Practices.

Any modification to the specifications or conditions of the service shall be communicated to users by the Certification Entity, via its Web page.

2.3 Publication frequency.

Information about the certification services provider, including policies and the Statement on Certification Practices, are published as they become available.

Changes to the Statement on Reporting Practices are governed by the provisions of section 1.5. of this document.

Information relating to the status of certificate revocation is published in accordance with the provisions of sections 4.9.9 and 4.9.10 of this Statement on Certification Practices.

2.4 Control of access to directories.

SIGNICAT SLU does not restrict access to reading the information in section 2.2. but establishes controls to prevent unauthorized persons from adding, modifying or otherwise deleting records from the Deposit, in order to protect the integrity and authenticity of information, especially that relating to the state of revocation.

SIGNICAT SLU uses reliable systems with regard to the Directory, so that:

- Only authorized persons can make annotations and modifications.
- The authenticity of the information can be verified.

- Certificates are only available for consultation if the natural person identified in the certificate has consented to it.
- Any technical modification affecting the security prerequisites can be detected.

3 Identification and authentication

3.1 Identification

3.1.1 Types of names

All certificates contain a distinguished name (DN) conforming to the X.501 standard in the Subject field, including a Common Name (CN=) component, relating to the identity of the subscriber and of the physical person identified in the certificate, as well as various information relating to additional identities in the SubjectAlternativeName field.

The names contained in the certificates are as follows:

Qualified Natural Person Certificate on the CLOUD without QSCD

Country (C) -	State[1]
Surname	Signatory surname
Given Name	Signatory given name
Serial Number	Identity card / NIE / Passport or other suitable identification number of the signatory, recognized in law
Common Name (CN)	Signatory surname and given name

Qualified Natural Person Certificate on the CLOUD with QSCD

Country (C)	State [2]

[1] The "State" field will correspond to that of the state where the contractual relationship occurs between the signatory and the entity to which he is linked (because it is an employee, member, partner or other type of link), regardless of the worker's nationality. [2] The "State" field will correspond to that of the state where the contractual relationship occurs between the signatory and the entity to which he is linked (because it is an employee, member, partner or other type of link), regardless of the worker's nationality.

Surname	Signatory surname
Given Name	Signatory given name
Serial Number	Identity card / NIE / Passport or other suitable identification number of the signatory, recognized in law
Common Name (CN)	Signatory surname and given name

3.1.2 Signification of names

The names contained in the SubjectName and SubjectAlternativeName fields are understandable in natural language, in accordance with the provisions of the previous section.

If the data indicated in the CN or Subject are fictitious or it is expressly indicated that the certificate is not valid, the latter will be deemed to be devoid of legal validity and, consequently therefore, without liability on the TSP, since the purpose of these certificates is that they are delivered in order to carry out technical and evaluation tests of the regulatory entity.

3.1.3 Issuance test certificates

As a general rule, test certificates will be issued with the following identifying data, without prejudice to any modifications that may arise as a result of regulatory changes and/or specific instructions issued by the National Supervisory Body:

- National Identity Document (DNI) number: 00000000T
- Foreigner Identity Number (NIE): X0000000T, Y0000000R, Z0000000W
- Name: Name
- First last name: Last name1
- Second last name: Last name2

The rest of the fields that make up the “DN” or “Subject” of the certificate must use words that denote its invalidity (e.g. “TEST” or “INVALID”).

If necessary and with prior notice to the National Supervisory Body, SIGNICAT SLU may generate test certificates with other data, the validity of which will be limited to the duration of the tests.

All test certificates will be considered without legal validity and therefore without any liability on SIGNICAT SLU.

These certificates are issued to carry out technical interoperability tests and allow the regulatory body to evaluate them.

3.1.4 Use of anonyms and pseudonyms

Pseudonyms may not be used under any circumstances to identify any entity, business, company, or signatory. Likewise, anonymous certificates are not issued under any circumstances.

3.1.5 Interpretation of names' formats

The names' formats are interpreted in accordance with the law of the subscriber's country of residence, in its own terms.

The "country" or "state" field will be that of the subscriber of the certificate.

The "serial number" field includes the Identity Card, NIE, Passport and other suitable identification number of the signatory, recognized in law.

3.1.6 Uniqueness of names

Names are unique to each individual subscriber.

A subscriber name already in use cannot be assigned to a different subscriber, which is a situation, in principle that cannot arise thanks to the presence of the Tax Identification Number or equivalent in the names scheme.

A subscriber may request more than one certificate provided that the combination of the following values, present in the request, is different from a currently existing and valid certificate:

- Tax Identification Number (TIN) or other legally valid identifier of the natural person.
- Tax Identification Number (TIN) or other legally valid identifier of the subscriber.
- Type of certificate (OID of the certification policy identifier).
- Certificate support (QSCD, software, centralized BNT, Centralized QSCD)

As an exception, this SCP allows a certificate to be issued in the event of a coincidental TIN of the subscriber, signatory, type of certificate, certificate support, with an active certificate, provided that there is a differentiating element between them, in the function (title) and / or service (Organizational Unit).

3.2 Initial validation of identity

The identity of the subscribers of certificates is validated when the contract is signed between the company and the subscriber, at which time the existence of the subscriber is verified by means of an official identity document.

3.2.1 Proof of possession of the private key

The possession of the private key is demonstrated through the reliable procedure of issuance and acceptance of the certificate by the subscriber using a seal certificate or by the signatory using a signature certificate.

3.2.2 Validation of Identity

SIGNICAT SLU shall verify when issuing a qualified certificate for a trusted service by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom a qualified certificate is issued where applicable. The identity of the natural person identified in the certificate must be rigorously confirmed, therefore, when issuing the certificate, the identity of the signatory is accredited before a registry operator, verifying it through the exhibition of documents or through its own information sources, keeping documentation accrediting the validity of the same. In this regard, SIGNICAT SLU will verify the information either directly or through a third party in accordance with national law:

a) in the presence of the natural person, for which purposes the subscriber must appear in person at the offices of SIGNICAT SLU at Av. de la Ciudad de Barcelona, 81, 4, 28007 Madrid as there are no delegated registration authorities;

b) remotely, using electronic identification means in accordance with the provisions of Order ETD/465/2021, dated May 6th, which regulates remote video identification methods for the issuance of qualified electronic certificates;

c) by means of a qualified electronic signature certificate or a qualified electronic seal issued in accordance with letter a) or b), or;

Documentary justification of the link of a natural person identified in a certificate with the entity tied to its consistency in the internal registry of the entity.

Notwithstanding the above, identity validation is not required when the identity or other permanent circumstances of the signatories to whom the certificates are issued are already recorded in SIGNICAT SLU by virtue of a pre-existing relationship, provided that a method of face-to-face identification has been used to identify the signatory and that no more than 5 years have elapsed.

3.2.3 Authentication of the identity of a natural person

The identity of the certificate applicant and the identity of the signing natural persons identified in the certificates shall be verified and validated by the operator or authorized personnel of the SIGNICAT SLU Registration Authority, as follows:

o When the identification has been performed physically, through the review of the:

- Identity document provided.

o When the identification has been done through the electronic identification method via SIGNICAT SLU video identification, through the process identified in section 3.2.4 of this document by means of:

- Review of the videos and images taken of the identification document provided and of the applicant himself/herself.
- Review of the applicant's proof of life, through the results provided by the remote video identification system.
- Review of the comparison produced by the remote video identification system of the photo of the identity document with the images and video obtained during the registration of the applicant.
- Review generated by the remote video identification system, through artificial intelligence for the detection of false identity documents.

3.2.4 Unverified subscriber information.

SIGNICAT SLU does not include any unverified subscriber information in certificates.

3.2.5 Authentication of the identity of a RE and its operators

In the case of the linking of a new registration authority, the necessary verifications must be carried out to confirm the existence of the entity or organization in question, for which purpose documents or own sources of information can be used.

In the same way, directly or through the registration authority, the identity of the operators of the registration authorities should be verified by sending the corresponding identification documentation, as well as their authorization to act.

It must ensure that the operators of the Registration Authority have sufficient training for the performance of their functions, also evaluating them for this purpose

In the event that a Registration Authority operator wishes to obtain a certificate of any other certificate profile, provided that the conditions for issuance are met, they shall not act as the registration operator for the request of such certificate. In such cases, the RA operator must be a person other than the certificate applicant.

3.2.6 Validation of Identity by Electronic Means

The Video Identification Process or Asynchronous Video Conferencing (hereinafter referred to as the "Video Identification Process" or the "Process") is a method of real-time unattended remote video identity verification, which records the entire registration process of a person and allows for the remote validation of identity documents, by means of a video recording that captures and validates the identity document in real-time and in an automated manner (approximately 10-20 seconds), which is carried out by SIGNICAT SLU through its verification operators.

The process consists of two parts, an automatic module in which multiple controls of security elements of the document shown during the video recording are carried out, as well as a biometric facial comparison between the bearer of the document, the user, and the photo of the same, carrying out a proof of life and accurate data extraction by turns.

All this information serves as a decision support element for a human agent of the registration authority, who will review the complete video recording later (asynchronously), determining whether or not an identity can be granted on the basis of the evidence shown.

The technology verifies the authenticity of identity documents, including real-time security checks, such as the detection of holograms, badges, patterns and other document security features.

Description of the video identification process

The video-identification process is developed on the basis of the following elements:

- Voice and text guidance during the video-identification process.
- Automated control of the elements of the environment (lighting conditions, network, camera quality) to obtain an optimal recording of the video identification and its evidence.
- Comparison of images with original documents through pattern matching technology to verify the authenticity of the document.
- Data extraction (OCR) from the MRZ or other parts of the document and possibility to call up credentials in real time.
- Verification that the front and back (if applicable) are from the same document.
- Biometric enrolment of the person and real-time comparison with the image of the identity document.
- Registration Authority Verification Tool, for review of the process by a qualified human being previously groomed by specific training.

In this sense, once the user selects the document to be used to carry out the process, a streaming video recording controlled by the application will be made in which the process is initiated and in

which the user will show the front and back of his/her document for identification and validation in real time. In addition, the user will also be asked to show his face for a facial recognition process based on automatic biometric scoring, including life detection, asking the User to interact with a movement and data extraction of the document by OCR.

For the asynchronous review by a human agent, there is a security protocol based on EU good practices that relies on the tool offered to the human agent in which the evidence obtained during the Process is shown, as well as the flags or notifications of those not obtained. The whole process is tracked with a time stamp at each step.

Therefore, the system ensures the chain of custody of the verification from the evidence collected by the automatic video process to the traces that link the identification to the qualified agent of the registration authority. The result is a verified identity with technical security equivalent to that performed in the presence of the subject.

User's obligations in relation to the video-identification process

The user, throughout the process, undertakes to:

- Use the service in accordance with the provisions of the terms and conditions of the video identification process and issue of qualified certificates, in the Certification Practices Statement, in the particular conditions that may be applicable, and with any other instruction, manual or procedure provided by SIGNICAT SLU.

- Ensure that the document used in the process is an authentic, legally valid document and, furthermore:

    - Is neither a photocopy nor a printed card.
    - Is not in digital format (mobile, tablet or computer).
    - It is not inside a cover.
    - It is complete and uncompromised by deterioration, containing all security elements.

- And throughout the process and while recording the video, to avoid rejection:

    - That lighting conditions in the video allow a clear view of both the identified person's face and the document.
    - The video must have a constant flow with no interruptions or delays.
    - A living person must show the identification.
    - Should someone other than the person subject to identification be carrying out the process, then identification will be rejected.
    - Should someone else be present in the video but is obviously not acting in concert with the person to be identified, then the identification may still be valid, in the same way that it is supposed that a certain person is helping is disabled person to carry out the identification.

- All areas of what is captured by the document must be clearly seen, from the rear, from the front as well as the person's face.
- The user may not be asleep or otherwise display signs which may be interpreted as being under the influence of drugs or alcohol.

Information retention period

All information in relation to the video-identification process and the issue of qualified electronic certificates in the identity video-identification process, including biometric information, will be kept for the duration of the contractual relationship, as long as the deletion thereof is not requested, and for the period of limitation of any legal actions that may arise, or claims that may be received from official bodies.

The maximum period of conservation of the relevant information in relation to the video-identification process and issuance of qualified certificates will be 15 years from the time of issuance of the certificate, unless otherwise provided by law. Once our relationship has ended, the Data will be duly blocked, in accordance with the provisions of the applicable regulations. In addition, it is reported that all evidence of incomplete identification processes that have not been completed due to suspicion of attempted fraud will be retained for a period of 5 years from the execution of the Process, specifying the reason for non-completion, in accordance with the policy established for this purpose.

3.3 Identification and authentication of renewal requests

3.3.1 Usual renewal identification and authentication

Before renewing a certificate, the operator or other authorized personnel verifies that the information used to verify the identity and the remaining data of the subscriber and the natural person identified in the certificate are still valid.

SIGNICAT SLU or an operator or staff authorized by the Registration Authority authenticates requests and files relating to the revocation, suspension or reactivation of a certificate, verifying that they come from an authorized person.

The identification of subscribers and / or signatories during the procedure for revocation, suspension or reactivation of certificates may be carried out by:

The subscriber and/or signatory:

- By identification and authentication through the use of the Revocation Code (ERC) on the UANATACA web page, 24x7. The use of the "ERC" code relating to the previous certificate, or other personal authentication methods consisting of information that only the natural person identified in the certificate knows, which allows her to renew his certificate automatically provided that the legally set maximum deadline has not expired.

- Other means of communication such as telephone, e-mail, etc. provided that there are reasonable guarantees with regard to the identity of the applicant of the suspension or revocation, of the notice of SIGNICAT SLU and / or the Registration Authorities.

The SIGNICAT SLU registration authorities will have to identify the signatory when requesting revocation, suspension or reactivation, depending on the means deemed necessary.

If, during business hours, the subscriber wishes to request a revocation and there are doubts as to his identification, his certificate shall then go into a state of suspension.

One method by which the status of certificates can be verified is to consult the most recent Certificate Revocation List issued by the SIGNICAT SLU Certification Entity.

Certificate Revocation Lists are published on the Certification Entity Directory, as well as on the following Web addresses, as indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

The validity of certificates can also be checked through the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

3.3.2 Identification and authentication for the purposes of renewal following revocation

Prior to renewal, the authorized personnel of the Registration Authority must verify that the information used at the time to verify the identity and the remaining data of the subscriber and of the natural person identified in the previous certificate remains valid.

Renewal of certificates following revocation will only be possible in the following cases:

- Certificate incorrectly revoked from a person other than the one identified in the certificate.
- Certificate revoked through unauthorized issue by the natural person identified in the certificate.
- Certificate containing false or erroneous information.

Whenever the subscriber' information or that of the natural person identified in the certificate changes, the new information is to be duly recorded and full identification is to take place.

3.4 Identification and authentication of the request for revocation

SIGNICAT SLU or an operator or staff authorized by the Registration Authority authenticates requests and files relating to the revocation, suspension or reactivation of a certificate, verifying that they come from an authorized person.

The identification of subscribers and / or signatories during the procedure for revocation, suspension or reactivation of certificates may be carried out by:

- The subscriber and/or signatory:

o By identifying and authenticating through the use of the Revocation Code (ERC) on the UANATACA Web page, 24x7.

o Other means of communication like telephone, email, etc. provided that there are reasonable guarantees having regard to the identity of the applicant for the suspension or revocation, the opinion of SIGNICAT SLU and / or the Registration Authorities.

- The SIGNICAT SLU registration authorities will have to identify the signatory when requesting revocation, suspension or reactivation, according to their own resources where deemed necessary.

If, during business hours, the subscriber wishes to request a revocation, and there are doubts as to his identification, his certificate shall then go into a state of suspension.

4 Operational prerequisites for the lifecycle of the certificate

4.1 4.1. Short term certificates

4.1.1 4.1.1. Request for short term certificates issuance.

The Certificate application process may be carried out either through SIGNICAT SLU or through third parties of a public or private nature with which SIGNICAT SLU has entered into certain contractual arrangements.

When the Applicant, either through SIGNICAT SLU or the third parties indicated above, requests the issue of a certificate, SIGNICAT SLU will send an email to confirm the issue of the certificate and to start the Identification process in accordance with the provisions of section 3.2.4 of this document (for the purposes of clause 4.1, hereinafter referred to as the Identification Process), as well as providing the applicant with the information relating to the necessary pre-configuration relating to the remote identity accreditation process and the issue and use of the qualified natural person certificate. In this process, the applicant will be provided via email with a link to start the Identification Process.

4.1.1.1 Legitimization in order to request the certificate issuance

By accessing the link, the applicant shall be deemed to accept the certificate issuance request and, additionally, must read and expressly accept the conditions of the identification process by ticking a checkbox enabled for this purpose. The ticking of this selection box by the applicant shall be deemed a simple signature

4.1.2 Processing of the certification request

4.1.2.1 Carrying out and completing identification and authentication functions

Prior to issuing the email to the Applicant, SIGNICAT SLU will generate an identification code that will be sent to the Applicant in said email for the purpose of linking the identification process with the specific certificate request by the Applicant.

When the Applicant accesses the video-identification system via the link provided in the email, SIGNICAT SLU will verify that the identification code provided corresponds to an identification request and, if correct, will allow the identification process to be initiated via the SIGNICAT SLU Application.

The identification process will obtain the necessary information to be included in the certificate, through the information included in the identity document used to carry out the identification process. If the identification process is correct and the identity of the Applicant is accredited, SIGNICAT SLU will approve the certificate request and proceed to issue the certificate in accordance with the provisions of this certification practice statement.

The documentation supporting the approval of the application must be kept and duly registered and with guarantees of security and integrity for a period of 15 years from the expiry of the certificate, even in the event of early loss of validity due to revocation.

4.1.2.2 Acceptance or Rejection of the Application

Once the identification process has been completed, the Applicant, within the Application environment, will wait for the Human Verification Agent to confirm and accredit their identity. If the identification process is correct and the Applicant's identity is accredited, the certificate issuance process will continue. At this point, and in order to continue with the certificate issuing process, the Applicant must expressly accept the general conditions of the electronic certification service for qualified short-term certificates and the Certification Practices Statement by ticking the checkboxes provided for this purpose. The ticking of these checkboxes by the Applicant shall be considered as a simple signature.

If the Applicant's identity is not accredited, the Applicant will be informed of this circumstance via the Application itself and, consequently, the accreditation of the identification process will be rejected and, therefore, it will not be possible to continue with the certificate issuance application process.

4.1.3 Issuance of the certificate

4.1.3.1 CA actions during the issuance procedure

Following the approval of the certification request by SIGNICAT SLU, the certificate is issued in a secure manner and is made available to the signatory for the purposes of its acceptance.

The procedures established in this section also apply in the event of renewal of certificates, since this involves the issuance of a new certificate.

During the procedure, SIGNICAT SLU must process a series of elements:

- Protect the confidentiality and integrity of the data to be recorded and made available to them.
- Use reliable systems and products that are protected against any alteration, guarantee the technical aspects and, where applicable, in addition the cryptographic security of the certification procedures for which they serve as a support.
- Generate the key pair through a certificate generation procedure securely linked to the key generation procedure.
- Use a certificate generation procedure that securely links the certificate to recorded information, including to the certified public key.
- Ensure that the certificate is issued by systems protected against falsification and modification, which guarantee the confidentiality of the keys during the process of generating the aforementioned keys.
- Indicate the date and time when a certificate has been issued.
- Guarantee the exclusive control of the keys by the user, SIGNICAT SLU or its Registration Authorities, they not being able to deduce them or use them in any way whatsoever.

4.1.4 Delivery and acceptance by way of certificate Use

In the short-term certificate issuance process, there is no specific delivery of the certificate to the Applicant, as it will be the Applicant itself who will use the certificate during the same process to electronically sign the documents, ending its validity with a single use and, in any case, within the maximum period established in the certificate, which shall not exceed 24 hours.

During this procedure, the operator or personnel authorized by the Registration Authority must perform the following actions:

- Definitively certify the identity of the natural person identified in the certificate, in accordance with the provisions of this document.
- Have the Trust Services Delivery Contract duly signed and accepted by electronic means by the Subscriber, as well as keeping all the Subscriber's traces regarding the affirmative manifestation in the corresponding checkboxes.
- Once the certificate has been issued and the documents electronically signed, deliver a document identifying the data of the certification service provider, the natural person subscribing the certificate, the identification data of the subscriber and signatory of the documents, the date and time, the documents electronically signed and the information relating to the events that have taken place during the certificate issuing process
- Issue the certificate delivery notice and acceptance sheet in due time to the natural person identified in the certificate, the minimum contents of which are as follows:

Acceptance of the certificate shall be carried out through its use.

4.1.5 Use of the Certificate: Use of Public and Private Keys

4.1.5.1 Use by the Subscriber

SIGNICAT SLU compels to do the following:

- To provide SIGNICAT SLU with complete and adequate information, in particular concerning the registration procedure.

- To give its consent prior to the issuance of a certificate.

- That all information provided by the signatory and contained in the certificate is correct.

- That the certificate is used exclusively for legal and other authorized purposes.

In order for the Applicant to use its electronic certificate and its public and private keys, SIGNICAT SLU shall carry out the following actions:

- REMOTE SIGNATURE: SHOWCASE 2

Once the identification process has been completed, the OTP has been entered by which, among other things, the user accepts the issuance of the certificate and the identity has been validated, the signatory's identity is guaranteed and the user is clearly presented with the following documents for the purposes of proceeding with the electronic signature:

o A viewer of the contract to be signed

o The call to action for the acceptance of this document

o A download option so that the user can save the document.

To continue the process, the user must view and accept the document, otherwise, he/she must be informed that the process is unable to continue.

For the acceptance of the document, the user is informed that a second SMS will be sent with a new OTP (6 digits) required to complete the signature, for which he/she will authorize SIGNICAT SLU as a qualified trusted service provider to apply the signature creation data of the User/Subscriber, thus guaranteeing its exclusive control.

The application will verify this information and if it is correct will proceed to issue the certificate and sign the document. The certificate is valid for 1 day and is used exclusively to sign the accepted document.

SIGNICAT SLU grants the SUBSCRIBER a non-exclusive, non-transferable license in order to use copies of eID's secure cryptographic device software for the operation of the signature device where applicable, as well as for the production of the electronic signature, certificate and other cryptographic services by the signatories.

The SUBSCRIBER may make copies of the software for archival or back-up purposes only.

In the event that any person other than SIGNICAT SLU makes modifications to the software supplied, all warranties with respect to the software shall be immediately cancelled.

- REMOTE SIGNATURE: SHOWCASE 3

The applicant accesses the application and the interface, prior to initiating the actions aimed at verifying the identity, asks the applicant to read and agree to the document relating to the terms and conditions of the service and to freely grant his/her consent to the processing of biometric data necessary to carry out the video identification.

- A viewer of the contract to be signed

- The call to action to accept this document.

- A download option so that the user can save/archive the document.

In the event that the applicant does not view the document and give this consent, the Process will not be able to continue.

Finally, prior to the start of the video-identification process, the user will be asked for a telephone number in order to send him/her an OTP.

By means of this OTP, the user will be authorizing the issue of the certificate, including in it any data extracted from the video-identification process, as well as the contractual document which was shown at the start of the process and on which the signature creation data will be applied by SIGNICAT SLU for the purpose of generating a qualified electronic signature.

Once the identification process has been completed and the identity has been validated by the verification agent, the signatory's identity will have been guaranteed and SIGNICAT SLU, as a qualified trust service provider, will apply the signature creation data of the user/subscriber to the document accepted at the start of the process by the USER (in accordance with Clause 3.1.1) on the document displayed and accepted through the introduction of the OTP, thus guaranteeing its exclusive control.

SIGNICAT SLU grants the SUBSCRIBER a non-exclusive, non-transferable license in order to use copies of eID's secure cryptographic device software for the operation of the signature device where applicable, as well as for the production of the electronic signature, certificate and other cryptographic services by the signatories.

The SUBSCRIBER may make copies of the software for archival or back-up purposes only.

In the event that any person other than SIGNICAT SLU makes modifications to the software supplied, all warranties with respect to the software shall be immediately cancelled.

4.1.5.2 Use by the third party entrusted with the certificate

SIGNICAT SLU informs the third party entrusted with the certificate that they must comply with the following obligations:

- Obtain independent advice on whether the certificate is appropriate for its intended use.
- Check the validity, suspension or revocation of certificates issued, using information relating to the status of certificates.
- Check all certificates in the certificate hierarchy before entrusting the digital signature or any of the hierarchy certificates to others.
- Recognize that verified electronic signatures, produced in a qualified signature creation device (QSCD) have the legal status of qualified electronic signatures; That is to say, equivalent to handwritten signatures, as well as the certificate allows the creation of other types of electronic signatures and encryption mechanism.
- Be aware of any limitation on the use of the certificate, regardless of whether it is included in the certificate itself or in the contract with the third party who trusts the certificate.
- Bear in mind any precaution stipulated in a contract or other instrument, regardless of its legal nature.
- Agree not to control, manipulate or perform reverse engineering activities relating to the technical implementation of SIGNICAT SLU certification services without prior written consent.

- Do not compromise the security of SIGNICAT SLU certification services.

4.1.6 Renewal of keys and certificates

N/A

4.1.7 Certificates modification

N/A

4.1.8 Revocation, suspension or reactivation of certificates

The revocation of a certificate entails the definitive loss of validity of this current one, which is irreversible.

The suspension (or temporary revocation) of a certificate entails the temporary loss of validity thereof, which is reversible. Only end-entity certificates can be suspended.

Reactivating a certificate causes it to go from the suspended state to the active state.

4.1.9 Causes of certificates revocation

SIGNICAT SLU revokes a certificate during the occurrence of one of the following reasons:

1) Circumstances affecting the information included in the certificate:

   a) Modification of any of the data included in the certificate following the corresponding issuance of the certificate containing the modifications.

   b) Where any of the data included in the certificate request is incorrect.

   c) Where any of the data included in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:

   a) Compromise of the private key, infrastructure or systems of the certification service provider which issued the certificate, where it affects the reliability of the certificates issued in the wake of this incident.

   b) Infringement, by SIGNICAT SLU, of the prerequisites set out in the certificate management procedures established in this Statement on Certification Practices.

   c) Compromise or suspicion of compromising the security of the key or certificate issued.

d) Unauthorized access or use of the private key corresponding to the public key contained in the certificate.

e) Irregular use of the certificate by the natural person identified with it, or lack of diligence in protecting the private key.

f) That is no longer compliant with the Certificate Practice Statement or Certificate Policy under which it has been issued.

3) Circumstances affecting the subscriber or the natural person identified in the certificate:

a) Termination of the legal service provision relationship between SIGNICAT SLU and the subscriber.

b) Modification or termination of the underlying legal relationship or cause leading to the issuance of the certificate to the natural person identified with the latter.

c) Breach by the applicant for the certificate of the pre-established prerequisites for the purposes of his request.

d) Breach of obligations, responsibilities and guarantees stipulated in the corresponding legal document by the subscriber or the person identified in the certificate.

e) Occurrence of incapacity or death of the owner of the keys.

f) Request for revocation of the certificate by the subscriber, in accordance with the provisions of section 3.4.

4) Other circumstances:

a) Termination of the certification service of the SIGNICAT SLU Certification Body.

b) Harmful and continuous use of the certificate for SIGNICAT SLU. In this instance, if use is considered harmful according to the following criteria:

- The nature and number of complaints filed.
- The identity of the bodies filing complaints.
- The relevant legislation in force at all times.
- The response of the subscriber or of the person identified in the certificate to complaints received.

4.1.10 Causes of suspension of a certificate

SIGNICAT SLU certificates may be suspended for the following reasons:

- When the subscriber or the natural person identified in the certificate so requests.

- When the documentation required during the revocation request is sufficient but the subscriber or the person identified in the certificate cannot be reasonably identified.
- Failure to use the certificate for an extended period, known beforehand.
- If the compromise of a key is suspected, until such time as it is confirmed. In this case, SIGNICAT SLU must ensure that the certificate is not suspended for longer than necessary in order to confirm this compromise.

4.1.11 Causes of reactivation of a certificate

SIGNICAT SLU certificates can be reactivated for the following reasons:

- When the certificate is in a state of suspension.
- When the subscriber or the person identified in the certificate requests it.

4.1.12 Who can request revocation, suspension or reactivation?

The revocation, suspension or reactivation of a certificate may be requested by:

- The person identified in the certificate.
- The subscriber of the certificate through the manager of the certification service.

4.1.13 Procedures for requesting revocation, suspension or reactivation

The entity needing to revoke, suspend or reactivate a certificate can request it directly from SIGNICAT SLU or the Subscriber's Registration Authority, or do so itself through the online service available on the SIGNICAT SLU Web page.

The request for revocation, suspension or reactivation must include the following information:

- Date of the request for revocation, suspension or reactivation.
- Subscriber’s identity.
- Name and status of the person requesting the revocation, suspension or reactivation.
- Contact information of the person requesting the revocation, suspension or reactivation.
- Detailed reasons in case of request for revocation.

The request must be authenticated by SIGNICAT SLU in accordance with the prerequisites stipulated in section 3.4 of this policy, before revoking, suspending or reactivating.

The revocation, suspension or reactivation service is available on the SIGNICAT SLU Web page at the following address: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures or in the following link.

In the event that the recipient of a request for revocation, suspension or reactivation from the natural person identified in the certificate is the subscribing entity, a request to this effect must be given to SIGNICAT SLU once the request has been authenticated.

The request for revocation, suspension or reactivation will be processed upon receipt, the subscriber will be informed of the change in status of the certificate and, where applicable, the natural person identified with the latter.

Both the revocation, suspension or reactivation management service and the consultation service are considered critical services, as noted in the contingency plan and the SIGNICAT SLU business continuity plan.

The entity requiring revocation, suspension, or reactivation of a certificate may request it through the following channels:

1. Directly by contacting SIGNICAT SLU. Users can submit a request via email, or send a written notice to the registered office of SIGNICAT SLU, as indicated in section 1.5 of this document.
2. Through the Subscriber's Registration Authority.
3. Independently via the online service available on the next link.

4.1.14 Temporary period of request for revocation, suspension or reactivation

Requests for revocation, suspension or reactivation will be immediately submitted as soon as they become known. In any case, requests shall be processed within 24 hours of receipt of the request.

In the event that, due to a technical or operational incident, the 24-hour deadline cannot be met, SIGNICAT SLU will log the request by assigning a unique case number, recording the date and time of receipt, and designating a responsible person for its follow-up.

4.1.15 Temporary deadline for processing the request for revocation, suspension or reactivation

The revocation, suspension or reactivation will occur immediately upon its receipt. In any case, requests shall be processed within 24 hours of receipt of the request.

In the event that, due to a technical or operational incident, the 24-hour deadline cannot be met, SIGNICAT SLU will log the request by assigning a unique case number, recording the date and time of receipt, and designating a responsible person for its follow-up.

4.1.16 Obligation to consult revocation information or suspension of certificates

Third parties should check the status of the certificates they want to trust.

One method by which the status of certificates can be checked is to consult the most recent Certificate Revocation List issued by the SIGNICAT SLU Certification Entity.

The Certificate Revocation Lists are published in the Certification Entity Directory, as well as the following Web addresses, as indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

The validity of certificates can also be checked through the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.1.17 Frequency of issuance of certificate revocation lists (CRL)

SIGNICAT SLU issues an CRL at least every 24 hours.

The CRL indicates when a new CRL is expected to be issued, although a CRL may be issued earlier than the timeframe specified in the previous CRL, to reflect the subsequent changes.

The CRL obligatorily maintains the revoked or suspended certificate until its expiry.

To ensure accuracy in the management of certificate revocation by the Certification Authority, the systems involved in the issuance and publication of Certificate Revocation Lists (CRLs) synchronize with UTC at least once a day.

4.1.18 Maximum deadline for publication of CRLs

CRLs are published on the Directory within an immediate but reasonable time following their generation which, in any case, is not more than a few minutes.

4.1.19 Availability of the online certificate status check service

In order to check the last CRL issued in each CA, it is necessary to download:

- *Primary Certification Authority (UANATACA ROOT 2016):*

- http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
- http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Intermediate Certification Authority 1 (ELECTRONIC IDENTIFICATION CA1):*

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

In the event of failure of the certificate status verification systems for causes not attributable to SIGNICAT SLU, the latter must strive to ensure that this service remains inactive for as little time as possible and, in any case, for no more than one day.

SIGNICAT SLU provides information to third parties who trust the certificates, relating to the operation of the certificate status information service.

One method by which the status of certificates can be checked is to consult the most recent Certificate Revocation List issued by the SIGNICAT SLU Certification Entity.

The Certificate Revocation Lists are published in the Certification Entity Directory, as well as at the following Web addresses, as indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

The validity of certificates can also be checked through the OCSP protocol.

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

4.1.20 Obligation to consult certificate status verification services

It is mandatory to consult the status of certificates before being able to trust them.

Third parties should verify the status and force of the certificates they wish to trust, using one of the aforementioned verification methods in the previous paragraph (CRL or OCSP).

4.1.21 Special prerequisites in case of compromise of the private key

The compromise of the SIGNICAT SLU private key is notified to all participants in the certification services, to the extent possible, by posting this fact on the SIGNICAT SLU Web page, as well as, if necessary, on other means of communication, even in paper form.

4.1.22 Maximum period of the state of suspension of a digital certificate

The maximum period of a suspended digital certificate shall be ninety (90) days from the request for suspension by the SUBSCRIBER or SIGNATORY. After the maximum period without being reactivated, SIGNICAT SLU will proceed to its revocation directly.

If during the period of suspension, the digital certificate expires or its revocation is requested, its validity will expire under the same conditions as a valid digital certificate.

Without prejudice to the foregoing, the maximum period of ninety (90) days may be altered depending on an investigation procedure by SIGNICAT SLU or ongoing judicial or administrative procedure. In these cases, the digital certificate will be suspended for the required period, and, after that, it will be definitively revoked. In no case may the period of suspension of the digital certificate exceed the period of validity of this.

4.1.23 Subscription termination

Once the certificate's validity period has expired, the subscription to the service will end.

4.2 4.2. Long-term certificates

4.2.1 Request for long-term certificates issuance

4.2.1.1 Legitimization in order to request the issuance

The Certificate applicant must sign a contract with SIGNICAT SLU for the provision of certification services.

Likewise, prior to the issuance and delivery of a certificate, the request for it must exist in the contract itself, either in a specific certificate request sheet document or with the registration authority.

If the applicant is a person distinct from the subscriber, an authorization from the latter must ensue in order for the applicant to carry out the request, by performing it on a certificate request sheet subscribed to by the applicant in his own name in instances of natural person certificates.

4.2.2 Processing of the certification request

4.2.2.1 Carrying out and completing identification and authentication functions

Once the certificate request is received, SIGNICAT SLU ensures that the certificate requests are complete, accurate and duly authorized before processing them.

If it can be processed, SIGNICAT SLU verifies the facilitated information by checking the points described in section 3.2.

In the event of a qualified certificate, the documentation justifying the approval of the request must be kept and duly recorded, provided with guarantees of security and integrity for a period of 15 years from the expiration of the certificate, or even in the case of anticipated loss of effect due to revocation. Approval or refusal of the request may be then granted.

4.2.2.2 Approval or rejection of the request

If the data is correctly verified, SIGNICAT SLU must approve the certificate request, issue it and hand it over.

If the verification indicates that the information is not correct, or if it is suspected of not being correct, or could otherwise damage the reputation of the Certification Authority, Registration Authorities or subscribers, SIGNICAT SLU has the right to refuse the request or withhold its approval until completion of the additional verifications deemed relevant.

If the additional verifications do not reflect the correctness of the information to be verified, the request will be definitively refused.

SIGNICAT SLU will notify the approval or denial of the request to the applicant.

SIGNICAT SLU will be able to automate the procedures for verifying the correctness of the information which will be included in the certificates, as well as for the approval of requests.

4.2.2.3 Deadline for processing the request

SIGNICAT SLU processes certificate requests in their order of arrival and within a reasonable time frame, a maximum time guarantee that may be specified in the certificate delivery contract.

Requests remain active until their approval or refusal has been declared.

4.2.3 Issuance of the certificate

4.2.3.1 CA actions during the issuance procedure

Following the approval of the certification request, the certificate is issued in a secure manner and is made available to the signatory for the purposes of its acceptance.

The procedures established in this section also apply in the event of renewal of certificates, since this involves the issuance of a new certificate.

During the procedure, SIGNICAT SLU must process a series of elements:

- Protect the confidentiality and integrity of the data to be recorded and made available to them.

- Use reliable systems and products that are protected against any alteration, guarantee the technical aspects and, where applicable, in addition the cryptographic security of the certification procedures for which they serve as a support.
- Generate the key pair through a certificate generation procedure securely linked to the key generation procedure.
- Use a certificate generation procedure that securely links the certificate to recorded information, including to the certified public key.
- Ensure that the certificate is issued by systems protected against falsification, which guarantee the confidentiality of the keys during the process of generating the aforementioned keys.
- Indicate the date and time when a certificate has been issued.
- Guarantee the exclusive control of the keys by the user, SIGNICAT SLU or its Registration Authorities, they not being able to deduce them or use them in any way whatsoever.

4.2.3.2 Notification of issuance to the subscriber

SIGNICAT SLU notifies the issuance of the certificate to the subscriber and / or to the natural person identified in the certificate, as well as the generation / download method.

4.2.4 Delivery and acceptance of the certificate

4.2.4.1 CAs responsibilities

During this procedure, the operator or personnel authorized by the Registration Authority must perform the following actions:

- Definitively certify the identity of the natural person identified in the certificate, in accordance with the provisions of this document.
- Have the Trust Services Delivery Contract duly signed and accepted by the Subscriber through electronic means.
- To deliver, when applicable, depending on the type of certificate issued, the delivery and acceptance sheet of the certificate to the natural person identified in the certificate, with the following minimum contents:

- Basic information relating to the use of the certificate, including, in particular, information relating to the certification service provider and the applicable Statement on Certification Practices, as well as its obligations, powers and responsibilities.
- Information relating to the certificate.
- Acknowledgement of receipt of the certificate by the signatory and / or of the mechanisms used for the purposes of its generation / downloading, as well as acceptance of the aforementioned elements.
- Summary of the signatory's obligations.
- Signatory's responsibility.
- Exclusive signatory attribution method, including his private key and his certificate activation data.
- Delivery and receipt date.

All of this information can be included in the Trust Services Provision Contract itself. That said, when the Subscriber signs the Trust Services Provision Contract, delivery and acceptance of the certificate will then be considered complete.

- Obtain the signature of the person identified in the certificate.

The Registration Authorities are responsible for carrying out these procedures, and must record previous minutes in a documentary manner and keep the original documents mentioned (remittance and acceptance sheets), supplying an electronic copy to SIGNICAT SLU, as well as the originals if SIGNICAT SLU needs to have access to these.

4.2.4.2 Behavior constituting acceptance of the certificate

When the acceptance sheet is delivered, acknowledgement of the certificate by the natural person identified in the certificate ensues by signing the delivery and acceptance sheet.

When the generation and delivery of the certificate takes place at the same time in accordance with the procedures defined by SIGNICAT SLU, the acceptance of the certificate by the natural person identified in the certificate is deemed to take place through the signing of the Contract for the Provision of Trust Services.

4.2.4.3 Publication of the certificate by the CA

Once the Certificate has been generated by the Certification Services Provider, it will be published in the Directory, specifically in the input field corresponding to the distinctive name of the Subscriber, as defined in the "Certificate issuance" paragraph of this appendix.

If the Applicant has provided an email address during the request procedure, a communication relating to the disposal of his Certificate for its use will be sent to him.

4.2.4.4 Notification of delivery to third parties

SIGNICAT SLU does not make any notification of the issuance to third parties.

4.2.5 Use of the keys pair and certificate

4.2.5.1 Use by the subscriber

SIGNICAT SLU contractually obliges the subscriber to:

- Facilitate complete and adequate information to the Certification Authority, in accordance with the prerequisites of this Statement on Certification Practices and, in particular, with regard to the registration procedure.
- Express his consent prior to the issuance and delivery of a certificate.
- Communicate to SIGNICAT SLU, to the Registration Authorities and to any person that the Subscriber believes he can entrust with the certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his private key.
    - The loss of control of his private key due to the compromise of the activation data (for example, the PIN code) or any other cause.
    - Inaccuracies or modifications made to the content of the certificate, known or possibly made known to the subscriber.
    - The loss, alteration, unauthorized use, theft or compromise, where applicable, of the card.
- Communicate the compliance with their specific obligations to the natural persons identified in the certificate, and establish mechanisms to guarantee effective compliance with these obligations.
- Not to control, manipulate or perform reverse engineering acts relating to the technical implementation of the certification services of ELECTRONIC IDENTIFICATION, S.L, without its prior written consent.
- The subscriber, as the holder of the certificate, cannot transfer its use to third parties.

- Do not compromise the security of the certification services of the SIGNICAT SLU certification service provider.

4.2.5.2 Use by the third party entrusted with the certificate

SIGNICAT SLU informs the third party entrusted with the certificate that they must comply with the following obligations:

- Obtain independent advice on whether the certificate is appropriate for its intended use.
- Check the validity, suspension or revocation of certificates issued, using information relating to the status of certificates.
- Check all certificates in the certificate hierarchy before entrusting the digital signature or any of the hierarchy certificates to others.
- Recognize that verified electronic signatures, produced in a qualified signature creation device (QSCD) have the legal status of qualified electronic signatures; That is to say, equivalent to handwritten signatures, as well as the certificate allows the creation of other types of electronic signatures and encryption mechanism.
- Be aware of any limitation on the use of the certificate, regardless of whether it is included in the certificate itself or in the contract with the third party who trusts the certificate.
- Bear in mind any precaution stipulated in a contract or other instrument, regardless of its legal nature.
- Agree not to control, manipulate or perform reverse engineering activities relating to the technical implementation of SIGNICAT SLU certification services without prior written consent.
- Do not compromise the security of SIGNICAT SLU certification services.

4.2.6 Renewal of keys and certificates

Short-term certificates cannot be renewed.

4.2.7 Certificates modification

The modification of certificates, subject to the modification of the certified public key, which is deemed a renewal, will be treated as a new issuance of the certificate, and the provisions of sections 4.1, 4.2, 4.3 and 4.4. will then become applicable.

4.2.8 Revocation, suspension or reactivation of certificates

The revocation of a certificate entails the definitive loss of validity of this current one, which is irreversible.

The suspension (or temporary revocation) of a certificate entails the temporary loss of validity thereof, which is reversible. Only end-entity certificates can be suspended.

Reactivating a certificate causes it to go from the suspended state to the active state.

4.2.8.1 Causes of certificates revocation

SIGNICAT SLU revokes a certificate during the occurrence of one of the following reasons:

1) Circumstances affecting the information included in the certificate:

   a) Modification of any of the data included in the certificate following the corresponding issuance of the certificate containing the modifications.

   b) Where any of the data included in the certificate request is incorrect.

   c) Where any of the data included in the certificate is incorrect.

2) Circumstances affecting the security of the key or certificate:

   a) Compromise of the private key, infrastructure or systems of the certification service provider which issued the certificate, where it affects the reliability of the certificates issued in the wake of this incident.

   b) Infringement, by SIGNICAT SLU, of the prerequisites set out in the certificate management procedures established in this Statement on Certification Practices.

   c) Compromise or suspicion of compromising the security of the key or certificate issued.

   d) Unauthorized access or use of the private key corresponding to the public key contained in the certificate.

   e) Irregular use of the certificate by the natural person identified with it, or lack of diligence in protecting the private key.

   f) That is no longer compliant with the Certificate Practice Statement or Certificate Policy under which it has been issued.

3) Circumstances affecting the subscriber or the natural person identified in the certificate:

a) Termination of the legal service provision relationship between SIGNICAT SLU and the subscriber.

b) Modification or termination of the underlying legal relationship or cause leading to the issuance of the certificate to the natural person identified with the latter.

c) Breach by the applicant for the certificate of the pre-established prerequisites for the purposes of his request.

d) Breach of obligations, responsibilities and guarantees stipulated in the corresponding legal document by the subscriber or the person identified in the certificate.

e) Occurrence of incapacity or death of the owner of the keys.

f) Request for revocation of the certificate by the subscriber, in accordance with the provisions of section 3.4.

4) Other circumstances:

a) Termination of the certification service of the SIGNICAT SLU Certification Body.

b) Harmful and continuous use of the certificate for SIGNICAT SLU. In this instance, if use is considered harmful according to the following criteria:

- The nature and number of complaints filed.
- The identity of the bodies filing complaints.
- The relevant legislation in force at all times.
- The response of the subscriber or of the person identified in the certificate to complaints received.

4.2.8.2 Causes of suspension of a certificate

SIGNICAT SLU certificates may be suspended for the following reasons:

- When the subscriber or the natural person identified in the certificate so requests.
- When the documentation required during the revocation request is sufficient but the subscriber or the person identified in the certificate cannot be reasonably identified.
- Failure to use the certificate for an extended period, known beforehand.
- If the compromise of a key is suspected, until such time as it is confirmed. In this case, SIGNICAT SLU must ensure that the certificate is not suspended for longer than necessary in order to confirm this compromise.

4.2.8.3 Causes of reactivation of a certificate

SIGNICAT SLU certificates can be reactivated for the following reasons:

- When the certificate is in a state of suspension.
- When the subscriber or the person identified in the certificate requests it.

4.2.8.4 Who can request revocation, suspension or reactivation?

The revocation, suspension or reactivation of a certificate may be requested by:

- The person identified in the certificate.
- The subscriber of the certificate through the manager of the certification service.

4.2.8.5 Procedures for requesting revocation, suspension or reactivation

The entity needing to revoke, suspend or reactivate a certificate can request it directly from SIGNICAT SLU or the Subscriber's Registration Authority, or do so itself through the online service available on the SIGNICAT SLU Web page.

The request for revocation, suspension or reactivation must include the following information:

- Date of the request for revocation, suspension or reactivation.
- Subscriber's identity.
- Name and status of the person requesting the revocation, suspension or reactivation.
- Contact information of the person requesting the revocation, suspension or reactivation.
- Detailed reasons in case of request for revocation.

The request must be authenticated by SIGNICAT SLU in accordance with the prerequisites stipulated in section 3.4 of this policy, before revoking, suspending or reactivating.

The revocation, suspension or reactivation service is available on the SIGNICAT SLU Web page at the following address: https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

In the event that the recipient of a request for revocation, suspension or reactivation from the natural person identified in the certificate is the subscribing entity, a request to this effect must be given to SIGNICAT SLU once the request has been authenticated.

The request for revocation, suspension or reactivation will be processed upon receipt, the subscriber will be informed of the change in status of the certificate and, where applicable, the natural person identified with the latter.

Both the revocation, suspension or reactivation management service and the consultation service are considered critical services, as noted in the contingency plan and the SIGNICAT SLU business continuity plan.

The entity requiring revocation, suspension, or reactivation of a certificate may request it through the following channels:

1. Directly by contacting SIGNICAT SLU. Users can submit a request via email, or send a written notice to the registered office of SIGNICAT SLU, as indicated in section 1.5 of this document.
2. Through the Subscriber's Registration Authority.
3. Independently via the online service available on the next link.

4.2.8.6 Temporary period of request for revocation, suspension or reactivation

Requests for revocation, suspension or reactivation will be immediately submitted as soon as they become known. In any case, requests shall be processed within 24 hours of receipt of the request.

In the event that, due to a technical or operational incident, the 24-hour deadline cannot be met, SIGNICAT SLU will log the request by assigning a unique case number, recording the date and time of receipt, and designating a responsible person for its follow-up.

4.2.8.7 Temporary deadline for processing the request for revocation, suspension or reactivation

The revocation, suspension or reactivation will occur immediately upon its receipt. In any case, requests shall be processed within 24 hours of receipt of the request.

In the event that, due to a technical or operational incident, the 24-hour deadline cannot be met, SIGNICAT SLU will log the request by assigning a unique case number, recording the date and time of receipt, and designating a responsible person for its follow-up.

4.2.8.8 Obligation to consult revocation information or suspension of certificates

Third parties should check the status of the certificates they want to trust.

One method by which the status of certificates can be checked is to consult the most recent Certificate Revocation List issued by the SIGNICAT SLU Certification Entity.

The Certificate Revocation Lists are published in the Certification Entity Directory, as well as the following Web addresses, as indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

The validity of certificates can also be checked through the OCSP protocol.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.2.8.9 Frequency of issuance of certificate revocation lists (CRL)

SIGNICAT SLU issues an CRL at least every 24 hours.

The CRL indicates when a new CRL is expected to be issued, although a CRL may be issued earlier than the timeframe specified in the previous CRL, to reflect the subsequent changes.

The CRL obligatorily maintains the revoked or suspended certificate until its expiry.

To ensure accuracy in the management of certificate revocation by the Certification Authority, the systems involved in the issuance and publication of Certificate Revocation Lists (CRLs) synchronize with UTC at least once a day.

4.2.8.10 Maximum deadline for publication of CRLs

CRLs are published on the Directory within an immediate but reasonable time following their generation which, in any case, is not more than a few minutes.

4.2.8.11 Availability of the online certificate status check service

In order to check the last CRL issued in each CA, it is necessary to download:

- *Primary Certification Authority (UANATACA ROOT 2016):*

- http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
- http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Intermediate Certification Authority 1 (ELECTRONIC IDENTIFICATION CA1):*

- http://crl1.uanataca.com/public/pki/crl/EID.crl
- http://crl2.uanataca.com/public/pki/crl/EID.crl

In the event of failure of the certificate status verification systems for causes not attributable to SIGNICAT SLU, the latter must strive to ensure that this service remains inactive for as little time as possible and, for no more than one day.

SIGNICAT SLU provides information to third parties who trust the certificates, relating to the operation of the certificate status information service.

One method by which the status of certificates can be checked is to consult the most recent Certificate Revocation List issued by the SIGNICAT SLU Certification Entity.

The Certificate Revocation Lists are published in the Certification Entity Directory, as well as at the following Web addresses, as indicated in the certificates:

- http://crl1.uanataca.com/public/pki/crl/EID.crl

- http://crl2.uanataca.com/public/pki/crl/EID.crl

The validity of certificates can also be checked through the OCSP protocol.

http://ocsp1.uanataca.com/public/pki/ocsp/

http://ocsp2.uanataca.com/public/pki/ocsp/

4.2.8.12 Obligation to consult certificate status verification services

It is mandatory to consult the status of certificates before being able to trust them.

Third parties should verify the status and force of the certificates they wish to trust, using one of the aforementioned verification methods in the previous paragraph (CRL or OCSP).

4.2.8.13 Special prerequisites in case of compromise of the private key

The compromise of the SIGNICAT SLU private key is notified to all participants in the certification services, to the extent possible, by posting this fact on the SIGNICAT SLU Web page, as well as, if necessary, on other means of communication, even in paper form.

4.2.8.14 Maximum period of the state of suspension of a digital certificate

The maximum period of a suspended digital certificate shall be ninety (90) days from the request for suspension by the SUBSCRIBER or SIGNATORY. After the maximum period without being reactivated, SIGNICAT SLU will proceed to its revocation directly.

If during the period of suspension, the digital certificate expires or its revocation is requested, its validity will expire under the same conditions as a valid digital certificate.

Without prejudice to the foregoing, the maximum period of ninety (90) days may be altered depending on an investigation procedure by SIGNICAT SLU or ongoing judicial or administrative procedure. In these cases, the digital certificate will be suspended for the required period, and, after that, it will be definitively revoked. In no case may the period of suspension of the digital certificate exceed the period of validity of this.

4.2.9 Subscription termination

Once the certificate's validity period has expired, the subscription to the service will end.

As an exception, the subscriber may keep the service in force by requesting the renewal of the certificate, within the prior period set in this Statement on Certification Practices.

SIGNICAT SLU may issue a new certificate of office, provided that the subscribers maintain its status.

4.2.10 Deposit and retrieval of keys

4.2.10.1 Key deposit and retrieval policy and practices

SIGNICAT SLU only stores the keys of certificates issued in the cloud profiles. These keys are non-exportable and remain under the exclusive control of the certificate holder.

SIGNICAT SLU does not provide private key recovery services.

4.2.10.2 Policy and practices relating to encapsulation and retrieval of session keys

Without stipulation.

5 Physical, managerial and operational security controls

5.1 The infrastructure and equipment supporting the video identification service.

The infrastructure and equipment that supports the video-identification service is located in protected rooms with restricted access, where access shall only be possible through the planned and monitored entrances and all personnel accessing these rooms shall be identified, with entries and exits being recorded. SIGNICAT SLU ensures that the requirements set out in Chapter V of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 are complied with.

If external infrastructure providers are used, only those that comply with these controls will be authorized.

5.2 Physical security controls

SIGNICAT SLU, by means of the public key infrastructure of UANATACA, SA provides its certification services and has established physical and environmental security controls in order to protect the resources of the facilities where the systems, own individual systems and equipment are located when used in the provision of electronic trust services.

Concretely, the security policy applicable to electronic trust services provides the following:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (electronic energy, telecommunications, etc.)
- Collapse of the structure.
- Floods.
- Anti-theft protection.
- Unauthorized release of equipment, information, media and applications relating to components used by the services of the certification service provider.

These measures are applicable to the facilities from which the electronic trust services are provided, to their production and contingency environments, which are periodically audited in accordance with the applicable regulations and the policies dedicated to these ends.

Facilities rely on preventive and corrective maintenance systems with 24/365 assistance within 24 hours of the launch of an alerting.

5.2.1 Location and construction of facilities

Physical protection through the creation of clearly defined security perimeters around the services. The quality and solidity of the construction materials of the facilities ensure adequate levels of protection against forcible intrusions, and they are located in an area of low disaster risk and which allow rapid access.

The infrastructure of the room where cryptographic operations are carried out within the Data Processing Center is redundant and relies on several alternative sources of electricity and refrigeration in case of emergency.

We have facilities that physically protect the provision of approval services from certificate requests and management of revocations, and compromise which results from unauthorized access to systems or data, as well as from their disclosure.

5.2.2 Physical access

We have three levels of physical security (Entrance to the Building where the CPD is located, access to the CPD room and access to the Rack) in order to protect the certificate generation service, with access being achieved from the levels below to the upper levels.

Physical access to outbuildings where certification procedures are carried out is restricted and protected through a combination of physical and procedural measures. Therefore:

- It is limited to expressly authorized personnel, with identification at the time of access and recording thereof, including filming on closed circuit television and its archiving.
- Access to the rooms is achieved through identification card readers and is managed by a computer system that maintains an automatic history of entries and exits.
- Regarding access to the rack where cryptographic procedures take place, it is necessary firstly to authorize the administrators of the hosting service who have the key in order to open the cage.

5.2.3 Electricity and air conditioning

The facilities have current stabilizing equipment and a system of dual power supply to the equipment through a generator.

The rooms where the computer equipment is located have temperature control systems, with air conditioning equipment.

5.2.4 Exposure to water

The facilities are located in an area with a low risk of flooding.

The rooms where the computer equipment is located have a humidity detection system.

5.2.5 Fire prevention and protection

Facilities and assets rely on automatic fire detection and extinguishing systems.

5.2.6 Storage of supports

Only authorized personnel have access to storage means.

The information with the highest level of classification is kept in a safe, outside the facilities of the Data Processing Center.

5.2.7 Waste processing

The elimination of supports, both paper and magnetic, is carried out by means of mechanisms ensuring the impossibility of retrieving the information.

Magnetic supports are discarded, physically destroyed, or reused through a permanent elimination or formatting process. The paper documentation is destroyed using a shredder or bins arranged for this purpose in order to be subsequently destroyed under controlled conditions.

5.2.8 Backup copy outside the facilities

We use an external and secure warehouse to protect documents, magnetic and electronic devices, which are independent from the operation center.

5.3 Procedures controls

SIGNICAT SLU guarantees that its systems are operated in a safe manner, for the purposes of which it has established and implemented procedures relating to the functions which affect the provision of its services.

Staff working for SIGNICAT SLU performs administrative and management procedural functions in accordance with the security policy.

5.3.1 Reliable functions

In accordance with the security policy, the following reliable functions or roles have been identified:

- **Internal Auditor:** Responsible for compliance with operational procedures. This is an external person in the Information Systems department. The tasks of the Internal Auditor are incompatible in time with the tasks of Certification and Systems. These

functions are subordinated to the operational authority, to which he reports, as well as to the technical direction.

- **Systems Manager:** Responsible for the correct functioning of Hardware and software to support of the certification platform.

- **CA Administrator**: Responsible for the actions to be carried out with the cryptographic material, or the performance of a function involving the activation of the private keys of the certification authorities as described in this document, or any of its elements.

- **CA Operator**: Responsible with the CA Administrator for the protection of the cryptographic key activation material, also responsible for the backup copy operations and maintenance of the CA.

- **Registration Operator**: Person responsible for approving certification requests made by the subscriber and issuing digital certificates.

- **Qualified Worker for Revocation**: Person responsible for making changes to the status of certificates, mainly suspending and revoking them.

- **Security Manager**: Responsible for coordinating, controlling and enforcing the security measures defined in the security policies. He / she must be responsible for aspects relating to information security: logical, physical, networks, organizational matters, etc.

The persons performing the aforementioned functions are subject to specific investigation and checking procedures. In addition, criteria and procedures are implemented in order to segregate functions, as a measure for prevention of fraudulent activities.

5.3.2 Number of persons per task

At least two people are required to perform the tasks relating to the generation, recovery and backup copy production of the private key of the Certification Authorities. The same criterion is applied to carrying out of the tasks of issuing and activating the certificates and private keys of the Certification Authorities and, in general, of any handling of the key protection device of the primary and intermediate Certification Authority.

5.3.3 Identification and authentication of each function

The people assigned to each role are identified by the internal auditor who will ensure that each of them in turn performs the operations which have been assigned to them.

Each person controls only the assets necessary for their role, ensuring that no one can access unassigned resources.

Access to resources is based on the asset, by means of user / password, digital certificate, physical access card and / or keys.

5.3.4 Roles that require segregation of tasks

The following tasks are performed by at least two persons:

- The tasks specific to the role of Auditor are incompatible with the operation and administration of systems and, in general, with those associated with the direct provision of electronic trust services.

- The issuance and revocation of certificates are tasks which are incompatible with the administration and operation of systems.

- The administration and operation of the systems, as well as the CAs, are incompatible with each other.

5.3.5 PKI management system

The PKI system consists of the following modules:

- Certification Authority Module. The CA is designed as a two-tier solution, consisting of a Primary CA and one or more Subordinate CAs (Sub CA, thereafter). The Primary CA issues certificates for the Sub CAs, while the latter issue certificates for end entities such as services, companies, users or time stamping services.

- Registration Authority Module. EA is the certificate lifecycle management application. This application allows the operator to manage the complete life cycle of the certificate.

- Validation Authority Module. The Validation Authority is the application that provides the OCSP online certificate validation service.

- Requests management module. Department responsible for processing and redirecting all requests and requests associated with the Provision of Trust Services, with the rest of the components that are part of the Public Key Infrastructure.

- Key management module (HSM). The HSM is responsible for storing the master key used for the purposes of managing all key pairs created by the system. It also performs cryptographic operations with these keys.

All keys used across the platform comply with the ENS regulation and the CCN-STIC-807 guide about cryptography. These keys will be symmetric and with a specificity of SYMMETRIC_DEFAULT.

The default key spec, SYMMETRIC_DEFAULT, is the key spec for symmetric CMKs. When you select the **Symmetric key type in the AWS KMS console, it selects the SYMMETRIC_DEFAULT key spec. In the* CreateKey *operation, if you don't specify a CustomerMasterKeySpec value, SYMMETRIC_DEFAULT is selected. If you don't have a reason to use a different key spec, SYMMETRIC_DEFAULT is a good choice.*

The encryption algorithm for symmetric CMKs is also known as SYMMETRIC_DEFAULT. Currently, this represents a symmetric algorithm based on Advanced Encryption Standard (AES) in Galois Counter Mode *(GCM) with 256-bit keys, an industry standard for secure encryption. The ciphertext that this algorithm generates supports additional*

authenticated data (AAD), such as an encryption context*, and GCM provides an additional integrity check on the ciphertext. For technical details, see* AWS Key Management Service Cryptographic Details.

Data encrypted under AES-256-GCM is protected now and in the future. Cryptographers consider this algorithm to be quantum resistant*. Theoretical future, large-scale quantum computing attacks on ciphertexts created under 256-bit AES-GCM keys* reduce the effective security of the key to 128 bits*. But this security level is sufficient to make brute force attacks on AWS KMS ciphertexts infeasible.*

You can use a symmetric CMK in AWS KMS to encrypt, decrypt, and re-encrypt data, and generate data keys and data key pairs. AWS services that are integrated with AWS KMS use symmetric CMKs to encrypt your data at rest. You can import your own key material *into a symmetric CMK and create symmetric CMKs* in custom key stores.

- Database module. The component responsible for the Database compiles and stores all the information facilitated by the whole infrastructure.

5.4 Personnel controls

5.4.1 Prerequisites in terms of history, qualifications, experience and authorization

All personnel are qualified and / or have been suitably trained to carry out the operations assigned to them.

Staff performing trust functions must not have personal interests which conflict with the development of the task entrusted to them.

SIGNICAT SLU ensures that registration personnel are confident in performing registration tasks. The Registration Administrator receives training to perform the requests validation tasks.

In general, an employee will cease to exercise his functions of trust in the event of awareness or knowledge of the existence of a conflict of interest and / or the commission of any tort whatsoever that could interfere with the performance of his functions.

A person who is not suitable for the position will not be assigned to a position of trust or management, especially because of a fault that harms her adequacy for the purposes of the function. For this reason, an investigation is carried out in advance to the extent permitted by law, relating to the following aspects:

- Studies, including alleged diplomas.
- Previous jobs (up to n-5), including professional references.
- Professional references.

In any case, the Registration Authorities will be able to establish different procedures for background checks, while preserving SIGNICAT SLU policies and being responsible for the intervention of the persons they authorize in their operations.

5.4.2 History verification procedures

Before hiring a person or allowing them to occupy their workstation, the following checks are carried out:

- References on jobs from previous years
- Professional references
- Studies, including alleged diplomas.

SIGNICAT SLU obtains the unequivocal consent of the person concerned by this preliminary investigation, processes and protects all their personal data in accordance with the regulations in force in terms of protection of personal data, contained in European Regulation n° 2016/679 General Data Protection and, in general, to any applicable national regulations.

All checks are carried out to the extent permitted by the applicable legislation in force. The reasons which may give rise to the refusal of the candidate for a position of trust are as follows:

- Counterfeit documents provided in the search for employment, carried out by the candidate.
- Very negative or very unreliable professional references with regard to the candidate.

5.4.3 Training prerequisites

SIGNICAT SLU trains staff in positions of trust and management until they achieve the necessary qualification, records of this training being archived.

Training programs are periodically reviewed, updated and improved.

The training includes the following contents as a minimum:

- Security principles and mechanisms of the certification hierarchy, as well as the user environment of the person to be trained.
- Tasks that the person must perform.
- Security policies and procedures. Use and operation of installed machines and applications.
- Management and processing of security incidents and compromises.
- Business continuity and emergency procedures.

- Management and security procedure with regard to the processing of personal data.

SIGNICAT SLU guarantees that the verification of documents and verification of identity are carried out by personnel duly trained for these purposes.

5.4.4 Prerequisites and frequency of formative updating

SIGNICAT SLU updates staff training in accordance with existing needs and with sufficient frequency to perform their duties competently and satisfactorily, especially when there are substantial changes to certification tasks.

5.4.5 Sequence and frequency of staff turnover

Not applicable.

5.4.6 Sanctions for unauthorized actions

SIGNICAT SLU has a sanctioning system in order to purify the responsibilities derived from unauthorized actions, in accordance with the applicable labor legislation.

Disciplinary actions include the suspension, separation of duties, or even dismissal of the person responsible for the harmful action, in a manner proportionate to the seriousness of the unauthorized action.

5.4.7 Prerequisites for hiring professionals

Employees hired to perform trust functions first sign the confidentiality clauses and operational prerequisites used by SIGNICAT SLU. Any action that compromises the security of the accepted procedures may result in the termination of the employment contract upon assessment.

In the event that all or part of the certification services are operated by a third party, the controls and forecasts carried out in this section, or other parts of the Statement on Certification Practices, will be applied and respected by the third party performing the operational functions of certification services, notwithstanding, the certification entity will be responsible for the actual execution in any case. These aspects are stipulated in the legal instrument used to entrust the provision of certification services to a third party separate from SIGNICAT SLU.

5.4.8 Provision of documentation to staff

The certification services provider will provide the documentation that its staff strictly need at all times in order to perform their work competently and satisfactorily.

5.5 Security audit procedures

5.5.1 Types of events recorded

The following events, relating to the security of the entity, are likely to occur and are to be recorded:

- System start-up and shutdown.
- Attempts to create, delete, establish passwords or modify privileges.

- Connection and disconnection attempts.
- Unauthorized access attempts to the CA system through the network.
- Unauthorized access attempts to the archive system.
- Physical access to histories.
- System configuration changes and maintenance.
- CA applications registrations.
- CA application starting and shutdown.
- Changes to the details of the CA and / or its keys.
- Changes in the creation of certificate policies.
- Generation of own keys.
- Creation and renewal of certificates.
- Records of destruction of means containing keys and activation data.
- Events relating to the life cycle of the cryptographic module such as receipt, use and uninstallation of the latter.
- Key generation ceremony and key management databases.
- Physical access records.
- Maintenance and modification of the system configuration.
- Staff changes.
- Compromise reports and disputes.
- Records of the destruction of equipment containing information relating to keys, activation data or personal information of the subscriber, in the case of individual certificates, or of the natural person identified in the certificate, in the case of corporate certificates.
- Possession of activation data for the purposes of operations using the private key of the Certification Entity.
- Complete reports of physical intrusion attempts in infrastructure in support of the issuance and management of certificates.
- Events related to outages of the services provided through the Public Key Infrastructure used by SIGNICAT SLU for the provision of services.

- Events related to the malfunction of equipment used by SIGNICAT SLU in connection with the provision of trust services.
- Events related to firewalls associated with the Public Key Infrastructure.
- Events related to time synchronization, as well as any loss thereof, concerning the trusted time sources used to provide timestamps in the records related to the Public Key Infrastructure used by SIGNICAT SLU for the provision of its services.

Entries on the registers include the following:

- Date and time of the entry.
- Serial number or sequence of entry into automatic registers.
- Identity of the person entering the register.
- Type of entry.

5.5.2 Frequency of processing of audit logs

The logs are revised in the event of a system alert motivated by the existence of any incident.

The processing of the audit logs consists of a review of the logs including checking for non-handling, a brief search of all entries on the log and a more thorough investigation of any alerts or irregularities contained in the logs. The actions carried out following the audit review are documented.

We maintain a system that guarantees:

- Sufficient space to store logs.
- That files cannot be overwritten.
- That the protected information includes at least: type of event, date and time, user who executes the event and result of the operation.
- Logs files will be stored in structured files, which may incorporate a BBDD for the purposes of their subsequent examination.

5.5.3 Retention period for audit records

Historical information is stored for a period of 1 to 15 years, depending on the type of information recorded.

Likewise, the audit logs related to the management of the digital certificates' lifecycle shall be retained for a minimum period of seven (7) years from the expiration of the certificate or the termination of the service provided, in accordance with the applicable regulations.

5.5.4 Protection of audit records

System histories:

- Are protected against manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Their availability is protected by means of their storage in facilities external to the center where the CA is located.

Access to the history files is exclusively reserved for authorized persons. Likewise, the devices are handled at all times by authorized personnel.

There is an internal procedure which details all the management processes of the devices containing the data of the audit history.

5.5.5 Backup copy procedure

We have an adequate backup copy procedure so that, in the event of loss or destruction of relevant files, the corresponding backup copies of the logs are available at short notice.

A safe backup copy procedure for audit logs is implemented, making a copy of all logs once a week in an external support file. In addition, a copy is kept in an external protection center.

5.5.6 Location of the audit log accumulation system

Information from the audit of events is collected internally and automatically by the operating system, network communications and certificate management software, in addition to manually generated data, which will be stored by duly authorized personnel. The whole represents the system of accumulation of audit records.

5.5.7 Notification of an audit event to its manager

When the audit log accumulation system records an event, it is not necessary to send a notification to the person, company, device or application which caused the event.

5.5.8 Vulnerability analysis

Vulnerability analysis is covered by the public key infrastructure audit procedures.

Vulnerability analyzes should be performed, reviewed and revised through a review of these controlled events. These analyzes must be carried out periodically in accordance with the internal procedures provided for this purpose.

System audit data is stored for use in investigating any negative impact and thus being able to locate vulnerabilities.

5.6 Information files

We guarantee that all certificate information is retained for an appropriate period, in accordance with the provisions of section 5.5.2 of this policy.

5.6.1 Types of archived registries

The following documents, relating to the life cycle of the certificate, are stored by SIGNICAT SLU (o by the registration entities):

- All system audit data.
- All data relating to certificates, including contracts with signatories and data relating to their identification and location.
- Requests for issuance and revocation of certificates.
- Type of document presented when requesting a certificate.
- Identity of the Registration Entity which accepts the certificate request.
- Unique identification number provided by the previous document.
- All certificates issued or published.
- CRLs issued or registers of the status of certificates generated.
- History of keys generated.
- Communications between elements of the PKI.
- Certification Policies and Practices.
- All audit data identified in section 5.4.
- Information relating to certification requests.
- Documentation provided in order to justify certification requests.
- Information relating to the life cycle of the certificate.

SIGNICAT SLU and / or Registration Authorities, as applicable, will be responsible for the proper archiving of all such material.

5.6.2 Time limit for keeping records

The previously specified registers are archived for a period of at least 15 years, or during the period established by the legislation currently in force.

In particular, the registers of revoked certificates, available in the Lists of Revoked Certificates and through the online certificate status verification service (OCSP), are accessible for free consultation for a period of at least 15 years from the time of their issuance, or the time limit established by the legislation in force at the time of their change of status.

5.6.3 Protection of archives

The archives are protected in such a way that only duly authorized persons can have access to them. These archives are protected against viewing, modification, deletion or other undue manipulation by means of their storage in a reliable system.

Appropriate protection of archives is guaranteed through the assignment of qualified personnel to the purposes of their processing and storage in external and secure facilities.

5.6.4 Backup copy procedure

We have an external storage center to ensure the availability of copies of the electronic file archives. Physical documents are stored in secure places, access to which is restricted to authorized personnel only.

Backup copies of all electronic documents are made daily on a gradual basis and weekly in the event of data recovery.

In addition, SIGNICAT SLU (or the companies performing the registration function) keeps a hard copy in a safe place, separate from the facilities of its own Certification Entity.

5.6.5 Prerequisites for time stamping

Records are dated from a reliable Source via NTP.

This information does not need to be digitally signed.

5.6.6 Location of the archiving system

A centralized system collects information relating to the activity of the equipment concerned by the certificates management service.

5.6.7 Procedures for obtaining and verifying information from the archives

A procedure describes the process of verifying that archived information is correct and accessible. Information and means of verification are provided to the auditor.

5.7 Keys renewal

Prior to the expiration of the use of the CA's private key, a modification to the keys will be made. The old CA and its private key will be used exclusively for signing LRCs if there are active certificates issued by this CA. A new CA will be generated, with a new private key and a new DN. The modification of the subscriber's keys is carried out by carrying out a new issuance procedure.

Alternatively, in the case of subordinate Certification Authorities, the renewal of the certificate with or without change of keys may be an option, the procedure described above thus not being inapplicable.

5.8 Compromise of keys and reactivation following a disaster

5.8.1 Incidence and compromise management procedures

SIGNICAT SLU has developed security and business continuity policies which allow it to manage and reactivate systems in the event of incidents and compromise of operations, thus ensuring critical certificate revocation and status publication services.

5.8.2 Corruption of resources, applications or data

Upon the occurrence of a resource, application, or data corruption event, relevant management procedures will be implemented in accordance with EID's security and incident management policies, which contemplate scalability, investigation and response to the incident. Where necessary, procedures for compromise of keys or reactivation following a disaster will be initiated.

5.8.3 Compromise of the entity's private key

Whenever such compromise is known or suspected, the key compromise procedures will be activated in accordance with security policies, incident management, and business continuity allowing the recovery of critical systems, if necessary, in an alternative data center.

5.8.4 Business continuity following a disaster

SIGNICAT SLU will restore critical services (suspension, revocation and publication of certificate status information) in accordance with the existing impact and business continuity plan, restoring normal operation of the aforementioned services within 24 hours from the occurrence of the disaster.

SIGNICAT SLU has an alternative center should it be necessary to set up the certification systems described in the business continuity plan.

5.8.5 Notification of Incidents to the National Supervisory Authority for Trust Services

In accordance with Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), SIGNICAT SLU will notify any security breach or loss of integrity impacting the provision of trust services within 24 hours of becoming aware of it, to the competent supervisory authority, regardless of the denomination it holds at any given time.

In addition, the same timeframes shall be respected for any security breach or loss of integrity impacting the Video Identification service, as well as the content of both the initial and subsequent notifications.

Notifications will be carried out in accordance with internal procedures and protocols established for the management and communication of security incidents, ensuring timely, complete, and consistent reporting to the competent authority and, where applicable, to the affected data subjects. Likewise, SIGNICAT SLU will comply with the communication protocols, formats, and channels established by the national supervisory authority, and any additional requirements that may be issued by it in relation to incident reporting.

5.8.6 Notification to the National Data Protection Authority

In compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR), when personal data may be compromised due to a security breach, SIGNICAT SLU, as the data controller, will notify the Spanish Data Protection Agency (AEPD) within 72 hours of becoming aware of the breach. In addition to the above Notification to the Data Subjects section, SINGICAT SLU will notify the affected data subjects if the breach entails a high risk to their rights and freedoms.

The same timeframes shall be respected for any security breach or loss of integrity impacting the Video Identification service, as well as the content of the notification.

Notifications will be carried out in accordance with internal procedures and protocols established for the management and communication of security incidents, ensuring timely, complete, and consistent reporting to the competent authority and, where applicable, to the affected data subjects. Likewise, SIGNICAT SLU will comply with the communication protocols, formats, and channels established by the AEPD, and any additional requirements that may be issued by it in relation to incident reporting.

5.9 Service termination

SIGNICAT SLU guarantees subscribers and third parties that possible interruptions would be minor following the completion of the services of the certification services provider. In this sense, continuous keeping of the registers defined in paragraph 5.5.1. is guaranteed, during the period established in paragraph 5.5.2 of this Statement on Certification Practices.

Notwithstanding the foregoing, SIGNICAT SLU will, if necessary, perform all relevant actions in order to transfer to a third party or notarial deposit, the record keeping obligations specified during the corresponding period, by virtue of this Statement on Certification Practices or corresponding legal provision.

Before completing its services, SIGNICAT SLU develops a completion plan, with the following provisions, namely that:

- It will provide the necessary funds, including third party liability insurance, to continue to complete revocation activities.

- It will inform all Signatories / Subscribers, trusting Third Parties and other CAs with whom it has entered into agreements or other type of relationship, within a prior period of at least 6 months.

- It will revoke any authorization to subcontracted entities in order to act on behalf of the CA during the certificate issuance procedure.

- It will transfer its obligations relating to the preservation of register information and its history for the period indicated to subscribers and users.

- It will destroy or disable CA private keys to prevent their misuse.

- It will preserve active certificates, as well as the verification and revocation system until the extinction of all issued certificates.

- It will carry out all necessary tasks for the transfer of the obligations of preservation of the information of the register and of the recording archives of the events during the respective deadlines, indicated to the subscriber and to third parties trusting in the certificates.

- It will inform the national Supervisor of the completion of its activity and the destination of the certificates within a period of at least 2 months, specifying whether management is transferred and to whom, or whether it ceases to be in force.

- It will also inform the national Superior of the initiation of any collective proceedings against SIGNICAT SLU, as well as any other relevant circumstance likely to prevent the continuity of the activity.

6 Technical security controls

SIGNICAT SLU, through the PKI of Uanataca, S.A., uses reliable systems and products, protected against any alteration, which guarantee the technical and cryptographic security of the certification procedures for which they support.

6.1 Generating and installing the key pair

6.1.1 Generating the key pair

The key pair of the intermediate certification entity "ELECTRONIC IDENTIFICATION CA1" is created by the primary certification entity "UANATACA ROOT 2016" in accordance with the ceremonial procedures of UANATACA, within the high security perimeter intended for this task.

The activities carried out during the key generation ceremony are recorded, dated and signed by all involved parties in the presence of an Auditor. These records are protected for audit and monitoring purposes for an appropriate period.

For the purposes of generating the primary and intermediate certification entities' keys, devices with FIPS 140-2 level 3 and Common Criteria EAL4 + certifications are used.

UANATACA ROOT 2016	4.096 bytes	25 years
ELECTRONIC IDENTIFICATION CA1	4.096 bytes	13 years

-	Certificates of end entity	2.048 bytes	Up to 5 years

The Disclosure Text documents (PKI Disclosure Statement-PDS) for all digital certificate profiles indicated in this document are available at the link:

https://www.signicat.com/about/qualified-certificates-for-electronic-signatures

6.1.2 Generating the signatory key pair

The signatory can generate his keys himself by means of the procedure defined by SIGNICAT SLU, keys which will be made available to him thanks to the information provided during the certificate request. SIGNICAT SLU never generates keys outside of a QSCD to be sent to the signatory.

Keys are generated using the RSA public key algorithm, with a minimum length of 2048 bytes.

6.1.3 Sending the private key to the signatory

The signatory's private key is generated within a private space of the signatory in a remote HSM. Private key access credentials are entered by the signatory himself; they are not stored or likely to be deduced or intercepted by the remote generation and protection system. The private key is not sent to the signatory, that is to say, it never leaves the security environment that guarantees exclusive control of the private key by the signatory.

In the case of short-term certificates, there is no sending of the private key, SIGNICAT SLU guaranteeing exclusive control of the key by the user.

6.1.4 Sending the public key to the certificate issuer

The method of handing over the public key to the trust electronic services provider is PKCS # 10, other equivalent cryptographic evidence, or any other method approved by SIGNICAT SLU.

6.1.5 Distribution of the public key of the certification services provider

The keycodes are communicated to third parties trusting in the certificates, thus guaranteeing the integrity of the key and authenticating its origin through its publication in the Deposit.

Users can access the Deposit in order to obtain public keys and, in addition, in S / MIME applications; the data message may contain a chain of certificates which are thus distributed to users.

The Certificate of Primary and Subordinate Certification Authorities will be made available to users on the SIGNICAT SLU Web page.

6.1.6 Keys length

- The keys length of the Primary Certification Authority is 4096 bytes.
- The keys length of the Subordinated Certification Authorities is 4096

bytes.

- The keys length of the end Entity Certificates is 2048 bytes.

6.1.7 Generating public key parameters

The public key of the primary, subordinate Certification Authorities and subscriber certificates is encrypted in accordance with RFC 5280.

Additionally, SIGNICAT SLU follows the interoperability guidelines defined in the standard, including the maximum character limits for certificate fields.

No additional or more stringent restrictions have been defined beyond those specified in RFC 5280.

6.1.8 Checking the quality of the public key parameters

- Module Length = 4096 bytes
- Key generation algorithm: rsagen1
- Summary cryptographic functions: SHA256.

6.1.9 Generation of keys in IT applications or team assets

All keys are generated in team assets, in accordance with the provisions of section 6.1.1.

6.1.10 Purposes of key use

The uses of keys for CA certificates consist exclusively of signing certificates and CRLs.

The uses of keys for end-entity certificates consist exclusively of digital signature and non-repudiation issues.

6.2 Protection of the private key

6.2.1 Standards of the cryptographic modules

Regarding the modules managing the keys of SIGNICAT SLU and subscribers of electronic signature certificates, the required level is guaranteed by the standards as indicated in the previous sections.

6.2.2 Control by more than one person (n of m) of the private key

Multi-person control is required in order to activate the CA's private key. In the matter of this Statement on Certification Practices, there is a concrete policy of 3 to 6 people for the effects of the activation of the key.

Cryptographic devices are physically protected as determined in this document.

6.2.3 Deposit of the private key

SIGNICAT SLU does not store usable copies of the signatories' private keys by using its own resources.

6.2.4 Backup copy of the private key

The CA private keys are archived for a period of ten (10) years after the issuance of the last certificate. They are stored in secure, fireproof archives and in an external custody facility. The collaboration of at least two persons is required to recover the CA private key from the original cryptographic device.

Keys generated in QSCD: keys cannot be backed up, as it is not possible to export them from QSCD.

Keys generated in centralized HSM and in centralized QSCD: it is only possible to make backup copies of an encrypted blob using the Security World key of the HSM used, its decryption not being possible without the use of credentials that only the certificate holder is aware of.

6.2.5 Archiving the private key

The private keys of CAs are archived for a period of 10 years from the issuance of the last certificate. They will be stored in a secure fireproof archive and the external protection center. The intervention of at least two people will be necessary in order to retrieve the private key of the CAs in the initial cryptographic device.

Only in case of encryption certificates, the subscriber can keep the private key for the period deemed appropriate. In this case, SIGNICAT SLU also keeps a copy of the private key associated with the encryption certificate.

SIGNICAT SLU does not generate or archive certificate keys issued by software.

6.2.6 Introduction of the private key into the cryptographic module

Private keys are generated directly in cryptographic modules.

6.2.7 Private key activation method

The private keys of the Certification Entity are stored in an encrypted manner in cryptographic modules.

6.2.8 Private key deactivation method

The private key is activated by performing the corresponding secure connection procedure of the cryptographic module, by the persons indicated in section 6.2.2.

The keys of the CA are activated through a process of m of n (3 of 6).

The activation of the private keys of the intermediate CA is managed through the same m of n process as the keys of the CA.

6.2.9 Private key destruction method

In order to deactivate the private key, it will be necessary to follow the steps described in the administrator's manual of the corresponding cryptographic equipment.

6.2.10 Classification of cryptographic modules

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Archiving the public key

SIGNICAT SLU archives its public keys in the usual way, in accordance with the provisions of section 5.5 of this document.

6.3.2 Time limits for the use of public and private keys

The periods of use of the keys are determined by the duration of the certificate, after which they can no longer be used.

As an exception and if it exists, the private decryption key can continue to be used, even after the certificate expiry.

6.4 Activation data

6.4.1 Generation and installation of activation data

No activation data shall be required for short-term certificates.

The activation data of the devices that protect the private keys are generated in accordance with the provisions of section 6.2.2 and the key ceremony procedures.

The creation and distribution of said devices are recorded.

Likewise, activation data is generated in a secure manner.

6.4.2 Protection of activation data

The activation data of the devices that protect the private keys of the primary and subordinate certification authorities are protected by the holders of the administrator cards of the cryptographic modules, as noted in the key ceremony document.

The signatory of the certificate is responsible for protecting his private key, using one or more passwords as complete and complex as possible. The signatory must remember the stated password (s).

6.5 IT security controls

SIGNICAT SLU, thanks to the public key infrastructure of Uanataca, S.A., uses reliable systems to deliver its certification services. IT controls and audits have been implemented in order to establish a management of its IT assets, in line with the level of security required for the management of electronic certification systems.

With regard to information security, controls are carried out in accordance with the certification scheme relating to ISO 27001 information management systems.

The equipment used is initially configured with the appropriate security profiles by the systems personnel with regard to the following aspects:

- Security configuration of the operating system.
- Application security configuration.
- Correct sizing of the system.
- Configuration of Users and permits.
- Configuration of History events.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic prerequisites.

6.5.1 IT security technical prerequisites

Each server comprises the following features:

- Control of access to the services of subordinate Certification Authorities and management of privileges.
- Imposition of segregation of duties for the purposes of privilege management.
- Identification and authentication of roles associated with identities.
- Records of the subscriber's history, subordinate Certification Authorities and audit data.
- Audit of security related events.
- Security self-diagnosis relating to the services of the subordinate Certification Authorities.
- Key recovery mechanisms and of the system of subordinate Certification Authorities.

The exposed functionalities are achieved through a combination of an operating system, PKI software, physical protection and procedures.

6.5.2 IT security level assessment

The certification and registration authority applications used by SIGNICAT SLU are reliable.

6.6 Technical life cycle controls

6.6.1 Systems development controls

Applications are developed and implemented in accordance with development and change control standards.

Applications have methods to verify integrity and authenticity, as well as the appropriateness of the version to use.

6.6.2 Security management controls

SIGNICAT SLU develops specific activities for the training and awareness of employees in matters of security. The materials used for training and the documents describing the processes are updated following their approval by a group for security management. The performance of this function has an annual training plan.

SIGNICAT SLU requires by contract the equivalent security measures to any external service provider involved in the tasks of electronic trust services.

6.6.2.1 Classification and management of information and assets

An inventory of assets is kept, as well as documentation and a management procedure for these materials in order to guarantee their proper use.

EID's security policy details the procedures for managing classified information according to its level of confidentiality.

The documents are catalogued in three levels as: WITHOUT CLASSIFICATION, INTERNAL USE AND CONFIDENTIAL.

6.6.2.2 Management operations

SIGNICAT SLU has an adequate incident management and response program, through the implementation of an alert system and the generation of periodic reports.

The safety document outlines the incident management process in detail.

SIGNICAT SLU documents all the procedures relating to the functions and responsibilities of the personnel involved in the control and handling of the elements contained in the certification process.

6.6.2.3 Security supports processing

All supports are handled in a secure manner, in accordance with the prerequisites for the classification of information. Supports containing sensitive data are securely destroyed once they are no longer required.

6.6.2.4 System planning

The Systems department keeps a register of equipment capacities. With the resource control application of each system, a possible resizing can be considered.

6.6.2.5 *Incidence and response reports*

A procedure for monitoring incidents and their resolution records responses and performs the economic evaluation of the resolution of the negative impact.

6.6.2.6 *Operational procedures and responsibilities*

The activities assigned to people whose role is trusted are defined. These people are distinct from those responsible for carrying out daily operations without any confidentiality character.

6.6.2.7 *Access system management*

SIGNICAT SLU strives to confirm that the access system is limited to authorized persons.

In particular:

General CA

- It has controls through firewalls, antivirus and high availability IDS.
- Sensitive data is protected using cryptographic techniques or access controls with strong identification.
- It has a documented procedure for managing user registrations and unsubscriptions, as well as a detailed access policy to its security policy.
- It has procedures in place to ensure that operations are carried out in accordance with the roles policy.
- Each person has an associated role in order to carry out certification operations.
- Staff are responsible for their actions through the confidentiality agreement signed with the company.

Certificate generation:

Authentication for the purposes of the issuance process is carried out through a system of m of n operators in order to activate the private key.

Revocation management:

The revocation shall be carried out with strict authentication of the applications of an authorized administrator. Historical systems will generate evidence that guarantees non-repudiation of the actions performed by the system administrator.

Revocation status:

The revocation status application has access control through authentication with certificates or double identification factor to avoid any attempt to modify revocation status information.

6.6.3 Lifecycle security controls

SIGNICAT SLU ensures that cryptographic IT equipment used for signing certificates is not tampered with during transport through inspection of delivered equipment.

Cryptographic IT equipment is transported on prepared supports to avoid any manipulation.

All relevant device information is recorded in order to add them to the asset catalogue.

The use of cryptographic computer certificate signing equipment requires the use of at least two trusted employees.

Evidence tests are periodically performed to ensure correct operation of the device.

The device of the cryptographic computer equipment is only handled by trusted personnel.

The private SIGNICAT SLU signing key, stored in cryptographic IT equipment, will be discarded once the device is removed.

The configuration of the system, as well as its modifications and updates are documented and controlled.

Modifications or updates are authorized by the security manager and remain reflected in the corresponding work reports. These configurations will be performed by at least two trusted people.

6.7 Network security controls

Controls are established to protect physical access to network management devices, and an architecture tidies up generated traffic based on its security characteristics and creating clearly defined sections of the network. This division is done through the use of firewalls.

The transfer of confidential information over unsecured networks is carried out in an encrypted manner using SSL protocols or the VPN system with two-factor authentication.

6.8 Time Sources

A coordinated time synchronization procedure via NTP accesses two independent services:

- The first synchronization takes place thanks to a service using antennas and GPS receivers, which thus allows a STRATUM 1 trust level (with two systems whose high availability makes this feasible).

- The second has a complementary synchronization via NTP with the Royal Institute and Observatory of the Army (ROA). **Change of status of a Secure Signature Creation Device (SSCD)**.

In the event of a change in the status of the certification of qualified signature creation devices (QSCD), the following steps must be followed:

a) We have a list of various certified QSCDs, as well as a close relationship with the suppliers of said devices, in order to guarantee alternatives to possible loss of certification status of QSCD devices.

b) In the event of finalization of the validity period or loss of certification, these QSCDs will not be used for the purpose of issuing new digital certificates, whether they are new issues or possible renewals.

c) It will be necessary to immediately change the QSCD device, provided with a valid certification.

d) If it is demonstrated that a QSCD device has never been genuine to counterfeiting or other type of fraud, it will be necessary to immediately communicate it to the customers and to the regulatory entity, to revoke the digital certificates issued for these devices and replace them by issuing valid QSCDs.

7 Certificate profiles and lists of revoked certificates

7.1 Certificate profile general requirements

All qualified certificates issued under this policy comply with X.509 version 3 and RFC 3739 standards, as well as the various profiles described in EN 319 412.

Documentation relating to the profiles of standard EN 319 412 can be requested from SIGNICAT SLU.

7.1.1 Version number

SIGNICAT SLU issues certificates X.509 Version 3

7.1.2 Certificate extensions

Certificates extensions are detailed in section 7.2

7.1.3 Object identifier (OID) of the algorithms

The object identifier of the signature algorithm is: 1.2.840.113549.1.1.11 sha256WithRSAEncryption

The object identifier of the public key algorithm is: 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Names format

Certificates must contain the required information for its use, as determined by the appropriate policy.

7.1.5 Names restriction

Names contained in the certificates are restricted as “Distinguished Names” X.500, which are unique and not ambiguous.

7.1.6 Object identifiers (OID) of certificate types

All certificates include an identifier of the certificates policy under which they have been issued, in accordance with the indicated structure in section 1.5.531.

7.2 Certificate profiles

7.2.1 ROOT Certificate

The Root authority is available via the following link:

https://web.uanataca.com/common/project/pdf/autoridad-certificacion/01_raiz-ca-2016.cer


```
-----BEGIN CERTIFICATE-----
MIIHAzCCBOugAwIBAgIITWOS6Y7X5ZQwDQYJKoZIhvcNAQELBQAwgbkxCzAJBgNV
BAYTAkVTMUQwQgYDVQQHDDtCYXJjZWxvbmEgKHNlZSBjdXJyZW50IGFkZHJlc3Mg
YXQgd3d3LnVhbmF0YWNhLmNvbS9hZGRyZXNzKTEWMBQGA1UECgwNVUFOQVRBQ0Eg
Uy5BLjEVMBMGA1UECwwMVFNQLVVBTkFUQUNBMRswGQYDVQQDDBJVQU5BVEFDQSBS
T09UIDIwMTYxGDAWBgNVBGEMD1ZBVEVTLUE2NjcyMTQ5OTAeFw0xNjAzMTEwOTEz
NTNaFw00MTAzMTEwOTEzNTNaMIG5MQswCQYDVQQGEwJFUzFEMEIGA1UEBww7QmFy
Y2Vsb25hIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy51YW5hdGFjYS5jb20v
YWRkcmVzcykxFjAUBgNVBAoMDVVBTkFUQUNBIFMuQS4xFTATBgNVBAsMDFRTUC1V
QU5BVEFDQTEbMBkGA1UEAwwSVUFOQVRBQ0EgUk9PVCAyMDE2MRgwFgYDVQRhDA9W
QVRFUy1BNjY3MjE0OTkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
d5rtQey704cMzz7A1vuB4HLs0Y8YlH7BXKFAuxwzst1GOl7TzZzOeDEjGZMSjI00
JRUdmZ/lmG927tES5dDlrfDrNvKu3mof9j6Wjch4HmNqT6I30TXnhBNbtKEYHWxC
cIvQ0OKaFUUBEt+NzS6smyDAzbwyFUPSPid8JoGaGUMy7hhah38cLN408ffigCFT
ehZIsRvDnsU1WU34vcAYLLmgjsvBNmq2V+Ts8+vtrLcRbpQ8usMbwJSO1aoi71Lu
ISeBGJjqaszMPOty923PGHemImxHl5mHT13k5ha98EK4ZXMFfjxSVrypvpHgjThU
V3s4ZeaSpSbWkFxl6Tl++OTciMLOp66jwZV3I4DqeRmNXJkiRebs5u8bDDZxxeSP
RusoFI1cLm9cqCNy51hd2LNv8QECUNQ/RPon0sh+BSoSedppYXq6TFqpabE/FTnt
JBU7CMJV3EFJ/jSvXf6qj7JjInUQXajSxDdt0WrmDW8aQCRKCZ0Ml/Iwb8yk83/y
ZDt6E+Ez63V/x7sA2ZygG61zf4wOT95FNA4Z1atfOEcp/2uc5HXKrUTXTMDJJZfD
WMo30Ae1Rei94TRd/9XRqPdEk0B/VL5/991SlEX6Ol0NwKRPm6HNNZoWbdnmLEc+
CGnX1yj01R51Y4UTOalJ/W7oiNxmpZQAdAc9NN/gkwIDAQABo4IBCzCCAQcwHQYD
VR0OBBYEFFUs8byhXrnuoC+IVxBb/Jb3kZosMA8GA1UdEwEB/wQFMAMBAf8wgaYG
A1UdIASBnjCBmzCBmAYEVR0gADCBjzAzBggrBgEFBQcCARYnaHR0cDovL3d3dy51
YW5hdGFjYS5jb20vcHVibGljL3BraS9kcGMvMFgGCCsGAQUFBwICMEwMSkNlcnRp
ZmljYWRvIHJhw616IGRlIFVBTkFUQUNBLiBWZXIgaHR0cDovL3d3dy51YW5hdGFj
YS5jb20vcHVibGljL3BraS9kcGMvMA4GA1UdDwEB/wQEAwIBBjAcBgNVHREEFTAT
gRFpbmZvQHVhbmF0YWNhLmNvbTANBgkqhkiG9w0BAQsFAAOCAgEATAyOSKmK/yj6
JFb/RaHMmor8knkwQWVi3lFASKyfLQc6FfHoVjEgihu6HekIlMS7WBzetQVomaTR
TDu6eJeyo/+7CB+VGGHOYYjSdc8F8WI1HFN3f6ztKuM6zlVz3Xyj9BHhg1H4gqNL
Yxe99kq14xQEOR/fm0p7rVgVeeHhG8m1S5UGyyJ1ukeiB0d0PqwVWlG1np+i/nhf
nrxGSTnbRJyHzx6tuaLuQyHQU+Dg0TS8k65a8URioVkQ0CWb7yIyJ5bEBmPR2yqX
Owt6nYR8/3blrU99+wp67pmQttSggX3sB2a9WfY94Y5uIPB7JisOUBmqH23RjakE
c+UMLMjnvJQ82+1M7oGebnaVd1RVK+okemQ5zx57BzkzSl/i4G+Zxya8oQb2cIqF
HnvyCVXDOd4/CWNBLZQCTyGRUKOocvu1kKXgmVY6hTQGhM8Tr5yg/XT21gaAv3/7
th5ib2iGgq8Q8E3AW3ND+8N/qMjZ2aIkBKQYUFmLWiZt6n6ni73E2LQQEs+0uh9+
1xTPcI7AfDv+p0m6HDP0pq0t7BX0DQbh5QwPpiHBkB8atzE5gmQxnkt4/g0S2av5
```

Lc+U7ufZ5/ao7tLL1qkTX2r87jN7T8+lZOSHBbQan2QosyBfZWXgxaFYTspoy5tP
n4RMcCgXqHSYlArUKaQ8OWmT42AKLdY=
-----END CERTIFICATE-----

7.2.2 INTERMEDIATE CA Certificate

https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer

-----BEGIN CERTIFICATE-----
MIIIZzCCBk+gAwIBAgIIfGPd9OcmVZcwDQYJKoZIhvcNAQELBQAwgZsxCzAJBgNV
BAYTAkVTMQ8wDQYDVQQHDAZNQURSSUQxJzAlBgNVBAoMHkVsZWN0cm9uaWMgSWRl
bnRpZmljYXRpb24gUy5MLjEQMA4GA1UECwwHUFNDLUVJRDEmMCQGA1UEAwwdRUxF
Q1RST05JQyBJREVOVElGSUNBVElPTiBDQTExGDAWBgNVBGEMD1ZBVEVTLUI4NjY4
MTUzMzAeFw0yMDA0MDkxNzM3MDBaFw0yMjA0MDkxNzM3MDBaMIGHMQswCQYDVQQG
EwJFUzEiMCAGA1UEBAwZMWVyLUFwZWxsaWRvIDJkby1BcGVsbGlkbzEPMA0GA1UE
KgwGTm9tYnJlMRgwFgYDVQQFEw9JRENFUy0xMjM0NTY3OFAxKTAnBgNVBAMMIE5v
bWJyZSAxZXItQXBlbGxpZG8gMmRvLUFwZWxsaWRvMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAp89uHcT6Tg00JUsSpNl7YsryG7a40aW/FXtwkFusOlcP
glb7GdmSlYEVO2dYhz1PLHfnvMBOXqp95ftLujZm4uN74vMtPMy6m2VzxLsAH2vW
UJ83q/WQyV8fPCyZJRN+pdnX7cTNx03vmH307OHw6HlxebsXMxrl7j5JTw5wdyry
ZJzG667krsl5Us2kvXq3DNOXng6QdVPodODsRlTJ33WI2h0j9Fuy9B+GgdCXrXt0
nD/FcNkr8LGP+VIzNL1AOe1Jnsa3pJ3jgP9nIWfoisOYC14tP3RCFewHVisurZjw
fWIEvvD0HkDptxWy9Xd4ULpQzPg+tqHZA0SSmpa3ZQIDAQABo4IDvzCCA7swgZsG
CCsGAQUFBwEDBIGOMIGLMAgGBgQAjkYBATALBgYEAI5GAQMCAQ8wCAYGBACORgEE
MFMGBgQAjkYBBTBJMEcWQWh0dHBzOi8vd3d3LmVsZWN0cm9uaWNpZC5ldS9jZXJ0
aWZpY2F0aW9uLXByYWN0aWNlLXN0YXRlbWVudC1jcGQvEwJFTjATBgYEAI5GAQYw
CQYHBACORgEGATCB3gYIKwYBBQUHAQEEgdEwgc4wXAYIKwYBBQUHMAKGUGh0dHBz
Oi8vd3d3LmVsZWN0cm9uaWNpZC5ldS9wdWJsaWMvZG93bmxvYWQvdHNwLWNlcnRp
ZmljYXRlcy9lbGVjdHJvbmljaWRDQTEuY3J0MDYGCCsGAQUFBzABhipodHRwOi8v
b2NzcDEudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvb2NzcC8wNgYIKwYBBQUHMAGG
Kmh0dHA6Ly9vY3NwMi51YW5hdGFjYS5jb20vcHVibGljL3BraS9vY3NwLzAdBgNV
HQ4EFgQUk+bPyLTDPD3IoBINpHM7ZPRLacowDAYDVR0TAQH/BAIwADAfBgNVHSME
GDAWgBSFFWTNmwdInffmmkQHnHkKjKGWPzAfBgNVHRIEGDAWgRRpbmZvQGVsZWN0
cm9uaWNpZC5ldTCB/wYDVR0gBIH3MIH0MAkGBwQAi+xAAQIwgeYGCysGAQQBg68Z
AQECMIHWMIGEBggrBgEFBQcCAjB4HnYAQwBlAHIAdABpAGYAaQBjAGEAZABvACAA
YwB1AGEAbABpAGYAaQBjAGEAZABvACAAZABlACAAUABlAHIAcwBvAG4AYQAgAEYA
7QBzAGkAYwBhACAAUQBTAEMARAAgAGMAZQBuAHQAcgBhAGwAaQB6AGEAZABvME0G
CCsGAQUFBwIBFkFodHRwczovL3d3dy5lbGVjdHJvbmljaWQuZXUvY2VydGlmaWNh
dGlvbi1wcmFjdGljZS1zdGF0ZW1lbnQtY3BkLzB3BgNVHR8EcDBuMDWgM6Axhi9o
dHRwOi8vY3JsMS51YW5hdGFjYS5jb20vcHVibGljL3BraS9jcmwvZWlkLmNybDA1
oDOgMYYvaHR0cDovL2NybDIudWFuYXRhY2EuY29tL3B1YmxpYy9wa2kvY3JsL2Vp
ZC5jcmwwDgYDVR0PAQH/BAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEF
BQcDBDAhBgNVHREEGjAYgRZjb3JyZW9AZWxlY3Ryb25pY28uY29tMA0GCSqGSIb3
DQEBCwUAA4ICAQBl1iGUxcndEtFtAY/Z8hwyVtmVJarHWdnfM/eJxCKj4z8Bdl3J
wPh+X9PGXiM7rmBX17GbdBi/YnQLSsNmW6tZWV8SLgEG7qAOeYjIH6Oej8B92zQr
6DwN58ksuDdj4sJ6ZMMDCo3JD85SUNuzbkj+6Fo/hNXyZ5IGj36DKRDZb478W2n4
AMf+/JwLX6wjDO/jOQGGtVHi9kvsKJcStWBgVWFNJkED5CSmik8mDcLtMOYCAqFa
ebe2dgxqBk5vn+JsAKLl2RkSWt7NkcJ9kyYSEfQpg3hUOPLPt3Jq82ppGBaIpz7n
c4UnrHX+DcNO9pgxV6X6fJtjedrahoL4vWSZd5kLUZWIwtfriSFV3A9DvhnJ2OJA
TkSRgr1b01ceuAUvq2d3bWIIWmh//GNIiZViX4kVcbchISVX9PEZBCvs8d7veZ+2
BqjFXvXvayh87430+F71/14pNnaiMllKhkARAKIXvL/cHsW2tVW2idEPNzaYaMvq
5cndubJbfWdcdesgpd3Bj2NSKQpo4Qi09WcuaHwKePq8Ou6kmzNvly1sINMwbspq

```
/Io73Goe5K01PTT3BCvknexiozhTs1PCuPHmhZJBbk6vDUJsNF8CCOmIBd8NU9/d
Sk9ilQ0ujYrNpdqPDJU7pho59iItV9R+DT0AFL+lOUCgYy3TkynLNGfJJw==
-----END CERTIFICATE-----
```

7.2.3 Qualified Natural Person Certificate on the CLOUD without QSCD

Field	**CLOUD without QSCD**	**Remarks**
Natural Person	**Authentication and Signature**	**OID 1.3.6.1.4.1.55193.1.1.1**
1. Basic structure		
1.1. Version	"2"	The literal "2" corresponds to version 3.
1.2. Serial Number	Automatically established by the CA. Unique identification number of the certificate.	It cannot be a negative number or 0.
1.3. Signature Algorithm		
1.3.1. Algorithm	SHA-256 with RSA Signature	1.2.840.113549.1.1.11
1.3.2. Parameters	Not applicable	
1.4. Issuer		
1.4.1. Country Name (C)	"SP"	OID 2.5.4.6
1.4.2. Organization Name (O)	"Electronic IDentification S.L."	OID 2.5.4.10
1.4.3. Locality Name (L)	"Madrid"	OID 2.5.4.7
1.4.4. Organization Identifier	"VATES-B86681533"	OID 2.5.4.97
1.4.5. Common Name (CN)	ELECTRONIC IDENTIFICATION CA1	OID 2.5.4.3
1.4.6. Organization Unit (OU)	"PSC-EID"	
1.5. Validity		
1.5.1. Not Before	Starting date of validity	YYMMDDHHMMSSZ
1.5.2. Not After	Expiry Date	YYMMDDHHMMSSZ
1.6. Subject		
1.6.1. Country Name	Country of residence or nationality of the signatory.	OID 2.5.4.6
1.6.2. Organization Name	This field must not be filled.	OID 2.5.4.10
1.6.3. Organization Unit Name	This field must not be filled.	OID 2.5.4.11

1.6.4. Organization Identifier	This field must not be filled.	OID 2.5.4.97
1.6.5. Title	This field must not be filled.	OID 2.5.4.12
1.6.6 Surname	Family name of the signatory (as it appears on the official document)	OID 2.5.4.4
1.6.7. Given name	First name of the signatory (as it appears on the official document)	OID 2.5.4.42
1.6.8. Serial Number	Official document number encrypted according to ETSI EN 319 412-1 ("IDCES-12345678Z")	OID 2.5.4.5
1.6.9. Common Name	FIRST NAME AND FAMILY NAME OF SIGNATORY	OID 2.5.4.3
1.7. Subject Public Key Info		
1.7.1. AlgorithmIdentifier		
1.7.1.1. Algorithm	RSA encryption	OID 1.2.840.113549.1.1.1
1.7.1.2. Parameters	Not applicable	
1.7.2. SubjectPublicKey	Signatory public key	

Field	**CLOUD without QSCD**	**Remarks**
Natural Person	**Authentication and Signature**	**OID 1.3.6.1.4.1.55193.1.1.1**
2. Extensions		
2.1. Authority Key Identifier	Issuer key identifier	OID 2.5.29.35 (Marked as NON critical according to EN 319412-2)
2.1.1. KeyIdentifier		Derived from the public key
2.2. Subject Key Identifier	Signatory key identifier	OID 2.5.29.14 (Marked as NON critical according to EN 319412-2)
2.2.1. KeyIdentifier		Derived from the public key
2.3. Key Usage		OID 2.5.29.15
2.3.1. Digital Signature	Selected. "1"	
2.3.2. Content commitment	Selected. "1"	
2.3.3. Key Encipherment	Selected. "1"	

2.3.4. Data Encipherment	Not selected. "0"	
2.3.5. Key Agreement	Not selected. "0"	
2.3.6. Key Certificate Signature	Not selected. "0"	
2.3.7. CRL Signature	Not selected. "0"	
2.3.8. Encipher only	Not selected. "0"	
2.3.9. Decipher only	Not selected. "0"	
2.4. Certificate Policies		OID 2.5.29.32 (Marked as NON critical according to EN 319412-2)
2.4.1. Policy Information		
2.4.1.1. Policy Identifier	1.3.6.1.4.1.55193.1.1.1	SIGNICAT SLU policy identifier
2.4.1.2. Policy Qualifiers		
2.4.1.1.1 CPS URL	https://www.electronicid.eu/assets/documents/EID_DPC.pdf	SIGNICAT SLU SCP URL
2.4.1.1.2. User Notice/Explicit Text	"Qualified Natural Person Certificate cloud without QSCD."	Indicative text
2.4.2Policy information		
2.4.2.1. Policy Identifier	0.4.0.194112.1.0	Identifier of the qualified natural person certificate policy
2.5. Subject Alternative Names		OID 2.5.29.17 (Marked as NON critical according to EN 319412-2)
2.5.1. rfc822Name	Natural person's email	
2.6. Extended Key Usage		OID 2.5.29.37 (Marked as NON critical according to EN 319412-2)
2.6.1. clientAuth	Present (1.3.6.1.5.5.7.3.2)	
2.6.2. Email Protection	Present (1.3.6.1.5.5.7.3.4)	Actives itself subject to entering the signatory's email
Field	**CLOUD without QSCD**	**Remarks**

Natural Person	**Authentication and Signature**	**OID 1.3.6.1.4.1.55193.1.1.1**
2.7. cRLDistributionPoint		OID 2.5.29.31 This paragraph is not mandatory subject to the existence of the OCSP functionality. (Marked as NON critical according to EN 319412-2)
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/EID.crl	uniformResourcEIDentifier (**NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/EID.crl	uniformResourcEIDentifier (**NO HTTPS)**
2.8. Authority Info Access		OID 1.3.6.1.5.5.7.1.1 (Marked as NON critical according to EN 319412-2)
2.8.1. Access Description		
2.8.1.1. Access Method	id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp1.uanataca.com/public/pki/ocsp/	URL of access to OCSP **(NO HTTPS)** uniformResourcEIDentifier
2.8.1.1.2. Access Location	http://ocsp2.uanataca.com/public/pki/ocsp/	URL of access to OCSP **(NO HTTPS)** uniformResourcEIDentifier
2.8.2. Access Description		
2.8.2.1. Access Method	id-ad-caIssuers	OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer	URL of access to CA certificate (NO HTTPS) uniformResourcEIDentifier
2.9. Qualified Certificate Statements		OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance		OID 0.4.0.1862.1.1 Indication of qualified certificate

2.9.2. QcEuRetentionPeriod	"15"	OID 0.4.0.1862.1.3 Retention periods for records
2.9.4. QcPDS		OID 0.4.0.1862.1.5 (YES HTTPS) URL of access to disclosure text
2.9.4.1 PdsLocation		
2.9.4.1.1 url	https://www.electronicid.eu/assets/documents/EID_PDS.pdf	
2.9.4.1.2 language	"EN"	(SIZE (2))} --ISO 639-1 key language
2.9.5. QcType	id-etsi-qct-esign	OID 0.4.0.1862.1.6.1 Electronic signature certificate in accordance with Regulation (EU) Nº 910/2014
2.10. Basic Constraints		OID 2.5.29.19
2.10.1. cA	FALSE	

7.2.4 Qualified Natural Person Certificate on the CLOUD with QSCD

Field	**CLOUD with QSCD**	**Remarks**
Natural Person	**Authentication and Signature**	**OID 1.3.6.1.4.1.55193.1.1.2**
1. Basic Structure		
1.1. Version	"2"	The literal "2" corresponds to version 3.
1.2. Serial Number	Automatically established by the CA. Unique identification number of the certificate.	It cannot be a negative number or 0.
1.3. Signature Algorithm		
1.3.1. Algorithm	SHA-256 with RSA Signature	1.2.840.113549.1.1.11
1.3.2. Parameters	Not applicable	
1.4. Issuer		
1.4.1. Country Name (C)	"SP"	OID 2.5.4.6
1.4.2Organization Name	"Electronic IDentification S.L."	OID 2.5.4.10

(O)		
1.4.3. Locality Name (L)	"Madrid"	OID 2.5.4.7
1.4.4. Organization Identifier	"VATES-B86681533"	OID 2.5.4.97
1.4.5. Common Name (CN)	ELECTRONIC IDENTIFICATION CA1	OID 2.5.4.3
1.4.6. Organizational Unit (OU)	"PSC-EID"	
1.5. Validity		
1.5.1. Not Before	Validity starting date	YYMMDDHHMMSSZ
1.5.2. Not After	Expiry date	YYMMDDHHMMSSZ
1.6. Subject		
1.6.1. Country Name	Country of residence or nationality of the signatory.	OID 2.5.4.6
1.6.2. Organization Name	This field must not be filled.	OID 2.5.4.10
1.6.3. Organizational Unit Name	This field must not be filled.	OID 2.5.4.11
1.6.4. Organization Identifier	This field must not be filled.	OID 2.5.4.97
1.6.5. Title	This field must not be filled.	OID 2.5.4.12
1.6.6. Surname	Family name of the signatory (as indicated in the official document)	OID 2.5.4.4
1.6.7. Given Name	First name of the signatory (as appearing in the official document)	OID 2.5.4.42
1.6.8. Serial Number	Encrypted official document number in accordance with ETSI EN 319 412-1 ("IDCES-12345678Z")	OID 2.5.4.5
1.6.9. Common Name	FIRST NAME AND FAMILY NAME OF SIGNATORY	OID 2.5.4.3
1.7. Subject Public Key Info		
1.7.1. AlgorithmIdentifier		
1.7.1.1. Algorithm	RSA Encryption	OID 1.2.840.113549.1.1.1

1.7.1.2. Parameters	Not applicable	
1.7.2. SubjecPublicKey	Signatory public key	

Field	**CLOUD with QSCD**	**Remarks**
Natural Person	**Authentication and Signature**	**OID 1.3.6.1.4.1.55193.1.1.2**
2. Extensions		
2.1. Authority Key Identifier	Issuer key identifier	OID 2.5.29.35 (Marked as NON critical according to EN 319412-2)
2.1.1. KeyIdentifier		Derived from the public key
2.2. Subject Key Identifier	Signatory key identifier	OID 2.5.29.14 (Marked as NON critical according to EN 319412-2)
2.2.1. KeyIdentifier		Derived from the public key
2.3. Key Usage		OID 2.5.29.15
2.3.1. Digital Signature	Selected. "1"	
2.3.2. Content Commitment	Selected. "1"	
2.3.3. Key Encipherment	Selected. "1"	
2.3.4. Data Encipherment	Not selected. "0"	
2.3.5. Key Agreement	Not selected. "0"	
2.3.6. Key Certificate Signature	Not selected. "0"	
2.3.7. CRL Signature	Not selected. "0"	
2.3.8. Encipher Only	Not selected. "0"	
2.3.9. Decipher Only	Not selected. "0"	
2.4. Certificates Policies		OID 2.5.29.32 (Marked as NON critical according to EN 319412-2)
2.4.1. Policy Information		

2.4.1.1. Policy Identifier	1.3.6.1.4.1.55193.1.1.2	SIGNICAT SLU policy identifier
2.4.1.2. Policy Qualifiers		
2.4.1.1.1 CPS URL	ttps://www.electronicid.eu/assets/documents/EID_DPC.pd	SIGNICAT SLU SCP URL
2.4.1.1.2. User Notice/Explicit Text	"Qualified Natural Person Certificate Cloud with QSCD"	Indicative text
2.4.2. Policy Information		
2.4.2.1. Policy Identifier	0.4.0.194112.1.2	Identifier of the qualified natural person certificate policy
2.5. Subject Alternative Names		OID 2.5.29.17 (Marked as NON critical according to EN 319412-2)
2.5.1. rfc822Name	Natural person email	
Field	**CLOUD with QSCD**	**Remarks** **OID 1.3.6.1.4.1.55193.1.1.2**
Natural Person	**Authentication and Signature**	
2.6. Key Extended Use		OID 2.5.29.37 (Marked as NON critical according to EN 319412-2)
2.6.1. clientAuth	Present (1.3.6.1.5.5.7.3.2)	
2.6.2. Email Protection	Present (1.3.6.1.5.5.7.3.4)	Actives itself subject to entering the signatory's email
2.7. cRLDistributionPoint		OID 2.5.29.31 This paragraph is not mandatory subject to the existence of the OCSP functionality. (Marked as NON critical according to EN 319412-2)
2.7.1. distributionPoint	http://crl1.uanataca.com/public/pki/crl/EID.crl	uniformResourcEIDentifier (**NO HTTPS)**
2.7.2. distributionPoint	http://crl2.uanataca.com/public/pki/crl/EID.crl	uniformResourcEIDentifier (**NO HTTPS)**
2.8. Authority Info Access		OID 1.3.6.1.5.5.7.1.1

		(Marked as NON critical according to EN 319412-2)
2.8.1. Access Description		
2.8.1.1. Access Method	id-ad-ocsp	OID 1.3.6.1.5.5.7.48.1
2.8.1.1.1 Access Location	http://ocsp1.uanataca.com/public/pki/ocsp/	URL of access to OCSP **(NO HTTPS)** uniformResourcEIDentifier
2.8.1.1.2. Access Location	http://ocsp2.uanataca.com/public/pki/ocsp/	URL of access to OCSP **(NO HTTPS)** uniformResourcEIDentifier
2.8.2. Access Description		
2.8.2.1. Access Method	id-ad-caIssuers	OID 1.3.6.1.5.5.7.48.2
2.8.2.1.1 Access Location	https://www.electronicid.eu/assets/documents/ELECTRONICIDENTIFICATIONCA1.pem.cer	URL of access to CA certificate (NO HTTPS) uniformResourcEIDentifier
2.9. Qualified Certificate Statements		OID 1.3.6.1.5.5.7.1.3
2.9.1. qCCompliance		OID 0.4.0.1862.1.1 Indication of qualified certificate
2.9.2. QcEuRetentionPeriod	"15"	OID 0.4.0.1862.1.3 Retention period for records
2.9.3. QcSSCD		OID 0.4.0.1862.1.4 Qualified signature creation device
2.9.4. QcPDS		OID 0.4.0.1862.1.5 (YES HTTPS) URL of access to the disclosure text
2.9.4.1 PdsLocation		
2.9.4.1.1 url	https://www.electronicid.eu/assets/documents/EID_PDS.pdf	
2.9.4.1.2 language	"EN"	(SIZE (2))} --ISO 639-1 key language
2.9.5. QcType	id-etsi-qct-esign	OID 0.4.0.1862.1.6.1

		Electronic signature certificate in accordance with Regulation (EU) Nº 910/2014
2.10. Basic Constraints		OID 2.5.29.19
2.10.1. cA	FALSE	

7.3 Certificate Revocation List Profile

7.3.1 Version number

CRLs issued by SIGNICAT SLU belong to version 2.

7.4 OCSP's profile

7.4.1 Version number

In accordance with IETF RFC 6960 standard.

8 Compliance audit

SIGNICAT SLU has communicated the start of its activity as a provider of certification services to the MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION (State Secretariat for DIGITALIZATION AND ARTIFICIAL INTELLIGENCE - TELECOMMUNICATIONS AND DIGITAL INFRASTRUCTURES) and is subject to revisions control that this body deems necessary.

8.1 Compliance audit frequency

SIGNICAT SLU conducts an annual compliance audit, in addition to any time internal audits it performs according to its own criteria, due to suspected breach of security measures.

8.2 Identification and qualification of the auditor

The audits are carried out by an external and independent audit company, who are competent in technical matters and experienced in IT security, in security of information systems and compliance audits of public key certification services, as well as associated elements.

8.3 Relationship between the auditor and the audited entity

The prestige of audit companies is recognized. They have specialized services in performing IT audits, and as a result, there is no conflict of interest which could distort their intervention with regard to SIGNICAT SLU.

8.4 List of items subject to audit

In respect of SIGNICAT SLU, the audit verifies:

a) That the entity has a management system which guarantees the quality of the service provided.

b) That the entity meets the prerequisites of the Statement on Certification Practices and other documentation related to the issuance of certificates.

c) That the Statement on Certification Practices and other associated legal documentation comply with SIGNICAT SLU agreements and the provisions of the regulations in force.

d) That the entity manages its information systems adequately.

8.5 Actions to be taken following a lack of conformity

Once the compliance audit report has been received by management, the deficiencies are analyzed alongside the company that carried out the audit and corrective measures addressing these deficiencies are developed and completed.

If SIGNICAT SLU cannot develop and / or carry out the corrective measures or if the deficiencies are deemed an immediate threat to the security or integrity of the system, it must immediately communicate this to its Safety Committee in order to be able to carry out the following actions:

- Cessation of operations on a temporary basis.
- Revocation of the key from the Certification Authority and regeneration of the infrastructure.
- Termination of the service of the Certification Authority.
- Any other additional actions which may be necessary.

8.6 Processing of audit reports

Audit results' reports are submitted to the SIGNICAT SLU Security Committee within 15 days of completion of the audit.

9 Legal prerequisites

9.1 Financial capacity

9.1.1 Insurance cover

SIGNICAT SLU has sufficient guarantees to cover its professional civil liability, which it maintains in accordance with the applicable regulations currently in force.

9.1.2 Other assets

Without stipulation.

9.1.3 Insurance coverage for policyholders and third parties entrusted with the certificates

SIGNICAT SLU has sufficient guarantees to cover its civil liability, through professional liability insurance covering trust electronic services, to the minimum insured amount of Euros 3,000,000.

9.2 Confidentiality

9.2.1 Confidential information

SIGNICAT SLU considers confidential all information that is not expressly catalogued as public. Information considered confidential will not be disseminated without the express written consent of the entity or company which has conferred confidentiality to this information, subject to the existence of any legal impositions.

SIGNICAT SLU has an adequate information handling policy and model confidentiality agreements that all persons with access to confidential information must sign.

9.2.2 Non-confidential information

SIGNICAT SLU considers as non-confidential information:

a) That contained in this SCP and the Certification Policies.

b) The information contained in the certificates.

c) Any information whose accessibility is prohibited by the regulations in force.

9.2.3 Responsibility to protect confidential information.

SIGNICAT SLU is responsible for protecting confidential information generated or communicated during all operations. Delegated parties, such as entities which administer subordinate issuing CAs or registration authorities, are responsible for protecting confidential information generated or stored on their own. With respect to end entities, certificate subscribers are responsible for protecting their own private key, as well as any activation information (i.e., passwords or PIN) necessary to access or use the private key.

9.3 Protection of personal data

SIGNICAT SLU guarantees the compliance with the regulations in force in terms of the protection of personal data, stipulated in European Regulation Nº 2016/679 General Data Protection, in Organic Law 3/2018, dated December 5th, on the Protection of Personal Data and Guarantee of Digital Rights, including video-identification services and, in general, all applicable national regulations.

In witness whereof, it has documented the security and organizational aspects and procedures of this Statement on Certification Practices, in order to ensure that all personal data to which it has

access is protected against loss, destruction, damage, infringement and illegal or unauthorized procedures.

Below, all the information necessary with regard to the processing of personal data carried out by SIGNICAT SLU is detailed as follows:

Data Controller: ELECTRONIC IDENTIFICATION, S.L

NIF: B-86681533
Address: Avenida Ciudad de Barcelona, 81. 2ª Planta. C.P. 28004 Madrid (Spain).
Email: eidLegal@signicat.com

Purpose of processing

SIGNICAT SLU has a duty to inform users that all of their personal data provided is processed for the following purpose:

SIGNICAT SLU, in its capacity as qualified trust service provider for the provision of electronic trust services and the video identification service, shall process the data for the following purposes: (i) carrying out the management, development, compliance and control of the contractual relationship in relation to the provision of trust electronic services and the video identification service in accordance with the provisions of these CPS; (ii) sending any type of postal or electronic correspondence linked to said relationship; (iii) inclusion of the data in the contact agendas of a corporate, departmental and employee nature that so require; (iv) the correct economic, accounting, tax and invoicing management derived from the legal relationship maintained; (v) management of the corresponding contractual file for archiving and maintenance of the contractual file history; (vi) the issue and management of the electronic certificate of the natural person user; (vii) electronic identification of users through unassisted video for which, in the event that the user gives their express consent, we will use their facial biometric data based on obtaining a sample of key points of biometric data without SIGNICAT SLU at any time retaining all of the biometric data. This data is pseudonymized using an encryption algorithm, with only the pseudonymized data being used to carry out the relevant biometric comparisons. In this regard, information relating to your identity, including facial biometric pattern data, will be stored for the purpose of an identification process to enable SIGNICAT SLU to access and verify your identity.

SIGNICAT SLU informs that the facilitated personal data will be processed exclusively for the purposes previously described and will not be processed in a manner incompatible with these stated purposes.

Processing authorization

The authorization for processing for the purposes of the Provision of Trust Electronic Services, including the Video Identification Services, is the fulfillment of the contract for the services requested, to which the user is a party.

In the event of the processing of biometric data, this is based on the express consent of the data subject as these are specially protected data.

Category of personal data

The categories of personal data processed by SIGNICAT SLU, by way of illustration but not necessarily limited to these that may be processed by SIGNICAT SLU for the Provision of Electronic Trust Services and the Video identification service, include identification data (first name, last name and identity), contact data (postal address, email and telephone number) and Biometric data (Extraction of biometric and identification data from the user's identification document, extraction of biometric data from the video and Biometric Comparison between video and image of the user's identification document).

All the data provided by the user will be used for the purpose of carrying out the identity verification service and the provision of electronic trust services, as well as for the management of the certificates issued throughout their life cycle.

Retention Period

The Data will be kept for the duration of the contractual relationship, as long as their deletion is not requested, and during the period of limitation of any legal actions that may arise, or claims that may be received from official bodies, in relation to this Contract and after the termination of the same. In any case, the maximum period of processing will be 15 years from the time of issue of the certificate, unless otherwise provided by law. Once our relationship has ended, your data will be duly blocked, in accordance with the provisions of the applicable regulations.

Recipients

The Data may be disclosed to third parties in compliance with legal obligations such as: (i) Judges, Courts and law enforcement agencies, in compliance with requirements, legal obligations or within the framework of legal proceedings; (ii) banking institutions, for the management of collections and payments; (iii) Tax Agency, for the fulfilment of tax obligations; (iv) financial auditors for the fulfilment of financial obligations; (v) public notaries in the event of the document being notarized; and (vi) any other third parties to whom, by virtue of the applicable regulations in force in each case, it is necessary to make the transfer, such as competent government bodies, for reasons of control, registration and inspection.

Users' personal data may be transferred and/or communicated to third parties as a consequence of consulting the revocation lists or to third parties who require consultation on their validity and the validity of the certificates.

In addition, certain data may be made available to third parties, both in Spain and in the European Union, for the purpose of the services they provide to our company (such as data hosting or

identification support services), under the protection of a data processor contract, in which the appropriate protection measures are guaranteed, in accordance with the provisions of the legislation on personal data protection, and with the obligation to return and/or destroy the data at the end of the service.

UANATACA, by issuing qualified electronic certificates will act as a processor for SIGNICAT SLU, providing validation of the data contained in the certificate (it does not process any biometric data) following EID's instructions.

Users' rights

Users have the right to contact SIGNICAT SLU in order to exercise the following rights with regard to the processing of their personal data:

- Confirmation. All users have the right to obtain confirmation that SIGNICAT SLU is actually processing their personal data.

- Access and rectification. Users have the right to have access to all their personal data, as well as to request the rectification of any items that are inaccurate or erroneous.

- Deletion / cancellation. Users may request the deletion / cancellation of their data if, among other reasons, it is not necessary for the purposes for which it was collected.

- Limitation and opposition. The user may request the limitation of processing so that his personal data does not apply to the corresponding operations. In specific circumstances and for reasons relating to his particular situation, the user may oppose the processing of data, SIGNICAT SLU therefore being obliged to cease processing it, subject to compelling legitimate reasons, or for the purposes of mounting a defense the face of possible complaints.

- Portability. Interested persons may request their personal data to be sent to them or transmitted to another manager, in a structured electronic format for usual use.

- Automated individual decisions: you have the right not to be subject to a decision based solely on automated processing, including profiling, and you may request human intervention in the cases provided for by law.

In order to exercise their rights or withdraw the consent provided to SIGNICAT SLU, users can send a request to the email address eidLegal@signicat.com or send a letter to the address indicated in

the information paragraph relating to the Data Controller. They must clearly indicate which right they wish to exercise. Once received, SIGNICAT SLU will contact the User in order to be able to identify his or her identity.

Furthermore, if the user considers that his/her data have not been processed in accordance with the regulations in force, he/she has the right to file a complaint in Spain before the Spanish Data Protection Agency (www.aepd.es), as well as to request information and protection before this body regarding the exercise of his/her rights.

9.3.1 Information processed as private

Personal information of a person that is not publicly available in the contents of a certificate or CRL is considered as private.

9.3.2 Information not considered as private

The personal information which is available in the contents of a certificate or CRL is not considered private since it is necessary for the provision of the subscribed service, without prejudice to the corresponding rights of the holder of the personal data under LOPD / RGPD legislation.

9.3.3 Responsibility to protect private information

The data controller must protect private information adequately.

9.3.4 Remarks and consent to use private information

Before establishing a contractual relationship, SIGNICAT SLU will provide interested persons with prior information relating to the processing of their personal data and the exercise of their rights and, where applicable, will obtain the obligatory consent to the purposes of the different processing from the main processing in terms of the provision of subscribed services.

9.3.5 Disclosure in accordance with judicial or administrative proceedings.

Personal data, whether considered private or not, may be disclosed exclusively, if necessary, for the formulation, exercise, or defense of claims during judicial, administrative or extrajudicial proceedings.

This will not be handed over to third parties unless subject to a legal obligation.

9.4 Intellectual property rights

SIGNICAT SLU is the owner of the intellectual property rights of this SCP, the Certification Policy and the PDS. SIGNICAT SLU is also the holder of the SCPs of the subordinate CAs, linked to the hierarchies of SIGNICAT SLU, without prejudice to the assignments of use of their rights in favor of the subordinate CAs and without prejudice to the contributions of their own subordinate CAs who hold the title.

9.5 Limitation of liability

SIGNICAT SLU will solely respond in the event of deficiencies in the procedures specific to its activity as a Trust Service Provider and, in accordance with the provisions of the corresponding Certification Policies and Practices. It shall not be held responsible under any circumstances for

actions or losses incurred by the applicants, holders, user bodies or, where applicable, involved third parties, which are not down to any error attributable to SIGNICAT SLU during the corresponding delivery and / or management procedures. certificates. SIGNICAT SLU will not respond in the event of fortuitous events, force majeure, terrorist attack, wildcat strike, as well as any hypotheses relating to actions constituting a crime or harmful fault to its service providers, and subject to a serious fault likely to be attributable to them.

SIGNICAT SLU will not respond to persons whose behavior in using certificates has been negligent. Failure to comply with the provisions of this Statement on Certification Practices and, in particular, those of the paragraphs relating to the obligations and liability of the parties must be considered as acts of negligence for these purposes and effects.

The monetary cap on the value of transactions is expressed in their own end entity certificate. The expression of the monetary value will be adjusted to the provisions of section 5.2.2 of Standard TS 101 862 of ETSI (European Telecommunications Standards Institute), www.etsi.org

9.6 Liability disclaimer

Under the applicable legislation, the liability of SIGNICAT SLU and the RA does not include cases in which the improper use of the certificate arises from conduct attributable to the Person and the User, as follows:

- Failure to provide adequate information, either initially or subsequently, due to changes in the circumstances reflected in the electronic certificate, if their inaccuracy could not be detected by the certification services provider beforehand;
- Incurring negligence with regard to the conservation of signature creation data and their confidentiality;
- Not having requested the suspension or revocation of the data of the electronic certificate in case of doubt as to the preservation of confidentiality;
- Have used the signature following the expiry of the validity period of the electronic certificate;
- Exceeding the limits indicated in the electronic certificate.
- During conducts attributable to the User if the latter acts in a negligent manner, that is to say when he does not check or does not take into account the restrictions appearing in the certificate, relating to his possible uses and the cap of the number of transactions; or when it does not take into account the current status of the certificate.
- Damage caused to the Person or to third parties due to the inaccuracy of the data appearing in the electronic certificate, in cases where the latter have been accredited by means of a public document, registered in a public register where required.

- Inappropriate or fraudulent use of the certificate in the event that the Person / Holder has assigned it or authorized its use in favor of a third party by virtue of a legal agreement such as granting the mandate or power of attorney, the Person / the Holder remaining solely responsible for controlling the keys associated with their certificate.

Neither will SIGNICAT SLU and RAs be liable, under any circumstances, if they appear in any of the following circumstances:

- State of War, natural disasters or any other case of Force Majeure.
- In case of use of the certificate, if it exceeds the provisions of the regulations in force and the Certification Policies.
- In the event of undue or fraudulent use of certificates issued or CRL issued by the CA.
- In the event of use of the information contained in the Certificate or the CRL.
- Due to the damage caused during the period of verification of the causes of revocation / suspension.
- Due to the content of messages or documents signed or digitally encrypted.
- Due to the failure to recover encrypted documents using the Person's public key.

9.7 Notifications

All proposed changes to this policy will be immediately posted on the SIGNICAT SLU Website.

This same document has a paragraph relating to modifications and versions where it is possible to be made aware of the modifications introduced since its creation, as well as their date.

The modifications made to this document will be communicated to third party organizations and companies issuing certificates in accordance with this SCP. Specifically, the modifications shall be notified to the National Supervision bodies.:

- Spain: The State Secretariat for Information Society and the Digital Agenda of the Ministry of Energy, Tourism and Digital Agenda, or the body responsible at the time for the supervision of trust services providers.

9.8 Modifications

9.8.1 Modification mechanism.

The CA reserves the right to modify this document for technical reasons, either to reflect any modification of the procedures following legal or regulatory prerequisites (EIDAS, CA / B Forum, National Supervisory Bodies, etc.) or due to optimization of the work cycle. Each latest version of this SCP replaces all previous versions which however remains applicable to certificates issued while such versions were in force, and until the first expiry date of such certificates. An update

will be published at least once a year. These updates will appear in the table of versions at the top of the document.

Changes that may be made to this SCP do not require any prior notification, subject to directly affecting the rights of Persons / Signatories of certificates, in which case they may send their comments to the organization of the administration of policies in a period of 15 days from their publication.

9.8.2 Circumstances in which the OID must be changed.

Not stipulated.

9.9 Applicable Law, Complaints and Dispute Resolution.

Any controversy or conflict arising from this document shall be definitively resolved by means of arbitrational intervention by an appointed arbitrator, operating within the framework of the Spanish Court of Arbitration, and in accordance with its Rules and Statutes, to which the administration of the arbitration is entrusted, and the appointment of the arbitrator or Arbitration Tribunal.

The parties declare their commitment to respect the arbitration resolution handed down.

The execution, interpretation, modification or validity of this SCP shall be governed by the provisions of Spanish and European Union legislation in force at all times.

9.10 Miscellaneous Clauses

9.10.1 Entire Agreement

The holders and third parties trusting in the Certificates assume the content of this Statement on Certification Practices in its entirety.

9.10.2 Assignment

The parties to this SCP may not assign any of their rights or obligations under these or applicable agreements without the written consent of SIGNICAT SLU.

9.10.3 Severability

If the individual provisions of this SCP become ineffective or incomplete, their nature will be void without prejudice to the effectiveness of all other provisions.

An ineffective provision will be replaced by an effective provision which will be deemed to more closely reflect the meaning and purpose of the ineffective provision. In the event of incomplete provisions, a modification shall be agreed to correspond to what would have been reasonably agreed in accordance with the meaning and the purposes of this SCP, where the matter had been under consideration beforehand.

9.10.4 Enforcement

SIGNICAT SLU may seek compensation and attorney's fees from a party for damages, losses and costs relating to that party's behavior. Failure by SIGNICAT SLU to enforce any provision of this SCP does not eliminate EID's right to enforce this SCP in the future, or the right to enforce any other provision of this SCP. In order to be effective, any waiver must be made in writing and duly signed by SIGNICAT SLU.

02534305G JORGE GUILLAMET PUNCERNAU (R: B86681533)

Firmado digitalmente por 02534305G JORGE GUILLAMET PUNCERNAU (R: B86681533)
Fecha: 2025.10.09 14:19:29 +02'00'