


VinCAsign Certification Practice Statement



10/06/2025: v2r26

General Information

Document information

Security classification:	Public document
Target entity:	
Version:	2.26
Issued by:	10/06/2025
File name:	Vintegris CPS v2r26.docx
Format:	Office 365
Author:	Vintegris

Formal status

Prepared by:	Reviewed by:	Approved by:
Name: RR Date: 10/06/2025	Name: VH Date: 10/06/2025	Name: VH Date: 10/06/2025

Version control

Version	Section changes	Changes description	Change author	Version issue date
1.0	Original	Document creation.	AC, FA, NA	26/02/2016
1.1	5.8	Communication to the SB in case of termination is included.	AC	03/05/2016
1.2	1.2 y 1.4	Inclusion of company seal certificates. References to law 11/2007 are eliminated for those of law 40/2015.	AC	20/04/2017
	Entire document	Inclusion of REIDAS aspects. The denomination of recognized certificates is changed to qualified certificates. The name of DSCF is changed to DCCF.	AC	20/04/2017
2.0	1.3.1.3	Reference to nebulaCERT product included	SSF	05/05/2017
	1.3.1.4	The reference to the termination of the previous hierarchy is included.	SSF	05/05/2017
2.1	1.3	Extended information on CRL and OCSP signing. Rewriting.	SSF	11/05/2017

Version	Section changes	Changes description	Change author	Version issue date
	5.8	Modification of contingency funds.	SSF	11/05/2017
2.2	4.9.3.	Revocation request procedures. Email method is included in help section of website.	SSF	22/05/2017
	4.9.7	Including that revocation statuses remain in the CRLs indefinitely.	SSF	30/05/2017
	9.6.10	Expanded complaint and dispute handling	SSF	30/05/2017
2.3		Incorporation certificate of representative of an entity without legal personality	AC	30/08/2017
2.4	1.3.1.3, 6.1.1	Indication of the new subordinate CA	AC	09/10/2017
	1.3.1.6	New OCSP services		
	4.9.6, 4.9.9, 4.9.11	New CRLs and OCSP		
	Entire document	References to the Electronic Signature Law are changed to REIDAS.		
2.5	2.5	Indication of the cryptographic hardware used	AC	14/02/2018
	6.2.5	New wording including the description of the creation of users' private keys in the		

Version	Section changes	Changes description	Change author	Version issue date
		centralized cryptographic hardware.		
	6.8	It describes which cryptographic hardware is used in each case.		
2.6	6.2.7.2	Key import conditions are clarified	NA	08/03/2018
2.7		Annual CPS review	AC VH	14/05/2018 19/05/2018
		VinCAsign nebulaSUITE Authority removal	AC	17/07/2018
		Change references to the GDPR	FA	20/07/2018
		Minor changes	AC	18/10/2018
2.8		Inclusion of new types of certificates	AC	16/01/2019
		Updating ETSI references	GA	06/02/2019
		Complete revision due to Pseudonym-certificate inclusion	AC/FA	27/02/2019
		Change of location of definitions and acronyms to conform to RFC 3647	AC	27/02/2019
	3.5; 4.5.3.1; 4.9.7; 9.3.2; 9.6.5.2	Aspects related to suspension are modified	VH/AC	12/03/2019

Version	Section changes	Changes description	Change author	Version issue date
	4.7.3	Modification on the renewal of certificates	VH	12/03/2019
	1.3.1	OCSP data modification and others	VH	12/03/2019
	4.9	URL Modifications	VH	12/03/2019
	6.9	Modifications on time sources	VH	12/03/2019
	4.9	Sections related to the suspension are deleted	VH/AC	13/03/2019
	1.4.1; 3.1.1	Change designation "1 use" to "ephemeral".	AC	14/03/2019
	5.4.8	Change in the timing of vulnerability analyses	VH	15/3/2019
	4.9.9	Creation of the last CRL	AC	18/03/2019
2.9		Inclusion of unbound natural person certificate types (individual subscribers).	AC/FA	20/06/2019
		Inclusion of unqualified certificate types for individual subscribers.	AC/FA	05/07/2019
		Inclusion of the use of video- identification for unqualified certificates.	AC	10/07/2019
		Inclusion of certificate types AGID representative	VH	17/09/2019
2.10	1.4.1.4; 1.4.1.6; 1.4.1.8;	Extension of certificate management to decentralized	VH	20/04/2020

Version	Section changes	Changes description	Change author	Version issue date
	1.4.1.10; 1.4.1.12; 1.4.1.14; 1.4.1.16; 1.4.1.18; 1.4.1.20; 1.4.1.22; 1.4.1.23; 1.4.1.26; 1.4.1.32;	management (software and QSCD card).		
		Inclusion of web authentication certificates	VH	30/04/2020
	1.2.1; 2.2; 4.9.9;	CA/B Forum Modifications	VH	03/05/2020
		CPS Annual review	VH	05/06/2020
2.11		Inclusion subordinate inclusion nebulaSUITE5 Inclusion of new regulations and elimination of repealed regulations.		16/11/2020
2.12		Alignment of CPS with RFC 3647 Separation of authentication and signature certificates for public employee with pseudonym. CAA field validation	VH	10/03/2021
2.13	1.4.2; 1.5.2; 1.5.4; 2.4;3.1.4; 3.2.1; 3.2.4; 3.2.7; 4.2.2; 4.9.1; 4.9.12;	Key commitment, complaints and suggestions Revision of CPS Added Audits per		05/10/2021

Version	Section changes	Changes description	Change author	Version issue date
	4.10.2; 5.3.1; 5.3.7; 5.7.3; 6.1.1; 6.7; 9.2.1; 9.5.2; 9.15	Baseline Requirements Reference EV Guidelines Verification Source Selection Criteria. Reference RFC 6844 errata 5065 Inclusion of revocation circumstances		
		Key Commitment Verification Forms Validation Specialist Training Notification of key compromise. Loss of QSCD qualification Insurance required by EV Guidelines Prevalence of EV Guidelines and resolution of conflicts with national legislation		
2.14	3.2 3.3 9.4 9.14	Issuance of certificates through video identification Inclusion of legislation related to video identification (Order ETD/465/2021)	VH	
	6.6	Provision in the CPS for the periodic review of		

Version	Section changes	Changes description	Change author	Version issue date
		systems, applications and the Security Policy.		
	1.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 4.8.6; 4.8.7; 6.1.7; 9.3.3	CPS update in accordance with RFC 3647 structure		
2.15	4.9.9, 4.5.2.1, 4.5.2.2, 4.5.3.1, 3.1.1.9, 7.1.3	General review and correction of observations	VTs	28/03/2022
	4.1.1.4, 4.9.9, 1.2.1, 6.1.7.1, 6.1.1.1.1	NC eIDAS		
2.16	9.2.1	Correction of the amount covered by civil liability insurance	RR	09/05/2022
	4.2.2	Update RFC validation CAA		
	1.5.1, 1.5.2	Víntegris address update		
2.17	3.2.4.4, 3.2.4.4.2	Updating due to MINECO requirement for correction nebulald	RR	08/06/2022
2.18	2.3, 2.4, 3.1.1.12, 3.1.1.13, 3.2.3.1, 4.1.1.4, 4.2.2, 4.2.3, 4.9.10, 4.10.2, 6.7, 7.1.4, 8.6,	Update after revision of BR 1.8.4 requirements for CCADB	RR	21/10/2022
	1.3.1.1.6-8, 1.3.1.2.5	OCSP renewal		
	Entire document	Rewritten in English		
2.19	2.1, 5.7.3, 6.2.1	Repository update.	RR	10/02/2023

Version	Section changes	Changes description	Change author	Version issue date
		Last CRL in case of CA compromise inclusion. QSCD EU Norm added. Annual update.		
2.20	3.1.1.6, 4.9.9, 6.5.1	eIDAS NC-plan	RR	22/03/2023
2.21	9.4.2	Mistake correction on GDPR role (Data controller)	RR	20/12/2023
	1.3.1.1.*; 6.1.1.1; 6.2.11.*	Nebula4 and nebula5 revokation and decommissioning		
2.22	5.8	QTSP Termination mistake	RR	13/12/2023
	1.2.1, 1.4.1.23	New profile: non qualified electronic seal	RR	13/12/2023
	1.1, 1.2.1, 1.3.1.*, 1.3.3, 3.2.1.3, 3.2.3.1, 3.2.4.3, 3.2.4.4, 3.3, 4.1.1.3, 4.1.1.4, 4.2.2, 4.3.2, 5.3.1, 6.1.1.3.2, 6.2.11.5, 7.1, 7.1.4, 8.1, 8.6, 9.14	QWAC service removal and revokation SSL TrustServices	RR	05/02/2024
	1.4.1.*	SMIME removal review	RR	05/02/2024
	1.4.1.25, 3.1.1.10, 6.1.1.1	TSA nebulaSUITE revokation	RR	05/02/2024
	1.3.1.3, 6.1.1.3.1, 6.1.7.1, 6.2.12, 6.2.9	SAM in remote qualified signature service	RR	05/02/2024

Version	Section changes	Changes description	Change author	Version issue date
	Entire document	Change from nebulaCERT to nebulaSUITE	RR	05/02/2024
	1.1, 1.2.1, 1.4.1.32-35, 4.9, 6.1.1.1, 6.1.5	Removal of AGID and SSL profiles	RR	19/02/2024
	1.4.1.3, 1.4.1.4, 1.4.1.7, 1.4.1.8, 1.4.1.11, 1.4.1.12, 1.4.1.21, 1.4.1.22, 1.4.1.28, 1.4.1.29, 1.4.1.31	Change to 72 maximum time on ephemeral certificates	RR	19/02/2024
	Entire document	Error review	RR	19/02/2024
2.23	1.2.1	Fix error in OIDs of AGID Legal Representative	RR	25/03/2024
	3.2.4.3.2	Fix NC eIDAS Audit	RR	01/04/2024
2.24	1.1, 1.2, 1.3, 1.4, 3.1.1.11, 3.1.1.12, 3.2.6, 4.1.1, 4.1.2, 4.9.12, 5.1, 5.3.3, 5.4, 5.7.3, 5.8, 6.1.1, 6.1.5, 6.1.6, 6.6.2, 8.3, 9.2.1, 9.4.4, 9.14	<p>Annual review of operations.</p> <p>Adaptation to the following regulations:</p> <ul style="list-style-type: none"> Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024, amending Regulation (EU) No 910/2014. Directive (EU) 2022/2555 (NIS 2) 	RR	06/03/2025

Version	Section changes	Changes description	Change author	Version issue date
		<p>Directive) and its Implementing Regulation of 17/10/2024.</p> <ul style="list-style-type: none"> Standard ETSI EN 319401 V3.1.1 <p>Extension of issuance periods to 4 years</p> <p>New certificate profile: graduate</p>		
	1.1, 1.2.1, 1.4.11, 1.4.12, 1.4.1.33, 1.4.1.34, 1.4.1.35, 1.4.1.36	New certificate profiles: licensed professional and student	RR	01/04/2025
	4.9.5, 4.3.3	eIDAS Audit obs.	RR	10/04/2025
2.25	3.2.4	Correction of identity validity period	RR	07/05/2025
2.26	3.1.1	Clarification about field sizes	RR	10/06/2025

Table of Contents

General Information	2
Document information	2
Formal status	2
Version control.....	3
Table of Contents	13
1. Introduction.....	24
1.1. Overview	24
1.2. Document name and identification.....	25
1.2.1. Certificate Identifiers (OIDs)	25
1.3. PKI Participants	31
1.3.1. Certification Authorities.....	31
1.3.2. Registration Authorities.....	40
1.3.3. Subscribers.....	41
1.3.4. Relying parties	42
1.3.5. Other participants.....	42
1.4. Certificate Usage	43
1.4.1. Appropriate Certificate Uses.....	43
1.4.2. Certificate prohibited usages	99
1.5. Policy administration	100
1.5.1. Organization Administering the Document.....	100
1.5.2. CPS approval procedures	100
1.5.3. Person Determining CPS suitability for the policy	100
1.5.4. Procedimientos de aprobación de la DPC	100
1.6. Definitions and Acronyms.....	101
1.6.1. Definitions.....	101
1.6.2. Acronyms	103

2. Publication and Repository Responsibilities.....	106
2.1. Repositories	106
2.2. Publication of information	106
2.3. Time or frequency of publication	107
2.4. Access controls on repositories	107
3. Identification and authentication	108
3.1. Naming.....	108
3.1.1. Types of names	108
3.1.2. Need for names to be meaningful.....	120
3.1.3. Anonymity or pseudonymity of subscribers.....	120
3.1.4. Rules for interpreting various name forms	120
3.1.5. Uniqueness of names	121
3.1.6. Recognition, authentication, and role of trademarks	121
3.2. Initial identity validation	122
3.2.1. By certificate type.....	122
3.2.2. Method to prove possession of private key	123
3.2.3. Authentication of Organization and Domain Identity	124
3.2.4. Authentication of individual identity.....	126
3.2.5. Non-verifies subscriber information	128
3.2.6. Validation of authority.....	129
3.2.7. Criteria for Interoperation or Certification.....	129
3.3. Identification and authentication for re-key requests	129
3.3.1. Identification and authentication for routine re-key	129
3.3.2. Identification and authentication for re-key after revocation	130
3.4. Identification and authentication for revocation request.....	130
4. Certificate Life-cycle operational requirements.....	132
4.1. Certificate application.....	132
4.1.1. Who can submit a certificate application.....	132

4.1.2.	Enrollment process and responsibilities	132
4.2.	Certificate application processing	133
4.2.1.	Performing identification and authentication functions.....	133
4.2.2.	Approval of rejection of certificate applications.....	134
4.2.3.	Time to process certificate applications.....	134
4.3.	Certificate issuance	135
4.3.1.	VinCAsign actions during certificate issuance	135
4.3.2.	Notification to subscriber by the CA of issuance of certificate	135
4.3.3.	Test certificates issuance.....	135
4.4.	Certificate acceptance	136
4.4.1.	Conduct constituting certificate acceptance.....	136
4.4.2.	Publication of the certificate by the CA.....	137
4.4.3.	Notification of certificate issuance by the CA to other entities	137
4.5.	Key pair and certificate usage.....	138
4.5.1.	Subscriber private key and certificate usage.....	138
4.5.2.	Use of the certificate and private key by the subscriber and the Registration Entity	139
4.5.3.	Relying party public key and certificate usage	143
4.6.	Certificate renewal.....	145
4.6.1.	Circumstance for certificate renewal	145
4.6.2.	Who may request renewal	145
4.6.3.	Processing certificate renewal requests.....	145
4.6.4.	Notification of new certificate issuance to subscriber	145
4.6.5.	Conduct constituting acceptance of a renewal certificate.....	145
4.6.6.	Publication of the renewal certificate by the CA.....	145
4.6.7.	Notification of certificate issuance by the CA to other entities	145
4.7.	Certificate re-key.....	146
4.7.1.	Circumstance for certificate re-key	146

4.7.2.	Who may request certification of a new public key.....	146
4.7.3.	Processing certificate re-keying requests.....	146
4.7.4.	Notification of new certificate issuance to subscriber.....	147
4.7.5.	Conduct constituting acceptance of a re-keyed certificate	147
4.7.6.	Publication of the re-keyed certificate by VinCAsign.....	148
4.7.7.	Notification of certificate issuance by VinCAsign to third parties.....	148
4.8.	Certificate modification	148
4.8.1.	Circumstance for certificate modification.....	148
4.8.2.	Who may request certificate modification	148
4.8.3.	Processing certificate modification requests	148
4.8.4.	Notification of new certificate issuance to subscriber.....	148
4.8.5.	Conduct constituting acceptance of modified certificate	148
4.8.6.	Publication of the modified certificate by VinCAsign.....	148
4.8.7.	Notification of certificate issuance by VinCAsign to other entities.....	149
4.9.	Certificate revocation and suspension	149
4.9.1.	Circumstances for revocation.....	149
4.9.2.	Who can request revocation	151
4.9.3.	Procedure for revocation request.....	151
4.9.4.	Revocation request grace period	152
4.9.5.	Time within which VinCAsign must process the revocation request.....	152
4.9.6.	Revocation checking requirement for relying parties.....	152
4.9.7.	CRL issuance frequency	154
4.9.8.	Maximum latency for CRLs.....	154
4.9.9.	On-line revocation/status checking availability	154
4.9.10.	On-line revocation checking requirements.....	155
4.9.11.	Other forms of revocation advertisements available	155
4.9.12.	Special requirements for re-key compromise.....	155
4.9.13.	Circumstances for suspension	156

4.9.14.	Who can request suspension	156
4.9.15.	Procedure for suspension request	156
4.9.16.	Limits on suspension period	156
4.10.	Certificate status services	157
4.10.1.	Operational characteristics.....	157
4.10.2.	Service availability	157
4.10.3.	Optional features.....	157
4.11.	End of subscription	157
4.12.	Key escrow and recovery	157
4.12.1.	Key escrow and recovery policy and practices.....	157
4.12.2.	Session key encapsulation and recovery policy and practices.....	157
5.	Management, operational and physical controls	158
5.1.	Physical security controls.....	158
5.1.1.	Site location and construction.....	159
5.1.2.	Physical access	159
5.1.3.	Power and air conditioning	160
5.1.4.	Water exposures.....	160
5.1.5.	Fire prevention and protection	160
5.1.6.	Media storage	160
5.1.7.	Waste disposal.....	160
5.1.8.	Off-site backup	161
5.2.	Procedural controls.....	161
5.2.1.	Trusted roles	161
5.2.2.	Number of Individuals Required per Task	162
5.2.3.	Identification and authentication for each role	162
5.2.4.	Roles requiring separation of duties	163
5.3.	Personnel controls	163
5.3.1.	Qualifications, experience, and clearance requirements.....	163

5.3.2.	Background check procedures	164
5.3.3.	Training Requirements and Procedures	164
5.3.4.	Retraining frequency and requirements	165
5.3.5.	Job rotation frequency and sequence	165
5.3.6.	Sanctions for unauthorized actions.....	165
5.3.7.	Independent contractor controls	166
5.3.8.	Documentation supplied to personnel.....	166
5.4.	Audit logging procedures.....	166
5.4.1.	Types of events recorded	166
5.4.2.	Frequency of processing audit log.....	168
5.4.3.	Retention period for audit log.....	168
5.4.4.	Protection of audit log.....	169
5.4.5.	Audit log backup procedures.....	169
5.4.6.	Audit collection System (internal vs external).....	169
5.4.7.	Notification to event-causing subject	169
5.4.8.	Vulnerability assessments	170
5.5.	Records archival.....	170
5.5.1.	Types of records archived.....	170
5.5.2.	Retention period for archive	171
5.5.3.	Protection of archive	171
5.5.4.	Archive backup procedures	171
5.5.5.	Requirements for time-stamping of records.....	171
5.5.6.	Archive collection system (internal or external)	172
5.5.7.	Procedures to obtain and verify archive information	172
5.6.	Key changeover.....	172
5.7.	Compromise and disaster recovery.....	173
5.7.1.	Incident and compromise handling procedures	173

5.7.2.	Recovery Procedures if Computing resources, software and/or data are corrupted	173
5.7.3.	Recovery procedures after key compromise	173
5.7.4.	Business continuity capabilities after a disaster	174
5.8.	VinCAsign termination	175
6.	Technical security controls	177
6.1.	Key pair generation and installation.....	177
6.1.1.	Key pair generation	177
6.1.2.	Private key delivery to subscriber	179
6.1.3.	Public key delivery to certificate issuer	179
6.1.4.	CA public key delivery to relying parties	180
6.1.5.	Key sizes.....	180
6.1.6.	Public key parameters generation and quality checking	180
6.1.7.	Key usage purposes (as per X.509 v3 key usage field)	180
6.1.8.	Key generation in software applications or capital assets	181
6.2.	Private Key Protection and Cryptographic Module Engineering Controls	182
6.2.1.	Cryptographic module standards and controls	182
6.2.2.	Private key (n out of m) multi-person control.....	182
6.2.3.	Private key escrow.....	182
6.2.4.	Private key backup.....	182
6.2.5.	Private key archival.....	183
6.2.6.	Private key transfer into or from a cryptographic module	183
6.2.7.	Private key storage on cryptographic module	183
6.2.8.	Activating Private Keys	185
6.2.9.	Deactivating Private Keys	185
6.2.10.	Destroying Private Keys	185
6.2.11.	Cryptographic Module Capabilities	185
6.2.12.	Cryptographic storage for signer's keys	186

6.3.	Other aspects of key pair management	187
6.3.1.	Public key archival	187
6.3.2.	Certificate operational periods and key pair usage periods	187
6.4.	Activation data	187
6.4.1.	Activation data generation and installation	187
6.4.2.	Activation data protection.....	187
6.4.3.	Other aspects of activation data	187
6.5.	Computer security controls	188
6.5.1.	Specific computer security technical requirements.....	188
6.5.2.	Computer security rating.....	189
6.6.	Life cycle technical controls	189
6.6.1.	System development controls.....	189
6.6.2.	Security management controls	189
6.6.3.	Life-cycle technical controls	192
6.7.	Network security controls.....	192
6.8.	Time-stamping	193
7.	Certificate, CRL, and OCSP profiles.....	194
7.1.	Certificate profile	194
7.1.1.	Version number(s)	194
7.1.2.	Certificate Content and Extensions; Application of RFC 5280	194
7.1.3.	Algorithm object identifiers.....	194
7.1.4.	Name forms	194
7.1.5.	Name constraints.....	195
7.1.6.	Certificate policy object identifier	195
7.1.7.	Usage of Policy Constraints extension	195
7.1.8.	Policy Qualifiers syntax and semantics.....	195
7.1.9.	Processing semantics for the critical Certificate Policies extension	195
7.2.	CRL profile	195

7.2.1.	Version number(s)	195
7.2.2.	CRL and CRL entry extensions	195
7.3.	OCSP profile	196
7.3.1.	Version number(s)	196
7.3.2.	OCSP extensions	196
8.	Compliance audit and other assessments	197
8.1.	Frequency or circumstances of assessment	197
8.2.	Identity/qualifications of assessor	197
8.3.	Assessor's relationship to assessed entity	197
8.4.	Topics covered by assessment	197
8.5.	Actions taken as a result of deficiency	198
8.6.	Communication of results	198
8.7.	Self-Audits	199
9.	Other business and legal matters	200
9.1.	Fees	200
9.1.1.	Certificate issuance or renewal fees	200
9.1.2.	Certificate access fees	200
9.1.3.	Revocation or status information access fees	200
9.1.4.	Fees for other services	200
9.1.5.	Refund policy	200
9.2.	Financial responsibility	200
9.2.1.	Insurance coverage	200
9.2.2.	Other assets	201
9.2.3.	Insurance or warranty coverage for end-entities	201
9.3.	Confidentiality of business information	201
9.3.1.	Scope of confidential information	201
9.3.2.	Information not within the scope of confidential information	201
9.3.3.	Responsibility to protect confidential information	202

9.4.	Privacy of personal information	203
9.4.1.	Privacy plan.....	203
9.4.2.	Information treated as private	204
9.4.3.	Information not deemed private.....	204
9.4.4.	Responsibility to protect private information	205
9.4.5.	Notice and consent to use private information	205
9.4.6.	Disclosure pursuant to judicial or administrative process	206
9.4.7.	Other information disclosure circumstances	206
9.5.	Intellectual property rights	207
9.5.1.	Certificate ownership and revocation information.....	207
9.5.2.	Ownership of Certificate Practice Statement.....	207
9.5.3.	Ownership of the information related to names	207
9.5.4.	Key ownership	208
9.6.	Representations and warranties.....	208
9.6.1.	VinCAsign representations and warranties	208
9.6.2.	RA representations and warranties.....	209
9.6.3.	Subscriber representations and warranties	210
9.6.4.	Relying party representations and warranties	212
9.6.5.	Representations and warranties of other participants	212
9.7.	Disclaimers of warranties	212
9.8.	Limitations of liability.....	212
9.9.	Indemnities	212
9.9.1.	Subscriber compensation clause	212
9.9.2.	Relying certificate third-party indemnity clause	213
9.10.	Term and termination.....	213
9.10.1.	Term.....	213
9.10.2.	Termination	213
9.10.3.	Effect of termination and survival	213

9.11.	Individual notices and communications with participants	214
9.12.	Amendments.....	214
9.12.1.	Procedure for amendment	214
9.12.2.	Notification mechanism and period	214
9.12.3.	Circumstances under which OID must be changed.....	214
9.13.	Dispute resolution provisions	214
9.14.	Governing law	215
9.15.	Compliance with applicable law	216
9.16.	Miscellaneous provisions.....	216
9.16.1.	Entire agreement.....	216
9.16.2.	Assignment	216
9.16.3.	Severability	217
9.16.4.	Enforcement (attorneys' fees and waiver of rights)	217
9.16.5.	Force Majeure.....	217
9.17.	Other provisions.....	218

1. Introduction

1.1. Overview

This document states the certification practices of VinCAsign, the Certification Authority of VÍntegris SLU.

The types of certificates issued are classified according to several criteria. Considering its usage:

- Corporate certificates for natural persons
- Certificates for natural persons representative of a Legal Entity
- Corporate certificates for Spanish public employees
- Electronic seal certificates for the Spanish public administration bodies
- Electronic seal certificate for private entities
- Electronic time stamp certificates
- Individual certificates for natural persons
- Individual certificates for graduate natural persons
- Individual certificates for student natural persons
- Individual certificates for licensed professional
- Electronic seal certificate for IoT

Regarding the issuance media:

- Certificates issued in qualified device of creation of electronic signature and seal (QSCD).
- Certificates issued in software media.

Regarding representation:

- Certificates of representative of legal entity
- Certificates of representative of an entity without legal personality.

In terms of time of validity:

- Certificates with temporary validity up to 4 years
- Ephemeral certificates.

In terms of its function/duty:

- Certificates to identify natural persons or legal entities.
- Certificates to identify objects (IoT)
- Certificates with pseudonym

Regarding their qualification:

- Qualified certificates, in accordance with Regulation (EU) EIDAS¹.
- Non-qualified certificates

1.2. Document name and identification

This document is the VinCAsign Certification Practice Statement.

Document name	CERTIFICATION PRACTICE STATEMENT -CPS-
Version	2r26
Date of the current version	10/06/2025
Location	BARCELONA
OID	1.3.6.1.4.1.47155

1.2.1. Certificate Identifiers (OIDs)

VinCAsign has assigned to each certificate policy an object identifier (OID), for its identification by the applications.

¹ REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

For each of the profiles, two different OIDs are established according to the hierarchy based on the OID granted by IANA, and on which two sub-trees of OIDs are established for the two Vintegris certification hierarchies (ref. *1.3 PKI Participants*)

OID	Certificate type
1.3.6.1.4.1.47155.1.1.1 1.3.6.1.4.1.47155.2.1.1	Corporate certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.1.2 1.3.6.1.4.1.47155.2.1.2	Corporate certificates for natural persons (Software)
1.3.6.1.4.1.47155.1.1.51 1.3.6.1.4.1.47155.2.1.51	Ephemeral corporate certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.1.52 1.3.6.1.4.1.47155.2.1.52	Ephemeral corporate certificates for natural persons (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.2.1 1.3.6.1.4.1.47155.2.2.1	Certificates for natural person representative of a Legal Entity (QSCD)
1.3.6.1.4.1.47155.1.2.2 1.3.6.1.4.1.47155.2.2.2	Certificates for natural person representative of a Legal Entity (Software)
1.3.6.1.4.1.47155.1.2.51 1.3.6.1.4.1.47155.2.2.51	Ephemeral certificates for natural person representative of a Legal Entity (QSCD)
1.3.6.1.4.1.47155.1.2.52 1.3.6.1.4.1.47155.2.2.52	Ephemeral certificates for natural person representative of a Legal Entity (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.2.11 1.3.6.1.4.1.47155.2.2.11	Certificates of natural person representative of an entity without legal personality (QSCD)

OID	Certificate type
1.3.6.1.4.1.47155.1.2.12 1.3.6.1.4.1.47155.2.2.12	Certificates of natural person representative of an entity without legal personality (Software)
1.3.6.1.4.1.47155.1.2.151	Ephemeral certificates of natural person representative of an entity without legal personality (QSCD)
1.3.6.1.4.1.47155.1.2.152	Ephemeral certificates of natural person representative of an entity without legal personality (Software)
1.3.6.1.4.1.47155.1.11.1 1.3.6.1.4.1.47155.2.11.1	Certificates of natural person representative of an AGiD entity without legal personality (QSCD)
1.3.6.1.4.1.47155.1.11.2 1.3.6.1.4.1.47155.2.11.2	Certificates of natural person representative of an AGiD entity without legal personality (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.4.1 1.3.6.1.4.1.47155.2.4.1	Corporate certificates for Spanish public employees (QSCD)
1.3.6.1.4.1.47155.1.4.2 1.3.6.1.4.1.47155.2.4.2	Corporate certificates for Spanish public employees (Software)
1.3.6.1.4.1.47155.1.4.11 1.3.6.1.4.1.47155.2.4.11	Corporate certificates for Spanish public employees with pseudonym (QSCD)
1.3.6.1.4.1.47155.1.4.12 1.3.6.1.4.1.47155.2.4.12	Corporate certificates for Spanish public employees with pseudonym (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.5.1 1.3.6.1.4.1.47155.2.5.1	Electronic seal certificates for the Spanish public administration bodies (QSCD)

1.3.6.1.4.1.47155.1.5.2 1.3.6.1.4.1.47155.2.5.2	Electronic seal certificates for the Spanish public administration bodies (Software)
----------------------------------------------------	--------------------------------------------------------------------------------------

OID	Certificate type
1.3.6.1.4.1.47155.1.6.1 1.3.6.1.4.1.47155.2.6.1	Electronic seal certificate for private entities (QSCD)
1.3.6.1.4.1.47155.1.6.2 1.3.6.1.4.1.47155.2.6.2	Electronic seal certificate for private entities (Software)
1.3.6.1.4.1.47155.1.6.51 1.3.6.1.4.1.47155.2.6.51	Ephemeral electronic seal certificate for private entities (QSCD)
1.3.6.1.4.1.47155.1.6.52 1.3.6.1.4.1.47155.2.6.52	Ephemeral electronic seal certificate for private entities (Software)
1.3.6.1.4.1.47155.2.6.3	Non qualified electronic seal certificate for private entities (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.7.2 1.3.6.1.4.1.47155.2.7.2	Electronic seal certificate for IoT
1.3.6.1.4.1.47155.1.7.62 1.3.6.1.4.1.47155.2.7.62	Non-qualified electronic seal certificate for IoT

OID	Certificate type
1.3.6.1.4.1.47155.1.9.1 1.3.6.1.4.1.47155.2.9.1	Electronic time stamp certificates

OID	Certificate type
1.3.6.1.4.1.47155.1.10.1 1.3.6.1.4.1.47155.2.10.1	Individual certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.10.2 1.3.6.1.4.1.47155.2.10.2	Individual certificates for natural persons (Software)
1.3.6.1.4.1.47155.1.10.51 1.3.6.1.4.1.47155.2.10.51	Ephemeral individual certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.10.52 1.3.6.1.4.1.47155.2.10.52	Ephemeral Individual certificates for natural persons (Software)
1.3.6.1.4.1.47155.2.13.1	Individual certificates for graduate natural persons (QSCD)
1.3.6.1.4.1.47155.2.13.2	Individual certificates for graduate natural persons (Software)
1.3.6.1.4.1.47155.2.2.150	Individual certificates for licensed professional person (QSCD)
1.3.6.1.4.1.47155.2.2.151	Individual certificates for licensed professional person (Software and centralized)
1.3.6.1.4.1.47155.2.2.152	Individual certificates for licensed professional person (Software and decentralized)
1.3.6.1.4.1.47155.2.2.153	Individual certificates for licensed professional person (Software and managed)
1.3.6.1.4.1.47155.2.14.1	Individual certificates for students (QSCD)
1.3.6.1.4.1.47155.2.14.2	Individual certificates for students (Software)

OID	Certificate type
1.3.6.1.4.1.47155.1.110.1 1.3.6.1.4.1.47155.2.110.1	Non-qualified individual certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.110.2 1.3.6.1.4.1.47155.2.110.2	Non-qualified individual certificates for natural persons (Software)
1.3.6.1.4.1.47155.1.110.51 1.3.6.1.4.1.47155.2.110.51	Ephemeral Non-qualified individual certificates for natural persons (QSCD)
1.3.6.1.4.1.47155.1.110.52 1.3.6.1.4.1.47155.2.110.52	Ephemeral Non-qualified individual certificates for natural persons (Software)

This CPS follows the structure specified in RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" that has been created by the Network Working Group of the IETF (Internet Engineering Task Force).

In case of contradiction between this CPS and other practice documents and procedures, the provisions of this CPS shall prevail.

In addition, Vintegris respects and conforms to the current version of the CA-Browser Forum document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates". Latest version published is available at <https://www.cabforum.org>.

In the event of any inconsistency between any statement in this CPS and the CAB Forum requirements (both Baseline Requirements and EV Guidelines), the latter shall prevail.

1.3. PKI Participants

1.3.1. Certification Authorities

The certification service provider is the person, natural or legal, who issues and manages certificates for end entities, using a Certification Authority, or provides other services related to electronic signatures.

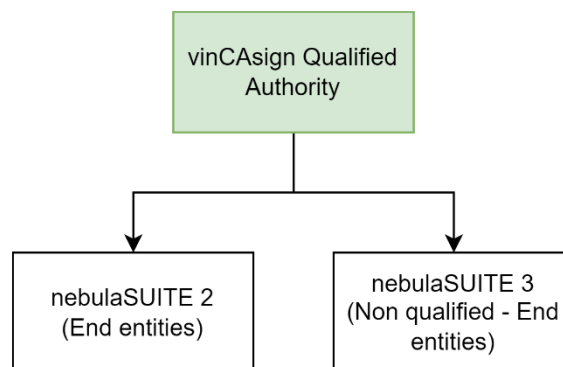
Víntegris SLU is a Trust Service Provider, acting in accordance with the provisions of Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, and the ETSI technical standards applicable to the issuance and management of qualified certificates, mainly ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2, in order to facilitate compliance with legal requirements and international recognition of its services.

As a TSP, Vintegris SLU has established two hierarchies of certification bodies on which the trust services it offers are based. Each of these two hierarchies maintains its independent naming structure based on the OID granted by IANA, being the bases:

Base OID	Hierarchy
1.3.6.1.4.1.47155.1.*	vinCAsign Qualified Authority
1.3.6.1.4.1.47155.2.*	CA Vintegris ROOT TrustServices

1.3.1.1. vinCAsign Qualified Authority Hierarchy

For the provision of certification services, Víntegris SLU has established a hierarchy of certification entities called "VinCAsign" (currently in process of discontinuation):



1.3.1.1.1. vinCAsign Qualified Authority

This is the **root certification authority** in the hierarchy that issues certificates to other certification authorities, and which public key certificate has been self-signed.

Identification data:

CN:	vinCAsign Qualified Authority
Fingerprint:	3e92ea167f59eab160fe5a7b74eb795bc3ec0173
Issuance date:	Thursday, 20/04/2017
Expiration date:	Sunday, 20/04/2042
RSA Key length:	4096 bits

1.3.1.1.2. vinCAsign nebulaSUITE2 Authority

It is a **subordinate Certification Authority** within the hierarchy that issues the certificates to the final entities, and which public key certificate has been digitally signed by the VinCAsign Qualified Authority.

Identification data:

CN:	vinCAsign nebulaSUITE2 Authority
Fingerprint:	0e9272b3cda96215a8ca55d7822b86a27a4ed466
Issuance date:	Wednesday, September 27th 2017, 16:20:46
Expiration date:	Friday, September 27th 2030 16:20:46
RSA Key length:	4096 bits

1.3.1.1.3. vinCAsign nebulaSUITE3 Authority

It is a **subordinate Certification Authority** within the hierarchy that issues the non-qualified certificates to the final entities, and which public key certificate has been digitally signed by the VinCAsign Qualified Authority.

Identification data:

CN:	vinCAsign nebulaSUITE3 Authority
Fingerprint:	7d274c84836d2e145aaf54fc0712552daa7b0bba
Issuance date:	8/08/2019 11:29:50 CEST
Expiration date:	8/08/2032 11:29:50 CEST
RSA Key length:	4096 bits

1.3.1.1.4. vinCAsign nebulaSUITE4 Authority (discontinued)

It is a **discontinued subordinate Certification Authority** within the hierarchy that issues the **qualified** certificates to the final entities, and which public key certificate has been digitally signed by the VinCAsign Qualified Authority.

Identification data

CN:	vinCAsign nebulaSUITE4 Authority
Fingerprint:	67d8255c38597d23398c465654b3440a25955be0
Issuance date:	Friday, May 8th 2020 13:19:48
Expiration date:	Sunday, May 8th 2033 13:19:48
RSA Key length:	4096

1.3.1.1.5. vinCAsign nebulaSUITE5 Authority (QWAC, discontinued)

It is a **discontinued subordinate Certification Authority** within the hierarchy that issues the **qualified** certificates to the final entities, and which public key certificate has been digitally signed by the VinCAsign Qualified Authority.

Identification data

CN:	vinCAsign nebulaSUITE5 Authority
Fingerprint:	724f627a2ca6abcb751cdc5c0f7f2e4be56f502c
Issuance date:	Wednesday, November 11th 2020 16:46:15
Expiration date:	Friday, November 11th 2033 16:46:15
RSA Key length:	4096

1.3.1.1.6. OCSF service for vinCAsign nebulaSUITE2

The signing certificate of the new VinCAsign OCSF services responses has been digitally signed by the "VinCAsign nebulaSUITE2 Authority".

Datos de la identificación:

OCSP1

CN:	Servicio OCSP1 vinCAsign
Fingerprint:	1F2B870B4E9F2A4B521E9466C367B41E615B9AA7
Issuance date:	2023-09-04 11:05:37+02:00
Expiration date:	2024-09-03 11:05:37+02:00
RSA Key length:	2048 bits

OCSP2

CN:	Servicio OCSP2 vinCAsign
Fingerprint:	25B071CB4788E7EA4535C3B84FF198347EA2E4C3
Issuance date:	2023-09-04 11:06:46+02:00
Expiration date:	2024-09-03 11:06:46+02:00
RSA Key length:	2048 bits

1.3.1.1.7. OCSF service for vinCAsign nebulaSUITE4 (discontinued)

The signing certificate of the new VinCAsign OCSF services responses has been digitally signed by the "VinCAsign nebulaSUITE4 Authority".

Identification data:

OCSP1

CN:	Servicio OCSP1 vinCAsign nebulaSUITE4
Fingerprint:	E7E80DD372A469D29BD538F1077D9D6DB2168C59
Issuance date:	2022-06-22 08:05:53+02:00
Expiration date:	2023-06-22 08:05:53+02:00
RSA Key length:	2048 bits

OCSP2

CN:	Servicio OCSP2 vinCAsign nebulaSUITE4
Fingerprint:	FDAC2E62DF21C76195A3031318DF7D00ADBA2EC2
Issuance date:	2022-06-22 08:02:53+02:00
Expiration date:	2023-06-22 08:02:53+02:00
RSA Key length:	2048 bits

As its Certification Authority has been discontinued, the OCSP service has been disabled for the CA "vinCAsign nebulaSUITE 4".

1.3.1.1.8. OCSP service for vinCAsign nebulaSUITE5 (discontinued)

The signing certificate of the new VinCAsign OCSP services responses has been digitally signed by the "VinCAsign nebulaSUITE5 Authority".

OCSP1

CN:	Servicio OCSP1 vinCAsign nebulaSUITE5
Fingerprint:	BC71BE413321689B01B2FA651485B301284499DE
Issuance date:	2022-09-27 09:57:32+02:00
Expiration date:	2023-09-27 09:57:32+02:00
RSA Key length:	2048 bits

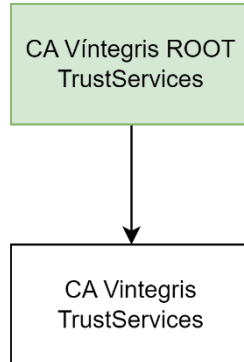
OCSP2

CN:	Servicio OCSP2 vinCAsign nebulaSUITE5
Fingerprint:	EF5247E09419426E872F16A47352308DDC938078
Issuance date:	2022-09-27 10:13:39+02:00
Expiration date:	2023-09-27 10:13:39+02:00
RSA Key length:	2048 bits

As its Certification Authority has been discontinued, the OCSP service has been disabled for the CA "vinCAsign nebulaSUITE 5".

1.3.1.2. CA Vintegris ROOT TrustServices hierarchy

In addition, Vintegris SLU has established a new hierarchy of Certification Authorities called “CA Vintegris TrustServices”:



1.3.1.2.1. CA Vintegris ROOT TrustServices

This is the **Root Certification Authority** in the hierarchy that issues certificates to other certification authorities, and which public key certificate has been self-signed.

Identification data:

CN:	CA Vintegris ROOT TrustServices
Fingerprint:	50117bbbe186a3d1082a2f1391fd4e4c9615d8b4
Issuance date:	Monday, January 22nd 2022 13:11:29
Expiration date:	Friday, January 18th 2047 13:11:28
RSA Key length:	4096

1.3.1.2.2. CA Vintegris TrustServices

It is a **Subordinate Certification Authority** within the hierarchy that issues certificates to end entities, and which public key certificate has been digitally signed by the CA Vintegris ROOT TrustServices.

Identification data:

CN:	CA Vintegris TrustServices
Fingerprint:	f785b43173431b5fa8406153a2aa19380e1d0434
Issuance date:	Monday, January 24th 2022 14:09:20
Expiration date:	Thursday, January 22nd 2032 14:09:19
RSA Key length:	4096 bits

1.3.1.2.3. CA Vintegris SSL TrustServices (withdrawn)

It is a **withdrawn Subordinate Certification Authority** intended exclusively for the issuance of qualified certificates of the web authentication certificate issuance service, and which public key certificate has been digitally signed by the CA Vintegris ROOT TrustServices.

Identification data:

CN:	CA Vintegris SSL TrustServices
Fingerprint:	62f4082af79c7833b1f9647f73923d97e48fdd12
Issuance date:	Monday, January 24th 2022 14:31:48
Expiration date:	Thursday, January 22nd 2032 14:31:47
RSA Key length:	4096

1.3.1.2.4. OCSP service for CA Vintegris TrustServices

The signing certificate of the OCSP service validation responses for certificates issued by the CA Vintegris TrustServices has been digitally signed by the "CA Vintegris TrustServices".

Identification data:

OCSP1

CN:	CA Vintegris OCSP1 TrustServices
Fingerprint:	4D67C3E521F81560A4ED860D775538D39DC68CD9
Issuance date:	2025-01-07 10:42:58+01:00
Expiration date:	2026-01-07 10:42:57+01:00

RSA Key length:	4096 bits
-----------------	-----------

OCSP2

CN:	CA Vintegris OCSP2 TrustServices
Fingerprint:	0C308DB9674C06437AD48E283F9272F3A9588528
Issuance date:	2025-01-07 10:45:16+01:00
Expiration date:	2026-01-07 10:45:15+01:00
RSA Key length:	4096 bits

1.3.1.2.5. OCSP service for CA Vintegris SSL TrustServices

The signing certificate of the OCSP service validation responses for certificates issued by the CA Vintegris TrustServices has been digitally signed by the "CA Vintegris SSL TrustServices".

Identification data:

OCSP1

CN:	CA Vintegris OCSP1 SSL TrustServices
Fingerprint:	3463742050BDE6F03943242AFB10B2DAB79AFEFB
Issuance date:	2022-02-16 13:04:03 CET
Expiration date:	2023-02-16 13:04:03 CET
RSA Key length:	4096 bits

OCSP2

CN:	CA Vintegris OCSP2 SSL TrustServices
Fingerprint:	AAF1973297830A0D9B44A9BDB480D539C6B6C62C
Issuance date:	2022-02-16 13:10:10 CET
Expiration date:	2023-02-16 13:10:10 CET
RSA Key length:	4096 bits

As its Certification Authority has been discontinued, the OCSP service has been disabled for the CA "CA Vintegris SSL TrustServices".

1.3.1.3. nebulaSUITE

Centralized certificate management platform for the following uses:

- Certificate requests and approvals management
- Certificate requests management
- Certificate renewal and revocation requests management

More information about the nebulaSUITE platform can be found at <https://vintegris.com/digital-identity-solution-nebulasuite/>.

This platform uses an HSM "nShield Connect XC" v12.60.15 which is certified according to Common Criteria EAL4 + AVA_VAN.5 as a qualified signature or electronic seal creation device (QSCD), and a SAM "Entrust Signature Activation Module" v1.0.4 as a Signature Activation Module according to Regulation (EU) 910/2014.

1.3.1.4. VinCAsign 2016 Hierarchy (withdrawn)

The initial VinCAsign Hierarchy created in 2016 has been renewed by the one described above.

This hierarchy has been discontinued as of the release date of CPS version v2r6.

1.3.1.4.1. *VinCAsign ROOT Authority (withdrawn)*

This is the root certification authority of the hierarchy that issued certificates to other certification authorities, and which public key certificate has been self-signed.

Identification data:

CN:	vinCAsign Root Authority
Fingerprint:	90 9e 58 84 aa 2f 36 45 78 67 79 05 24 47 79 43 66 6 ^a fd 1c
Issuance date:	Thursday, 28/01/2016
Expiration date:	Thursday, 28/01/2027
RSA Key length:	4096 bits

1.3.1.4.2. *VinCAsign GLOBAL Authority (withdrawn)*

This is the certification authority within the hierarchy that issued the certificates to the end entities, and which public key certificate has been digitally signed by the VinCAsign Root Authority.

Identification data:

CN:	vinCAsign Global Authority
Fingerprint:	ef 29 4b 28 3b 41 5f 7c 8f 10 89 2c f4 56 e8 a6 8c 55 b7 94
Issuance date:	Thursday, 28/01/2016
Expiration date:	Thursday, 28/01/2022
RSA Key length:	4096 bits

1.3.1.4.3. VinCAsign nebulaSUITE Authority (withdrawn)

It is a **Subordinate Certification Authority** within the hierarchy that issued certificates to the final entities, and which public key certificate has been digitally signed by the VinCAsign Qualified Authority.

Identification data:

CN:	vinCAsign nebulaSUITE Authority
Fingerprint:	65 a3 33 88 e0 b9 b4 0a 6d 84 f0 c7 3a af 9c ff f5 c3 b4 0d
Issuance date:	Jueves, 20/04/2017
Expiration date:	Sábado, 20/04/2030
RSA Key length:	4096 bits

1.3.2. Registration Authorities

In general, the Trust Service Provider (TSP) acts as the registrar of the certificate subscriber's identity.

As some of the certificates referred to in this document are considered corporate certificates, there are some additional entities acting as registrars (such as Personnel/HR departments) if they own the authentic records about the company-subscriber's association.

Other entities that have a contract as Registration Entities function as registrars of the so-called "individual" certificates referred to in this document.

Subscriber's registration functions are delegated, according to the instructions of the TSP, the indications of Article 24.1 of EU Regulation 910/2014, and under the full responsibility of the TSP against third parties.

Domain validation is performed by VínTEGRIS and is not delegated to any third party.

1.3.3. Subscribers

The end entities are the persons and organizations recipients of the issuance, management and use services of the digital certificates, suitable for identification and electronic signature.

The following are considered as end entities of VínTEGRIS certification services:

1. Certificate applicants
2. Certification service subscribers
3. Signatories.

1.3.3.1. Certificate applicants

They are those natural persons who, in their own name or on behalf of a third party, request the issuance of a certificate.

Depending on the certificate applied for, the applicant must meet the requirements set out in section 4.1 of this document.

1.3.3.2. Certification service subscribers

The subscribers of the certification service are the companies, entities or organizations that acquire a certificate from VinCAsign to be used in their corporate or organizational environment and are identified in the certificates.

The subscriber of the certification service acquires a license to use the certificate for its own use -electronic seal certificates-, or to facilitate the certification of the identity of a specific person duly authorized for various actions in the subscriber's organization -electronic signature certificates-. In the latter case, this person is identified in the certificate, as provided in the following section.

Therefore, the subscriber of the certification service is the client of the certification service provider, in accordance with commercial law, and has the rights and obligations defined by the Trust Service Provider, which are additional to and without prejudice to

the rights and obligations of the signatories, as authorized and regulated in the European technical standards applicable to the issuance of qualified electronic certificates, in particular ETSI EN 319 411-2, sections 5.4.2 and 6.3.4.

1.3.3.3. Signatories

Signatories are the natural persons who have under their sole control the digital signature keys for identification and advanced or qualified electronic signature; being typically the employees, customers and other persons linked to the subscribers (in case of certificates of natural person), the legal representatives and volunteers (in case of certificates of representative), or the persons in the service of the Public Administrations (in case of certificates of public employee).

Signatories are duly authorized by the subscriber and duly identified in the certificate by their name and surname, and their valid tax identification number (in the jurisdiction of issuance of the certificate), not being allowed the use of pseudonyms in general.

Signatories' private key cannot be recovered by the certification service provider because the identified natural or legal person has sole control over it.

Due to the existence of different certificate usages rather than for electronic signatures, such as identification, the more generic term "natural person identified in the certificate" is also used, always regarding with electronic signature legislation in relation to the rights and obligations of the signatory.

1.3.4. Relying parties

Relying parties are individuals and organizations that receive digital signatures, electronic seals, and digital certificates.

Previously trusting on the certificates, these parties must verify them, as established in this Certification Practice Statement and in the corresponding instructions available on the Certification Authority website: <https://www.VinCAsign.net> and in the disclosed texts issued for each type of certificate (PKI Disclosure Statement -PDS)

1.3.5. Other participants

Not stipulated.

1.4. Certificate Usage

This section lists the applications for which each type of certificate can be used, establishes limitations to certain applications and prohibits certain applications of the certificates.

1.4.1. Appropriate Certificate Uses

The allowed usage of the certificates (specified in the fields defined by the certificate profile) must be considered. Full details available in <https://www.vincasign.net>.

1.4.1.1. Corporate certificates for natural persons (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.1	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.1.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates work with qualified signature creation devices, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are centrally managed or issued on cryptographic cards.

These certificates guarantee the identity of the signatory and its link with the subscriber of the certification service, and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

- a) Website authentication.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows the following functions to be performed:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.2. Corporate certificates for natural persons (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.2	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.1.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the person indicated in the certificate, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

The certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform:
 - a. Digital signature (to carry out the authentication function).
 - b. Commitment to the content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:

- a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.3. Ephemeral corporate certificates for natural persons (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.51	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.1.51	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation devices, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are centrally managed.

These certificates guarantee the identity of the signatory and its link with the subscriber of the certification service, and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows the following functions to be performed:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.4. Ephemeral corporate certificates for natural persons (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.1.52	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.1.52	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and of the person indicated in the certificate and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

Certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to the content (to perform the electronic signature function).

- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field **does not contain** the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.5. Certificates for natural person representative of a Legal Entity (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.1	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.8	A certificate as a representative of a legal entity, with full powers, sole or joint administrator of the organization, or at least with specific general powers to act to the Spanish Public Administrations.

These certificates are managed centrally or issued on a cryptographic card.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the field "O" (Organization), and allow the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated

using a qualified device, whereby in accordance with the provisions of Article 25. 2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's authority to act on behalf of the entity he/she represents and, if mandatory, the registration of the registry data.

They can also be used in applications that do not require the electronic signature equivalent to the written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages.

In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.6. Certificates for natural person representative of a Legal Entity (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.2	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.8	A certificate as a representative of a legal entity, with full powers, sole or joint administrator of the organization, or at least with specific general powers to act to the Spanish Public Administrations.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the "O" (Organization) field and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's authority to act on behalf of the entity he/she represents and, if mandatory, the registration of the registry data.

On the other hand, the corporate certificates of representative natural person issued in software can be used in other applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.7. Ephemeral certificates for natural person representative of a Legal Entity (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.51	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.51	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.8	A certificate as a representative of a legal entity, with full powers, sole or joint administrator of the organization, or at least with specific general powers to act to the Spanish Public Administrations.

These certificates are managed centrally or issued on a cryptographic card.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the field "O" (Organization), and allow the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25. 2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's authority to act on behalf of the entity he/she represents and, if mandatory, the registration of the registry data.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages.

In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b) Commitment to content (to perform the electronic signature function).
- c) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- d) The "User Notice" field describes the use of this certificate

1.4.1.8. Ephemeral certificates for natural person representative of a Legal Entity (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.52	In the CA vinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.52	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.8	A certificate as a representative of a legal entity, with full powers, sole or joint administrator of the organization, or at least with specific general powers to act to the Spanish Public Administrations.

These certificates are centrally managed.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the "O" (Organization) field and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

This certificate includes a field (Description) in the Subject where the public document that reliably certifies the signatory's powers to act on behalf of the entity, he/she represents is indicated and, if mandatory, the registration of the registry data.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

On the other hand, the corporate certificates of natural person representative issued in software can be used in other applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.9. Certificates of natural person representative of an entity without legal personality (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.11	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.11	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.9	For being a certificate of representative of an entity without legal personality, in which the Representative has full capacity to act on behalf of the Entity without Legal Personality to the Public Administrations ² .

These certificates are managed centrally or issued on a cryptographic card.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's powers to act on behalf of the unincorporated entity he/she represents and, if mandatory, the registration of the registry data.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity without legal personality described in the field "O" (Organization), and allow the generation of the "qualified electronic signature" i.e. the advanced electronic

² In accordance with point 14.1.3.1 of the document "Perfiles de Certificados Electrónicos" of the Spanish Ministry of Finance and Public Administrations (April 2016)

signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25. 2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages.

In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate

1.4.1.10. Certificates of natural person representative of an entity without legal personality (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.12	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.12	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.9	For being a certificate of representative of an entity without legal personality, in which the Representative has full capacity to act on behalf of the Entity without Legal Personality to the Public Administrations.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's powers to act on behalf of the unincorporated entity he/she represents and, if mandatory, the registration of the registry data.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity without legal personality described in the "O" (Organization) field, and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

These certificates can be used in other applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate

1.4.1.11. Ephemeral certificates of natural person representative of an entity without legal personality (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.151	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.151	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.9	For being a certificate of representative of an entity without legal personality, in which the Representative has full capacity to act on behalf of the Entity without Legal Personality to the Public Administrations.

These certificates are centrally managed.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's powers to act on behalf of the unincorporated entity he/she represents and, if mandatory, the registration of the registry data.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity without legal personality described in the field "O" (Organization), and allow the generation of the "qualified electronic signature" i.e. the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25. 2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages.

In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.12. Ephemeral certificates of natural person representative of an entity without legal personality (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.2.152	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.2.152	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.9	For being a certificate of representative of an entity without legal personality, in which the Representative has full capacity to act on behalf of the Entity without Legal Personality to the Public Administrations5.

These certificates are centrally managed.

This certificate includes a field (Description) in the Subject indicating the public document that reliably certifies the signatory's powers to act on behalf of the unincorporated entity he/she represents and, if mandatory, the registration of the registry data.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity without legal personality described in the "O" (Organization) field, and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

These certificates can be used in other applications such as those listed below:

- a) Authentication in access control systems.

- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.13. Corporate certificates for Spanish public employees (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.1	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.4.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.7.1	which indicates that it is a Spanish public employee high-level certificate (QSCD)

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are managed centrally or issued on a cryptographic card.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, linking them to it, fulfilling the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of Public Administrations.

The certificates of natural person public employee high level, work with qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July 2014.

Likewise, the certificates of natural person public employee high level are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles" of the Subdirectorate General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and the signatory, and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions enabled and therefore allows the following functions to be performed:
 - a. Digital signature (to perform authentication)
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.14. Corporate certificates for Spanish public employees (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.2	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.4.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.7.2	which indicates that it is a Spanish public employee medium-level certificate (software)

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, linking them to the latter, complying with the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of the Public Administrations.

These certificates do not work with a qualified signature creation device.

The certificates of natural person public employee medium level are issued in accordance with the medium assurance levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles" of the Subdirectorato General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and of the person indicated in the certificate and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified. The "Qualified Certificate Statements" field does not contain the statement QcSSCD (0.4.0.1862.1.4), since this certificate is not used with a qualified device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.15. Corporate certificates for Spanish public employees with pseudonym (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.11	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.4.11	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd
2.16.724.1.3.5.4.1	which indicates that it is a Spanish public employee with pseudonym high-level certificate (QSCD)

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, linking them to the latter, complying with the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of the Public Administrations.

These certificates, due to privacy and security reasons, do not include the public employee's personal data, such as ID card number, Name and Surname. Instead, a pseudonym that corresponds to the employee's professional identification number is included.

VinCAsign stores in a strictly confidential manner, the real identity of the signatory.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

Likewise, these certificates are issued in accordance with the high assurance levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles"

of the Subdirectorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and the signatory, and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require an electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions enabled and therefore allows the following functions to be performed:
 - a. Digital signature (to perform authentication)
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.16. Corporate certificates for Spanish public employees with pseudonym (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.4.12	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.4.12	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n
2.16.724.1.3.5.4.2	which indicates that it is a Spanish public employee with pseudonym medium-level certificate (software)

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are issued to public employees to identify them as persons in the service of the Public Administration, linking them to the latter, complying with the requirements established in Article 43 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, for the electronic signature of personnel in the service of the Public Administrations.

These certificates, due to privacy and security reasons, do not include the public employee's personal data, such as ID card number, Name and Surname. Instead, a pseudonym that corresponds to the employee's professional identification number is included.

VinCAsign stores in a strictly confidential manner, the real identity of the signatory.

These certificates do not work with a qualified signature creation device.

The certificates of natural person public employee medium level are issued in accordance with the medium assurance levels of the certificate profiles established in point 10 of the document "Electronic Certificate Profiles" of the Subdirector General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and of the person indicated in the certificate and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the statement QcSSCD (0.4.0.1862.1.4), since this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.17. Electronic seal certificates for the Spanish public administration bodies (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.5.1	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.5.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.3	According ETSI policy QCP-I-qscd
2.16.724.1.3.5.6.1	That indicates that it is an electronic seal high-level certificate (QSCD) of a Spanish Public Administration body.

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates are issued for the identification and authentication of the exercise of competence in automated administrative action in accordance with Article 42 of Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

These certificates are issued in accordance with the high assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Subdirectorate General of Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the Public Body subscribing the certification service, and allow the generation of the "**qualified electronic seal**"; that is, the advanced electronic seal that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will enjoy

the presumption of integrity of the data and the correctness of the origin of the data to which the qualified electronic seal is linked.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows the following functions to be performed:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.18. Electronic seal certificates for the Spanish public administration bodies (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.5.2	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.5.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.1	According ETSI policy QCP-I
2.16.724.1.3.5.6.2	That indicates that it is an electronic seal medium-level certificate (software) of a Spanish Public Administration body.

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are issued for the identification and authentication of the exercise of competence in automated administrative action in accordance with 42 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

These certificates do not work with a qualified signature creation device.

These certificates are issued in accordance with the average assurance levels of the certificate profiles established in point 9 of the document "Electronic Certificate Profiles" of the Subdirectorate General for Information, Documentation and Publications of the Ministry of Finance and Public Administrations.

These certificates guarantee the identity of the subscriber and the public body included in the certificate.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:

- a. Digital signature (to perform the authentication function).
- b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.19. Electronic seal certificate for private entities (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.1	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.6.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.3	According ETSI policy QCP-l-qscd

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber of the certification service, and allow the generation of the "qualified electronic seal"; that is, the advanced electronic seal that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will enjoy the presumption of integrity of the data and the correctness of the origin of the data to which the qualified electronic seal is linked.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:

- a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as recognized.
- b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.20. Electronic seal certificate for private entities (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.2	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.6.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.	According ETSI policy QCP-I

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and of the company or entity included in the certificate.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.21. Ephemeral electronic seal certificate for private entities (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.51	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.6.51	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.3	According ETSI policy QCP-I-qscd

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber of the certification service, and allow the generation of the "qualified electronic seal"; that is, the advanced electronic seal that is based on a qualified certificate and that has been generated employing a qualified device, whereby in accordance with the provisions of Article 35.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall enjoy the presumption of integrity of the data and the correctness of the origin of the data to which the qualified electronic seal is linked.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).

- b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as recognized.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.22. Ephemeral electronic seal certificate for private entities (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.6.52	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.6.52	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.1	According ETSI policy QCP-I

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and of the company or entity included in the certificate.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.

d) The "User Notice" field describes the use of this certificate.

1.4.1.23. Non-qualified electronic seal certificate for private entities

This certificate has the following OIDs:

1.3.6.1.4.1.47155.2.6.3	in the CA Vintegris TrustServices Certification Hierarchy
-------------------------	-----------------------------------------------------------

These certificates are qualified in accordance with Article 36 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber, the company or entity and the technical identification of the thing where it is located, included in the certificate.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) The "Qualified Certificate Statements" field does not appear in the certificate.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.24. Electronic seal certificate for IoT

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.7.2	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.7.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.1	According ETSI policy QCP-I

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber, the company or entity and the technical identification of the thing where it is located, included in the certificate.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.25. Non-qualified electronic seal certificate for IoT

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.7.62	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.7.62	in the CA Vintegris TrustServices Certification Hierarchy

These certificates are qualified in accordance with Article 36 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber, the company or entity and the technical identification of the thing where it is located, included in the certificate.

These certificates do not allow the encryption of documents, contents, or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- d) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Content commitment (to perform the electronic signature function).
- e) The "Qualified Certificate Statements" field does not appear in the certificate.
- f) The "User Notice" field describes the use of this certificate.

1.4.1.26. Electronic time stamp certificate

This certificate has the following OIDs:

1.3.6.1.4.1.47155.2.9.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.1	According ETSI policy QCP-I

These certificates are qualified in accordance with Article 38 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

This certificate allows Time Stamping Units or TSUs to issue time stamps when they receive a request under the specifications of RFC3161.

The keys are generated in support of a qualified device (QSCD).

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Content Commitment
- b) The "extend key usage" field has the function activated:
 - a. TimeStamping
- c) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.27. Individual certificates for natural persons (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.1	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.10.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates, operate with qualified signature creation device, in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are centrally managed.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without linkage to any entity and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows the following functions to be performed:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.28. Individual certificates for natural persons (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.2	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.10.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without being linked to any entity, and allow the generation of the "advanced electronic signature based on qualified electronic certificate".

The certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to the content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:

- a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.29. Ephemeral individual certificates for natural persons (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.51	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.10.51	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates are centrally managed.

These certificates guarantee the identity of the individual holder (being the same person the signatory and subscriber) without linkage to any entity, and allow the generation of the "qualified electronic signature"; that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25.2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it will have a legal effect equivalent to that of a handwritten signature.

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows the following functions to be performed:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) The following statement appears in the "Qualified Certificate Statements" field:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.30. Ephemeral Individual certificates for natural persons (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.10.52	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.10.52	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates are centrally managed.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the individual holder (as the signatory and subscriber are the same person) without any link to any entity and allow the generation of the "advanced electronic signature based on a qualified electronic certificate".

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

Certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to the content (to perform the electronic signature function).

- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.1.31. Individual non-qualified certificates for natural persons

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.110.1	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.110.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.2042.1.3	According LCP

These certificates are not qualified (according to the European Regulation), but are compliant with the LCP policy (as determined by the technical norm ETSI EN 319 411-1)

These certificates are centrally managed.

These certificates do not work with a qualified signature creation device.

Certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).

b. Commitment to the content (to perform the electronic signature function).

b) These certificates do not have the “Qualified Certificate Statements”

1.4.1.32. Ephemeral individual non-qualified certificates for natural persons

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.110.51	In the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.110.51	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.2042.1.3	According LCP

These certificates are valid only for ephemeral use for a short period of time, after which the certificate expires. This period of time is maximum 72 hours.

These certificates are not qualified (according to the European Regulation), but are compliant with the LCP policy (as determined by the technical norm ETSI EN 319 411-1)

These certificates are centrally managed.

These certificates do not work with a qualified signature creation device.

Certificates can be used in applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications, in accordance with what the parties agree or with the legal regulations applicable in each case.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to the content (to perform the electronic signature function).
- b) These certificates do not have the “Qualified Certificate Statements”

1.4.1.33. Certificates for natural person representative of an Italian Legal Entity - AGID- (QSCD)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.11.1	in the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.11.1	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.2	According ETSI policy QCP-n-qscd

These certificates are centrally managed.

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates operate with qualified signature creation device in accordance with Annex II of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the field "O" (Organization), and allow the generation of the "qualified electronic signature" that is, the advanced electronic signature that is based on a qualified certificate and that has been generated using a qualified device, whereby in accordance with the provisions of Article 25. 2 of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014, it shall have a legal effect equivalent to that of a handwritten signature.

These certificates have been created based on the regulations and recommendations set by the Agency for Digital Italy AGID.

They can also be used in applications that do not require the electronic signature equivalent to a written signature, such as the applications listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages.

In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. qCCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
 - b. QcSSCD (0.4.0.1862.1.4), which informs that the certificate is used exclusively in conjunction with a qualified signature creation device.
- c) The "User Notice" field describes the use of this certificate.

1.4.1.34. Certificates for natural person representative of an Italian Legal Entity - AGID- (Software)

This certificate has the following OIDs:

1.3.6.1.4.1.47155.1.11.2	in the VinCAsign Qualified Authority certification hierarchy
1.3.6.1.4.1.47155.2.11.2	in the CA Vintegris TrustServices Certification Hierarchy
0.4.0.194112.1.0	According ETSI policy QCP-n

These certificates are qualified in accordance with Article 28 and Annex I of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 and comply with the provisions of the technical standard identified by reference ETSI EN 319 411-2.

These certificates do not work with a qualified signature creation device.

These certificates guarantee the identity of the subscriber and the signatory, and a relationship of legal representation or general power of attorney between the signatory and an entity, company or organization described in the "O" (Organization) field, and

allow the generation of the "advanced electronic signature based on qualified electronic certificate".

These certificates have been created based on the regulations and recommendations established by the Agency for Digital Italy AGID.

On the other hand, the corporate certificates of natural person representative issued in software can be used in other applications such as those listed below:

- a) Authentication in access control systems.
- b) Other digital signature applications.

These certificates do not allow the encryption of documents, contents or data messages. In any case, VinCAsign will not be liable for any loss of encrypted information that cannot be recovered.

The usage information in the certificate profile indicates the following:

- a) The "key usage" field has the following functions activated and therefore allows us to perform the following functions:
 - a. Digital signature (to perform the authentication function).
 - b. Commitment to content (to perform the electronic signature function).
- b) In the "Qualified Certificate Statements" field the following statement appears:
 - a. QcCompliance (0.4.0.1862.1.1), which informs that the certificate is issued as qualified.
- c) The "Qualified Certificate Statements" field does not contain the QcSSCD (0.4.0.1862.1.4) statement, as this certificate is not used with a qualified device.
- d) The "User Notice" field describes the use of this certificate.

1.4.2. Certificate prohibited usages

Certificates covered by this document are used for their intended function and purpose and may not be used for other functions and purposes.

Likewise, certificates must only be used in accordance with the applicable law, especially considering the import and export restrictions existing at any given time.

End Entity certificates are not allowed to be used to sign requests for issuance, renewal, or revocation of certificates, or to sign public key certificates of any kind, or to sign certificate revocation lists (CRLs).

The certificates are not designed, intended, and are not authorized for use or resale as hazardous situation monitoring equipment or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly lead to death, personal injury, or severe environmental damage.

The limits indicated in the various fields of the certificate profiles, visible on the VinCAsign website (<https://www.VinCAsign.net>), must be considered.

The use of digital certificates in operations that contravene this CPS, the legal documents binding with each certificate -or the contracts with the registration entities or with their signatories/subscribers-, are considered as disallowed for the appropriate legal purposes, therefore exempting VinCAsign, according to the current legislation, from any liability for this misuse of the certificates made by the signatory or any third party.

VinCAsign does not have access to the data on which the use of a certificate can be applied. Therefore, and because of this technical impossibility to access the content of the message, it is not possible for VinCAsign to make any assessment of such content, and therefore the subscriber, the signatory, or the person responsible for the custody, assumes any liability arising from the content associated with the use of a certificate.

Likewise, the subscriber, the signatory or the person responsible for the custody, shall be responsible for any liability that may arise from the use of the same outside the limits and conditions of use contained in this CPS, the legal documents binding each certificate, or the contracts or agreements with the registration entities or with their subscribers, as well as any other misuse of the same derived from this section or that may be interpreted as such according to the legislation in force.

1.5. Policy administration

1.5.1. Organization Administering the Document

VÍNTEGRIS SLU (vinCAsign)

Carrer Pallars, 99

Planta 3, Oficina 33

08018 Barcelona

Tel.: (+34) 934 329 098

Fax. +34 934 329 344

1.5.2. CPS approval procedures

VÍNTEGRIS SLU (vinCAsign)

Carrer Pallars, 99

Planta 3, Oficina 33

08018 Barcelona

Tel.: (+34) 934 329 098

Fax. +34 934 329 344

Complaints and suggestions and key compromise or misuse of the certificate:

- By phone: +34 93 432 90 98,
- By email: info@VinCAsign.net
- Contact form available at <https://www.VinCAsign.net> (“Help” section)

1.5.3. Person Determining CPS suitability for the policy

This CPS will be reviewed and updated annually by VinCAsign.

1.5.4. Procedimientos de aprobación de la DPC

VinCAsign document and organization system ensures, through the existence and application of the corresponding procedures, the correct maintenance of this document and related service specifications.

The procedure for review and approval of changes to this CPS is detailed in the internal documentation (VinCAsign Gestión Políticas v1r1.pdf).

VinCAsign has an Information Security Policy that is kept up to date and reviewed annually.

This CPS will be reviewed and updated at least annually by VinCAsign, or more often whenever there is any change of conditions, technical or legislative or any other by which it may be affected.

1.6. Definitions and Acronyms

1.6.1. Definitions

Activation Data	Private data, in order to activate the private key, i.e. passwords or PIN codes.
Applicant	In this document's context, the applicant will be a natural person, with a power of attorney in order to perform certain procedures on behalf of a legal entity, or himself for individual certificates or web authentication certificates.
Authentication	Electronic process that enables electronic identification of a natural or legal person, or origin and integrity of the data, in electronic format.
CPS	Certification Practice Statement, it is a set of practices adopted by a Certification Authority for the issuance of certificates in accordance with a specific certification policy.
CRL	Certificate Revocation List, it is a file that contains a list of the certificates that have been revoked in a given period of time, and that's signed by the CA.
Certificate	Digital file which associates the public key with some form of identification data of the subject/signer and that is signed by a certification authority.
Certification Authority	Entity responsible for issuance and manager of digital certificates.

Digital Signature	<p>Outcome transformation of a message, or any type of data, by applying the private key in conjunction with known algorithms, thus guaranteeing:</p> <p>a) The data has not been modified (integrity).</p> <p>b) The person signing the data is who they say they are (identification).</p> <p>c) The person signing the data cannot deny having done so (non-repudiation at source).</p>
Electronic Identification	<p>It is the process of using a person's identification data in electronic form, that uniquely represents a natural or legal person or its representative.</p>
Electronic identification means	<p>Material and/or immaterial unit that contains a person's identification data and is used for authentication in online services.</p>
Key pair	<p>Set formed by the public and the private keys, both related one another mathematically.</p>
OID	<p>Unique numeric identifier registered under the ISO standardization and referred to a specific object, or class of object.</p>
PKI	<p>Public Key Infrastructure, set of hardware, software, human resources, procedures, etc. elements that constitutes a system based on the creation and management of public key certificates.</p>
Private key	<p>Mathematical value only known to the Subject/Signer and used for the creation of a digital signature or data decryption.</p> <p>The private key of the CA will be used for signing certificates and signing CRLs.</p>
Public key	<p>A publicly known mathematical value used for verification of a digital signature or data encryption.</p>

QSCD	Qualified signature creation device, it is a software or hardware element, conveniently certified, used by the in orde to generate electronic signatures, so that cryptographic operations are carried out within the device and its control is guaranteed only by the Subject/Signer.
Qualified Electronic Seal/Signature Creation Device (QSCD)	Signature creation device that meets requirements of Annex II of Regulation (EU) No 910/2014.
Registry Authority	Entity responsible for the management of applications, identification and registration of applicants for a certificate. It can be part of the Certification Authority or be external.
Subject/Signer	In this document's context, it is the natural person whose public key is certified by the CA, and has exclusive access to a valid private key in order to generate digital signatures.
Subscriber	In this document's context, it is the legal entity that owns the certificate, at a corporate level, or the natural person in individual certificates.
User Part	In this document's context, it is a person who voluntarily trust the digital certificate, and uses it as means of proving the authenticity and integrity of the signed document. Relying parties for web authentication are both, client applications users and SSL/TLS services that connect to websites.

1.6.2. Acronyms

CA	<i>Certificate Authority.</i>
CPS	<i>Certification Practice Statement.</i>
CRL	<i>Certificate Revocation List.</i>
DN	<i>Distinguished Name.</i>

DPS	<i>Data Processing Centre.</i>
ETSI EN	<i>European Telecommunications Standards Institute – European Standard.</i>
FIPS	<i>Federal Information Processing Standard Publication.</i>
HSM	<i>Hardware Security Module.</i>
IETF	<i>Internet Engineering Task Force.</i>
NID	<i>National ID Document.</i>
NTP	<i>Network Time Protocol.</i>
OCSP	<i>On-line Certificate Status Protocol.</i>
OID	<i>Object Identifier.</i>
PDS	<i>PKI Disclosure Statements.</i>
PIN	<i>Personal Identification Number.</i>
PKCS#10	<i>Universally accepted standard developed by RSA Labs that defines the syntax of a certificate request.</i>
PKI	<i>Public Key Infrastructure.</i>
QCP	<i>Qualified Certificate Policy.</i>
QCP-I	<i>Policy for EU qualified certificate issued to a legal person.</i>
QCP-I-qscd	<i>Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD.</i>
QCP-n	<i>Policy for EU qualified certificate issued to a natural person.</i>
QCP-n-qscd	<i>Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD.</i>
QCP-w	<i>Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person.</i>
QSCD	<i>Qualified Electronic Signature/Seal Creation Device.</i>
RA	<i>Registration Authority.</i>

RFC	<i>Request for Comments.</i>
RSA	<i>Rivest-Shimar-Adleman.</i>
SEPBLAC	<i>Executive Service of the Commission for the Prevention of Money Laundering and Monetary Infractions (Sepblac in <u>spanish</u>).</i>
SHA	<i>Secure Hash Algorithm.</i>
SSL	<i>Secure Sockets Layer, protocol designed by Netscape and converted into a network standard, allows the transmission of encrypted information between an Internet browser and a server.</i>
TCP/IP	<i>Transmission Control. Protocol/Internet Protocol. System of protocols, defined within the framework of the IETF.</i>
TIN	<i>Tax ID Number.</i>
UTC	<i>Coordinated Universal Time.</i>
VPN	<i>Virtual Private Network.</i>

2. Publication and Repository Responsibilities

2.1. Repositories

VinCAsign has a certificate repository, in which information related to the certification services is published.

Said service is available 24 hours a day, 7 days a week and, in the event of a system failure beyond the control of vinCAsign, it will make its best efforts to make the service available, again within the period established in the section 5.7.4 of this CPS.

2.2. Publication of information

VinCAsign publishes the following information, in its repository:

- Certificates issued when the consent of the natural person identified in the certificate has been obtained.
- The lists of revoked certificates (CRL) and other information related to the revocation status of the certificates.
- Certification Practices Statement (CPS).
- PKI Disclosure Statements (PDS), at least in English.

In addition to what is specified in this CPS, vinCAsign has test websites, that allows application providers to test their software against web authentication certificates:

- VinCAsign Qualified Authority Hierarchy
Valid: <https://valid.vincasign.net>
Revoked: <https://revoked.vincasign.net>
Expired: <https://expired.vincasign.net>
- Vintegris ROOT TrustServices Hierarchy:
Valid: <https://valid.trustservices.vincasign.net/>
Revoked: <https://revoked.trustservices.vincasign.net/>
Expired: <https://expired.trustservices.vincasign.net/>

2.3. Time or frequency of publication

Certification service provider information, including disclosure texts and the CPS, is published as soon as it becomes available.

Changes in the CPS are governed by the provisions of the section 1.5 of this document. These changes will be published on the VinCAsign website (<https://www.vincasign.net>) and updated in the Common CA Database (CCADB) within a maximum of 7 days after the changes are published.

Certificate revocation status information is published in accordance with the provisions of sections 4.9.7 and 4.9.8 of this CPS.

2.4. Access controls on repositories

VinCAsign does not limit read access to the information set out in section 2.2, but establishes controls to prevent unauthorized users from adding, modifying, or deleting records from the repository, to protect integrity and authenticity of the information, especially revocation status information.

VinCAsign uses reliable systems for the repository, in such a way that:

- Only authorized personnel can modify the site.
- Information authenticity can be proved.
- Certificates are only available if the natural person identified in the certificate data has given consent.
- Any technical change which affects security requirements can be detected.

Likewise, audits required by the CA/B Forum Baseline Requirements document, as well as their certifications, will be published in public repositories.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

All certificates contain a differentiated X.500 name in the Subject field, including a Common Name (CN=) component, relating to the identity of the subscriber and the natural person identified in the certificate, as well as various additional identity information in the certificate SubjectAlternativeName field.

As specified in the applicable technical standards (ETSI EN 319 412-2 for natural persons and ETSI EN 319 412-3 for legal persons), the following DistinguishedName (DN) fields in the certificate exceed the size limit of the technical standard RFC 5280:

- commonName: 128 characters
- givenName: 64 characters
- surname: 64 characters
- pseudonym: 100 characters
- organizationName: 128 characters
- organizationalUnitName: 192 characters

A maximum of 600 characters is set for the total length of the DN.

The names contained in the certificates are as follows.

3.1.1.1. Natural person corporate certificates

- Issued in QSCD, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.1.1
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.1.1
- Issued in SOFT, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.1.2
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.1.2
- Issued in QSCD and ephemeral, OIDs:

- VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.1.51
- Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.1.51
- Issued in SOFT and ephemeral, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.1.52
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.1.52

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Signer affiliated organization.
Organizational Unit (OU)	Department in the Organization to which the signer is affiliated, or other information about the Organization.
Organizationidentifier	TIN of the legal entity to which it is affiliated in ETSI EN 319 412-1 format (I.e.: "VATES-Q0000000J")
Surname	Surname.
Given Name	First name.
Title	Position / others.
Serial Number	NID.
Common Name (CN)	Name, surname, and number of the natural person.

3.1.1.2. Natural person corporate certificates representing a legal entity

- Issued in QSCD, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.1
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.1
- Issued in SOFT, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.2
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.2
- Issued in QSCD and ephemeral, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.51
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.51
- Issued in SOFT and ephemeral, OIDs:

- VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.52
- Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.52

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Signer affiliated organization.
Organizational Unit (OU)	Notes on representation.
Organizationidentifier	Legal entity represented's TIN, in ETSI EN 319 412-1 format (I.e.: "VATES-Q0000000J")
Surname	Representative surname (NID).
Given Name	Representative first name (NID).
Title	Position or function regarding their representation.
Serial Number	Holder's NID number, or coding according to ETSI EN 319 412-1 (I.e., "IDCES-123456789Z").
Common Name (CN) ³	I.e.: "00000000T Ricardo Ribes (R: Q0000000J)"
Description	<ul style="list-style-type: none"> • Reg: XXX /Sheet: XXX /Volume:XXX /Section:XXX /Book:XXX / Folio:XXX /Date: dd-mm-yyyy /Inscription: XXX • Notary: Name Surname1 Surname2 /Protocol Number: XXX /Date Granted: dd-mm-yyyy • Official Bulletins: Boletín: XXX/ /Fecha: dd-mm-yyyy /Número de Resolución: XXX

3.1.1.3. Natural person corporate certificates representing a legal entity without legal personality

- Issued in QSCD, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.11
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.11

³ According to the proposal of section 14.1.3.3 (coding of the Common Name attribute) of the document "Electronic certificate profiles (April 2016)" of the Ministry of Finance and Public Administrations: NID, Name and Surname, (R:" NID of the represented company ").

- Issued in SOFT, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.12
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.12
- Issued in QSCD and ephemeral, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.151
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.151
- Issued in SOFT and ephemeral, OIDs:
 - VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.2.152
 - Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.152

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Entity without legal personality that the signatory represents.
Organizational Unit (OU)	Notes on representation.
Organizationidentifier	Legal entity represented's TIN, in ETSI EN 319 412-1 format (I.e.: "VATES-Q0000000J")
Surname	Representative surname (NID).
Given Name	Representative first name (NID).
Title	Position or function regarding their representation.
Serial Number	Holder's NID number, or coding according to ETSI EN 319 412-1 (I.e., "IDCES-123456789Z").
Common Name (CN) ⁴	I.e.: "00000000T Ricardo Ribes (R: Q0000000J)"
Description	Public document coding that accredits the powers of the signatory registration data.

⁴ In accordance with the proposal of section 14.1.3.3 (coding of the Common Name attribute) of the document "Electronic certificate profiles (April 2016)" of the Ministry of Finance and Public Administrations: NID, Name and Surname, (R:" NID of the represented company without legal personality").

3.1.1.4. Certificates for Spanish public employees

- Issued for HIGH level (QSCD), OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.4.1
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.4.1
- Issued for MEDIUM level (SOFTWARE), OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.4.2
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.4.2

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Public Administration in which the signatory provides services.
Organizational Unit (OU)	The unit the signer is assigned.
OrganizationIdentifier	TIN of the public administration, the signer is attached, in format ETSI EN 319 412-1 (I.e.: "VATES-Q0000000J").
Surname	Surname (NID).
Given Name	First name (NID).
Title	Position.
Serial Number	Holder's NID number, or coding according to ETSI EN 319 412-1 (I.e., "IDCES-123456789Z").
Common Name (CN) ⁵	I.e. Name Surname1 Surname2 – NID 00000000G

⁵ Name and two surnames must be entered according to the identity document (NID / Passport), as well as the NID number (see Composition Criteria of the CN field for a public employee of the document "Profiles of Electronic Certificates (April 2016)" of the Ministry of Finance and Public Administration).

OID: 2.16.724.1.3.5.7.1.4 (*high) OID: 2.16.724.1.3.5.7.2.4 (*medium)	Signer's NID number.
OID: 2.16.724.1.3.5.7.1.5 OID: 2.16.724.1.3.5.7.2.5	Persona ID number in the public administration code.
OID: 2.16.724.1.3.5.7.1.6 OID: 2.16.724.1.3.5.7.2.6	Signer's first name.
OID: 2.16.724.1.3.5.7.1.7 OID: 2.16.724.1.3.5.7.2.7	Signer's first surname.
OID: 2.16.724.1.3.5.7.1.8 OID: 2.16.724.1.3.5.7.2.8	Signer's second surname.
OID: 2.16.724.1.3.5.7.1.9 OID: 2.16.724.1.3.5.7.1.9	Signer's email.
Country [C]	I.e., "ES" (subscriber's country).

(* high) The OID branch indicated as 2.16.724.1.3.5.7.1.x corresponds to the High level.

(* medium) The OID branch indicated as 2.16.724.1.3.5.7.2.x corresponds to the medium level.

3.1.1.5. Certificates for Spanish public employees with pseudonym

- Issued for HIGH level, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.4.11
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.4.11
- Issued for MEDIUM level, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.4.12
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.4.12

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Public Administration in which the signatory provides services.
Organizational Unit (OU)	The unit the signer is assigned.
OrganizationIdentifier	TIN of the public administration, the signer is attached, in format ETSI EN 319 412-1 (I.e.: "VATES-Q000000J").
Pseudonym	Signer's pseudonym.
Title	Position.
Common Name (CN) ⁶	Position /"SEUDONIMO" – Registry Public Administration Number – Public Administration Name.
OID: 2.16.724.1.3.5.4.1.2 (*high) OID: 2.16.724.1.3.5.4.2.2 (*medium)	Certificate owner's entity.
OID: 2.16.724.1.3.5.4.1.3 OID: 2.16.724.1.3.5.7.2.3	Entity unique ID number.
OID: 2.16.724.1.3.5.4.1.9 OID: 2.16.724.1.3.5.7.2.9	Contact email.
OID: 2.16.724.1.3.5.4.1.11 OID: 2.16.724.1.3.5.4.2.11	Post held by the certificate subscriber within the administration.
OID: 2.16.724.1.3.5.4.1.12 OID: 2.16.724.1.3.5.4.2.12	Pseudonym.

(* high) The OID branch indicated as 2.16.724.1.3.5.4.1.x corresponds to the High level.

(* medium) The OID branch indicated as 2.16.724.1.3.5.4.2.x corresponds to the Medium level.

⁶ See "Composition Criteria of the CN field for a public employee with a pseudonym" in section 11.1 of the document "Profiles of Electronic Certificates (April 2016)" of the Ministry of Finance and Public Administrations).

3.1.1.6. Electronic seal certificates for the Spanish public administration bodies

- Issued for HIGH level, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.5.1
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.5.1
- Issued for MEDIUM level, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.5.2
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.5.2

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Seal's Public Administration.
Surname	Surnames of the holder of the administrative body to which the seal belongs.
Given Name	First name of the holder of the administrative body to which the seal belongs.
Common Name	Descriptive name of the system. It shall be ensured that it is convenient and unique.
Serial Number	Public Administration TIN.
OID: 2.16.724.1.3.5.6.1.4 (* high) OID: 2.16.724.1.3.5.6.2.4 (* medium)	NID number of the person responsible for the seal.
OID: 2.16.724.1.3.5.6.1.6 OID: 2.16.724.1.3.5.6.2.6	Name of the person responsible for the seal.
OID: 2.16.724.1.3.5.6.1.7 OID: 2.16.724.1.3.5.6.2.7	First surname of the person responsible for the seal.
OID: 2.16.724.1.3.5.6.1.8 OID: 2.16.724.1.3.5.6.2.8	Second surname of the person responsible for the seal.
OID: 2.16.724.1.3.5.6.1.9 OID: 2.16.724.1.3.5.6.2.9	Email of the person responsible for the seal.

(* high) The OID branch indicated as 2.16.724.1.3.5.6.1.x corresponds to the High level.

(* medium) The OID branch indicated as 2.16.724.1.3.5.6.2.x corresponds to the Medium level.

3.1.1.7. Electronic seal certificate for private entities

- Issued in QSCD, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.6.1
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.6.1
- Issued in SOFT, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.6.2
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.6.2
- Issued in QSCD and ephemeral, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.6.51
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.6.51
- Issued in SOFT and ephemeral, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.6.52
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.6.52

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Official name of legal entity.
organizationIdentifier	TIN of the legal entity to which this seal is linked, in ETSI EN 319 412-1 format.
Serial Number	NID of the legal entity.

3.1.1.8. Electronic seal certificate for IoT

- Issued in SOFT, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.7.2
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.7.2

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Official name of legal entity.
OrganizationUnit (OU)	ID for the thing.
organizationIdentifier	TIN of the legal entity to which this seal is linked, in ETSI EN 319 412-1 format.

Serial Number	TIN of the legal entity.
---------------	--------------------------

3.1.1.9. Non-qualified electronic seal certificate for an IoT device

- Issued in SOFT, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.7.62
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.7.62

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Official name of legal entity.
OrganizationUnit (OU)	ID for the thing.
organizationIdentifier	TIN of the legal entity to which this seal is linked, in ETSI EN 319 412-1 format.
Serial Number	TIN of the legal entity.

3.1.1.10. Electronic time stamp certificates

- Issued in SOFT, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.9.1

Country [C]	I.e., "ES" (subscriber's country).
Organization (O)	Official name of legal entity.
organizationIdentifier	TIN of the legal entity to which this seal is linked, in ETSI EN 319 412-1 format.
Common Name (CN)	Name of the TSU in the name of which this certificate has been issued.

3.1.1.11. Individual natural person certificate

- Issued in QSCD, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.10.1
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.10.1
- Issued in SOFT, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.10.2
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.10.2

- Issued in QSCD and ephemeral, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.10.51
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.10.51
- Issued in SOFT and ephemeral, OIDs:
 - o VinCAsign Qualified Authority hierarchy: 1.3.6.1.4.47155.1.10.52
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.10.52

Country [C]	I.e., "ES" (subscriber's country).
Surname	Surname.
Given Name	First name.
Serial Number	NID number.
Common Name (CN)	First name, surname and NID number of the subscriber.

3.1.1.12. Certificados individuales de persona física titulada

- Issued in QSCD, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.13.1
- Issued in SOFT, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.13.2

Country [C]	I.e., "ES" (subscriber's country).
Surname	Surname.
Given Name	First name.
Serial Number	NID number.
Common Name (CN)	First name, surname and NID number of the subscriber.
Title	Degree held by the certificate holder
OU	Degree identifier
OI	University center tax identification number (NIF)
O	University issuing the degree

3.1.1.13. Certificados individuales de persona física estudiante

- Issued in QSCD, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.14.1
- Issued in SOFT, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.14.2

Country [C]	I.e., "ES" (subscriber's country).
Surname	Surname.
Given Name	First name.
Serial Number	NID number.
Common Name (CN)	First name, surname and NID number of the subscriber.
OU	Degree identifier
OI	University center tax identification number (NIF)
O	University issuing the degree

3.1.1.14. Certificados individuales de persona física colegiada

- Issued in QSCD, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.150
- Issued in SOFT centralized, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.151
- Issued in SOFT decentralized, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.152
- Issued in SOFT managed, OIDs:
 - o Vintegris ROOT TrustServices CA hierarchy: 1.3.6.1.4.47155.2.2.153

Country [C]	I.e., "ES" (subscriber's country).
Surname	Surname.
Given Name	First name.
Serial Number	NID number.

Common Name (CN)	First name, surname and NID number of the subscriber.
Title	Type of registered or accredited professional
OU	Professional registration number
OU	Name of the organization affiliated with the professional body
O	Name of the professional body
OI	Identifier of the professional body
ST	Province of practice of the certificate holder

3.1.2. Need for names to be meaningful

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

3.1.3. Anonymity or pseudonymity of subscribers

In no case are anonymous certificates issued.

VinCAsign will issue pseudonymous certificates in such a way that the real signer of the certificate can be unequivocally identified.

The fields "pseudonym" and "common Name" of the "subject" of the certificate include the specific references of the pseudonym.

VinCAsign keeps the real identity of the signer confidential.

The pseudonym certificate is not provided by Vintegris to entities, companies, or organizations.

3.1.4. Rules for interpreting various name forms

Name formats will be interpreted in accordance with the legislation of the subscriber's country of establishment, on its own terms.

The "country" field will be that of the subscriber's country, and it will always be Spain in the certificates issued to the Spanish Public Administrations.

The certificate shows the relationship between a natural person and the company, entity, or organization with which it is linked, regardless of the nationality of the natural person. This derives from the corporate nature of the certificate, of which the entity, company or organization is a subscriber, and the individual linked to the person authorized to use it.

In the certificates issued to Spanish subscribers, the "serial number" field must include the NIF of the signatory, for the purpose of accepting the certificate for carrying out procedures with the Spanish Administrations. In the case of certificates with a pseudonym, the "pseudonym" field will be used for identification.

In addition, Vintegris considers the requirements of ISO 9595 (X.500) for the interpretation of the names contained in the certificates, as well as the requirements (Baseline Requirements) of CA/Browser-Forum.

3.1.5. Uniqueness of names

The names of the certificate subscribers will be unique, for each VinCAsign certificate policy.

A subscriber name that has already been used may not be assigned to a different subscriber, a situation that, in principle, should not occur, thanks to the presence of the National Identity Document number, or equivalent, in the name scheme.

A subscriber can request more than one certificate if the combination of the following values in the request is different from a valid certificate:

- Tax Identification Number (TIN) or other legally valid identifier of the natural person, when necessary.
- Tax Identification Number (TIN) or other legally valid identifier of the subscriber, when different from the signatory.
- Certificate Type (Certificate description field).

3.1.6. Recognition, authentication, and role of trademarks

Certificate applicants shall not include names in the applications that may imply infringement, by the future subscriber, of the rights of third parties.

VinCAsign will not be obliged to determine in advance that a certificate applicant has industrial property rights over the name that appears in a certificate application, but rather, in principle, it will proceed to certify it.

Likewise, it will not act as an arbitrator or mediator, nor in any other way should it resolve any dispute concerning the ownership of names of persons or organizations, domain names, trademarks, or commercial names.

However, in the event of receiving a notification regarding a conflict of names, in accordance with the legislation of the country of the subscriber, you may take the pertinent actions aimed at blocking or withdrawing the issued certificate.

In any case, the certification service provider reserves the right to reject a certificate request due to name conflict.

Any controversy or conflict arising from this document will be resolved definitively, through the arbitration of law by an arbitrator, within the framework of the Spanish Court of Arbitration, in accordance with its Regulations and Statute, which is entrusted with the administration of the arbitration and the appointment of the arbitrator or arbitral tribunal. The parties state their commitment to comply with the award that is issued.

VinCAsign checks, through consultations with official records or documents certified by third parties, the evidence of possession of the trademark that an applicant wishes to include in the requested certificate, claiming to have rights over it. VinCAsign does not assume any commitment on the issuance of certificates regarding the use of a trademark by applicants. The form of verification used by Vintegris is reflected in section 4.1.1 of this CPS.

3.2. Initial identity validation

3.2.1. By certificate type

3.2.1.1. Corporate certificates

The identity of the certificate subscribers is determined at the time of signing the contract between VinCAsign and the subscriber, when the existence of the subscriber is verified, and the powers of attorney of the person who represents it. For this verification, public or notarial documentation may be used, or direct consultation of the corresponding public records.

The identity of the natural persons identified in the certificates is validated through the corporate records of the entity, company, or organization of public or private law, subscribers of the certificates. The subscriber will produce a certification of the necessary

data, and will send it to VinCAsign, through the mediums that it enables, for the registration of the identity of the signatories.

In relation to the personal data of each entity, company or organization of public or private law, VinCAsign acts as **Data Controller** in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46/EC (General Data Protection Regulation) is repealed, and in the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD), and in the terms indicated in section 9.4 of this document.

3.2.1.2. Individual certificates

The identity of the natural persons identified in the certificates is validated by their physical presence before a Registration Entity, providing the necessary documentation that identifies them as a National Identity Document (such as Spanish DNI, TIE) or passport.

In relation to the personal data of this type of certificate, VinCAsign acquires the status of **Data Controller** in the terms indicated in section 9.4 of this document.

3.2.1.3. Non-qualified certificates

The identity of the natural persons identified in these certificates is carried out by videoconference in accordance with the SEPBLAC standard.

3.2.2. Method to prove possession of private key

Possession of the private key is demonstrated by virtue of the reliable procedure of delivery and acceptance of the certificate by the subscriber, in seal certificates, or by the signatory, in signature certificates.

If the key pair is generated by the subscriber, the subscriber must prove that they are in possession of the private key corresponding to the public key for which their certification is requested, by sending the certification request in PKCS#10 or other method VinCAsign deems valid and approved.

3.2.3. Authentication of Organization and Domain Identity

Natural persons with the capacity to act on behalf of the subscribing public or private persons may act as their representatives, if there is a prior situation of legal or voluntary representation between the natural person and the public or private person, which requires its recognition by VinCAsign, which will be carried out through the following face-to-face procedure:

1. The subscriber's representative will meet in person with an authorized VinCAsign representative, who will make an authentication form available to them.
2. The representative will complete the form, with the following information and will accompany it with the following documents:
 - Identification data, as representative:
 - Name and surname.
 - Date and place of birth.
 - TIN document of the representative.
 - Identification data, of the represented subscriber:
 - Name or social reason.
 - All existing registration information, including data related to the constitution and legal personality and the extension and validity of the powers of representation of the applicant.
 - TIN document of the public or private person.
 - Public documents that serve to certify the points cited in a reliable manner and their registration in the corresponding public registry if it is required. The verification may also be carried out by consulting the public registry in which the constitution and empowerment documents are registered, and the telematic mediums provided by the aforementioned public registries may be used.
 - In the case of Entities without Legal Personality that must be registered in a public or special registry, they will present the certificate or simple note accrediting their registration in the

registry, issued on the date of application or in the previous fifteen days.

- In the case of Entities without Legal Personality that do not have to be registered in any public or special registry, they will present the public deeds, contracts, statutes, agreements, or any other documents that can prove their constitution, validity and identification of the members that integrate them.
- Data related to the representation or the capacity to act that it holds:
 - V validity of the representation or the capacity to act (start and end date).
 - Scope and limits, if any, of representation or capacity to act:
 - TOTAL. Representation or total capacity. This verification may be carried out by telematic consultation of the public registry where the representation is registered.
 - PARTIAL. Representation or partial capacity. This verification may be carried out by means of an authentic electronic copy of the notarial deed of empowerment, under the terms of the notarial regulations.
 - In case of representation of Entities without Legal Personality:
 - Through notarial documents that certify the powers of representation of the applicant for the certificate, or through a special power of attorney granted for this purpose.
 - By means of private documents appointing a representative as appropriate in each case. Representation may be accredited by means of the following documents:
 1. Designation document of the representative of the recumbent estate, signed by all the heirs, stating the name, surnames and DNI or passport number of the representative, when a judicial administrator or executor with full administration powers has not been appointed.

2. Copy of the Minutes of the meeting of the Board of Owners in which the president of the Community was appointed, in the case of communities under a horizontal property regime.
 3. Document signed by enough members, in accordance with the provisions of article 398 of the Civil Code to represent most of the interests of the entity, in the case of community property and civil partnerships without legal personality, in which it is designated to the person who represents it to request the certificate.
3. Once the form has been completed and signed, it will be signed and delivered to VinCAsign together with the supporting documentation indicated.
 4. VinCAsign staff will verify the identity of the representative by the presented ID card, as well as the content of the representation, with the documentation.
 5. VinCAsign staff will deliver proof of authentication and will return the documentation provided to the subscriber's representative.
 6. Alternatively, in accordance with the provisions of article 24.1 of Regulation (EU) No 910/2014 of the European Parliament and of the Council, the signature of the form may be authenticated by a notary, and sent to VinCAsign by certified mail, in which case steps 3 through 5 above will not be accurate.

The provision of the digital certification service is formalized through the appropriate contract between VinCAsign and the subscriber, duly represented.

3.2.4. Authentication of individual identity

This section describes the methods of verifying the identity of a natural person identified in a certificate.

The subscriber must finalize the certificate issuance process before 20 days after the identity validation has been approved.

3.2.4.1. In corporate certificates

The identification information of the natural persons identified in the certificates is validated by comparing the information on the application with the records of the public

or private entity, company, or organization to which they are linked, ensuring the correctness of the information to be certified.

3.2.4.2. In individual certificates for natural persons

See initial section 3.2.

3.2.4.3. Need for reliable identification

Verification of the identity of a natural person will be carried out as follows:

- Through the physical presence of the applicant or the authorized representative of a natural or legal person.
- By appearing before a notary to make the request for the issuance of an electronic certificate, and the latter has legitimized it.
- Only for the issuance of a qualified signature certificate, through the video identification system that VinCAsign makes available to its clients to carry out such reliable identification for the issuance of qualified certificates.

3.2.4.3.1. *In corporate certificates*

To request the certificates, direct physical presence is not required due to the already accredited relationship between the natural person and the public or private entity, company, or organization to which they are linked.

However, before the delivery of a certificate, the subscribing entity, company, or organization of public or private law, through its certification manager, if it has one, or another designated member, must verify the identity of the natural person identified in the certificate by physical presence or by the VinCAsign video identification system.

During this process, the identity of the natural person identified in the certificate is irrefutably confirmed.

For this reason, in all cases in which a certificate is issued, the identity of the signing natural person is verified in person.

The Registration Authority will verify the rest of the data and attributes to be included in the certificate by displaying documents or through its own sources of information, keeping supporting documentation of their validity.

3.2.4.3.2. *In individual certificates for natural persons*

In all cases in which a certificate is issued, the identity of the signing natural person is irrefutably verified, either by physical presence or by means of the video identification system (only qualified signature certificates).

The Registration Authority will verify the rest of the data and attributes to be included in the certificate by displaying documents or through its own sources of information, keeping supporting documentation of their validity.

When the identification has been made through the VinCAsign video identification system, the registry operator must verify, before issuing the certificate:

- View and review the video and images captured by the system, both applicant and of their identity document.
- Check that the applicant is a real person, through the proof of life that has been collected in the video as well as the results thrown by the system.
- Review the documentation provided, its validity and veracity and the results obtained automatically by the video identification system.

3.2.4.3.3. *In non-qualified certificates*

The identity of the natural persons identified in these certificates is carried out by videoconference in accordance with the SEPBLAC standard.

3.2.4.4. Relationship of the natural person

In corporate certificates, the documentary justification of the relationship of a natural person identified in a certificate with an entity, company or organization of public or private law is given by its record in the internal records (employment contract as an employee, or the contract that binds him, or the minutes indicating his position, or the application as a member of the organization...) of each of the public and private organizations to which they are linked.

3.2.5. Non-verifies subscriber information

VinCAsign does not include any unverified subscriber information in the certificates.

The information contained in the web authentication certificates is verified and contrasted with independent sources of information, prior to their issuance.

3.2.6. Validation of authority

VinCAsign carries out the necessary verifications to confirm the existence of the organization that wishes to become a Registration Authority. VinCAsign obtains the documentation from the organization that is presented, in addition to using its own sources of information.

VinCAsign verifies and validates the identity of the operators of the Registration Authority with the information sent by the subscriber, which includes their authorization to act as such.

VinCAsign ensures that the operators of the Registration Authority receive sufficient training to perform their duties, which it will verify in the corresponding evaluations.

Operators and certification managers are always authenticated with digital certificates for the provision of their services before the Registration Authority.

3.2.7. Criteria for Interoperation or Certification

Not stipulated.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Before renewing a certificate, VinCAsign or a Registration Entity checks that the information used to verify the identity and the other data of the subscriber, and the natural person identified in the certificate are still valid.

Acceptable methodologies for such verification are:

- Use of the current certificate for its renewal, if it is a certificate issued by vinCAsign and the maximum term legally established for this possibility has not been exceeded.

The form of identification for the first issuance of the certificate to be renewed will be previously checked: if it had been carried out by face-to-face identification, online renewal will be possible; if the initial identification was made by video identification, the signatory must re-identify reliably.

- A renewal request is made through the nebulaSUITE application, the RA Operator verifies the request if the values defined and the documentation are correct and there have been no variations, the renewal is approved, and the certificate is issued.
- If any information of the subscriber or of the natural person identified in the certificate has changed, the new information is properly registered and a complete authentication occurs, in accordance with the provisions of section 3.2.

3.3.2. Identification and authentication for re-key after revocation

Before generating a certificate for a subscriber whose certificate was revoked, vinCAsign or a Registration Entity will verify that the information used to verify the identity and other data of the subscriber and the natural person identified in the certificate continues to be valid, in which case the provisions of the previous section shall apply.

The renewal of certificates after revocation will not be possible in the following cases:

- Certificate was revoked due to erroneous issuance to a person other than the one identified in the certificate.
- Certificate was revoked due to unauthorized issuance by the natural person identified in the certificate.
- The revoked certificate may contain wrong or false information.

If any information of the subscriber or of the natural person identified in the certificate has changed, the new information is properly registered and a complete authentication occurs, in accordance with the provisions of section 3.2.

3.4. Identification and authentication for revocation request

VinCAsign or a Registration Entity authenticates the requests for reports related to the revocation of a certificate, verifying that they come from an authorized person.

Acceptable methods for such verification are as follows:

- Sending of a revocation request by the subscriber or the natural person identified in the certificate, through the electronic platform nebulaSUITE, for managing the life cycle of the certificates.

- Sending a revocation request by the subscriber or the natural person identified in the certificate, signed electronically, using the contact form available at the vinCAsign website.
- The physical person in an office of the subscribing company, entity, or Organization.
- Other means of communication, such as the telephone, when there are reasonable guarantees of the identity of the revocation applicant, as defined per VinCAsign.

4. Certificate Life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

4.1.1.1. Corporate certificates

The public or private entity, company or organization in question must sign a contract for the provision of certification services with VinCAsign.

Likewise, prior to the issuance and delivery of a certificate, there must be a certificate request in a specific certificate request sheet document, which may be in electronic format through the NebulaSUITE platform.

When the applicant is a person other than the subscriber, there must be an authorization from the subscriber for the applicant to make the request, which is legally implemented by means of a certificate request form signed by said applicant on behalf of the entity, company, or organization of public or private law, which may be in electronic format through the NebulaSUITE platform.

4.1.1.2. Individual certificates

The individual subscriber makes a request, which is legally implemented through a certificate request form signed by said individual subscriber, which may be in electronic format through the NebulaSUITE platform.

4.1.2. Enrollment process and responsibilities

VinCAsign receives requests for corporate certificates, made by entities, companies or organizations of public or private law, and requests for individual certificates made by individual subscribers, as well as requests for web authentication certificates.

The requests are instrumented by means of a document in electronic format, completed, in the corporate certificates by the entity, company or organization of public or private law, or in the individual certificates by the individual subscriber, or by their applicant (whether a natural or legal person), in web authentication certificates, through the NEBULASUITE platform, whose recipient is VinCAsign, which will include the data of the people to whom the certificates will be issued. The request will be made by the operator

authorized by the subscriber or Registration Entity (responsible for certification) and that has been identified in the contract between this subscriber or Registration Entity and VinCAsign.

The request must be accompanied by supporting documentation of the identity and other circumstances of the natural person identified in the certificate, in accordance with the provisions of section 3.2.4. A physical address, or other data, that allows contacting the natural person identified in the certificate or in the request for web authentication certificates must also be attached. To do this, the method of communication with the applicant must be verified as follows:

VinCAsign verifies that the method of communication chosen by the applicant, be it email, telephone number or physical address, belongs to the applicant, or to an entity to which the Applicant belongs, comparing it with one of the headquarters of the parent company or subsidiary of the applicant through one of the following options:

- Records provided by the applicable telephone company;
- One of the verification sources established as trustworthy by VinCAsign (QGIS, QTIS or QIIS); either
- A verified professional letter.
- Document signed with Qualified Certificate of electronic seal or electronic signature linked to the organization.

VinCAsign will verify said method of communication, using it to obtain an affirmative answer that gives sufficient guarantees to conclude that said applicant or the parent company or subsidiary of the applicant can be reliably contacted by means of that verified method of communication.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

Once a certificate request is received, VinCAsign ensures that certificate requests are complete, accurate, and properly authorized before processing them.

If so, VinCAsign verifies the information provided, verifying the aspects described in section 3.2.

In the case of a qualified certificate, the documentation justifying the approval of the application must be kept and duly registered with security and integrity guarantees for a period of 15 years from the expiration of the certificate, even in the event of early loss of validity due to revocation. This documentation may be kept securely through the NebulaSUITE platform.

4.2.2. Approval of rejection of certificate applications

In case the data is verified correctly, VinCAsign must approve the request for the certificate and proceed to its issuance and delivery.

If the verification indicates that the information is not correct, or if it is suspected that it is not correct or that it may affect the reputation of the Certification Entity or the subscribers, VinCAsign will deny the request, or stop its approval until the verifications have been carried out. supplements you deem appropriate.

If the additional checks do not reveal the correctness of the information to be verified, VinCAsign will deny the request definitively.

VinCAsign notifies the applicant of the approval or denial of the application.

VinCAsign will be able to automate the verification procedures of the correctness of the information that will be contained in the certificates, and of approval of the requests, through the NebulaSUITE platform.

4.2.3. Time to process certificate applications

VinCAsign responds to requests for certificates in order of arrival, within a reasonable period of time, and a maximum term guarantee may be specified in the certificate issuance contract.

Requests remain active until approved or rejected.

4.3. Certificate issuance

4.3.1. VinCAsign actions during certificate issuance

After approval of the certification request, the certificate is issued securely and is made available to the signatory for acceptance, through the NebulaSUITE platform.

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

During the process, VinCAsign:

- Protects the confidentiality and integrity of the registration data you have.
- It uses reliable systems and products that are protected against any alteration and that guarantee the technical and, where appropriate, cryptographic security of the certification processes they support.
- Generates the key pair, using a certificate generation procedure securely linked with the key generation procedure.
- Employs a certificate generation procedure that securely links the certificate with registration information, including the certified public key.
- It ensures that the certificate is issued by systems that use protection against forgery and that guarantee the confidentiality of the keys during the process of generating said keys.
- The certificate includes the information established in Annex 1 of Regulation (EU) 910/2014, in accordance with what is declared in epigraphs 3.1.1 and 7.1, of this CPS.
- Indicates the date and time when the certificate was issued.

4.3.2. Notification to subscriber by the CA of issuance of certificate

VinCAsign notifies the issuance of the certificate to the subscriber and to the natural person identified in the certificate.

4.3.3. Test certificates issuance

VinCAsign issues test certificates for the following purposes:

- Generally, for review in inspection or notification processes by the Supervisory Body.
- In compliance evaluation or audit processes.
- Integration with third parties.
- Internal validation testing.

These certificates are generated with a maximum validity of 1 year and are issued under vinCAsign's production hierarchy. This responsibility is solely delegated to vinCAsign and cannot be delegated to third parties.

The fictitious data defined in the test certificates is strictly managed by vinCAsign, based on those authorized by the Supervisory Body for such purposes.

In general, the public keys of these certificates are accessible from <https://www.vincasign.net>. PKCS#12 key stores can be requested by any interested party; however, their delivery will be subject to vinCAsign's discretion.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The acceptance of the certificate by the natural person identified in the certificate occurs by signing the acceptance sheet.

When this acceptance is electronic, it is done through the NebulaSUITE platform.

4.4.1.1. VinCAsign liability

During this process, VinCAsign must perform the following actions:

- Definitely prove the identity of the natural person identified in the certificate, with the collaboration of the subscriber (company, entity or organization in corporate certificates and web authentication certificates), and with the Registration Entity (in individual certificates) in accordance with what is established in the epigraphs 3.2.1.1 and 3.2.1.2 of this document.
- Deliver to the natural person identified in the certificate with the collaboration of the subscriber (company, entity, or organization) or the Registration Entity

the delivery and acceptance sheet of the certificate with the following minimum contents:

- Basic information about the use of the certificate, including especially information about the certification service provider and the applicable Trust Practices Statement, as well as its obligations, powers, and responsibilities.
 - Information about the certificate.
 - Acknowledgment, by the signatory, of receipt of the certificate and acceptance of the previously mentioned elements.
 - Obligations regime of the signatory.
 - Responsibilities of the signatory.
 - Exclusive imputation method to the signatory, of their private key and their certificate activation data, in accordance with the provisions of sections 6.2 y 6.4 of this document.
 - The date of the act of acceptance of the certificate.
- Obtain the signature, written or electronic, of the person identified in the certificate. In the option of the electronic signature of the delivery sheet, this is done through the services of the NebulaSUITE platform.

The subscriber or the Registration Entity collaborates in these processes, having to document the previous acts and keeping the original documents (delivery and acceptance agreement), sending an electronic copy to VinCAsign, as well as the originals when VinCAsign requires access to them. When this documentation is stored electronically, it is done through the services of the NebulaSUITE platform.

4.4.2. Publication of the certificate by the CA

VinCAsign publishes the certificate in the Repository referred to in 2, with the pertinent security controls and provided that VinCAsign has the authorization of the natural person identified in the certificate.

4.4.3. Notification of certificate issuance by the CA to other entities

VinCAsign does not make any notification of the issue to third parties.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

4.5.1.1. Use of the certificate and private key by the signer

VinCAsign obliges the signatory to:

- Provide VinCAsign with complete and adequate information, in accordance with the requirements of this Trust Practices Statement, especially regarding the registration procedure.
- Express your consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4 of this CPS.
- When the certificate works together with a QSCD, recognize its ability to produce qualified electronic signatures; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.
- Be especially diligent in the custody of your private key, in order to avoid unauthorized use, in accordance with the provisions set in sections 6.1, 6.2 and 6.4 of this document.
- Notify VinCAsign and any person believed to trust the certificate, without unjustifiable delay:
 - The loss, theft, or potential compromise of your private key.
 - Loss of control over your private key, due to compromise of activation data (for example, PIN code) or for any other reason.
 - The inaccuracies or changes in the content of the certificate that the subscriber knows or could know.
- Stop using the private key after the period indicated in 6.3.2.
- Stop using the private key in case of compromise of said key, revocation, or compromise of the keys of the CA.

4.5.2. Use of the certificate and private key by the subscriber and the Registration Entity

4.5.2.1. Corporate Subscriber Obligations

VinCAsign contractually obligates the corporate and web authentication subscriber to:

- Provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Trust Practices Statement, especially regarding the registration procedure.
- Express your consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions described in section 1.4 of this document.
- Check the following aspects before using the certificate:
 - That the obtained certificate is valid (as well as any of the certificates of the hierarchy under which it has been issued) using any of the certificate validation methods exposed by VinCAsign.
 - That the key uses for which the certificate has been issued are correct and coincide with those specified in the corresponding Practices Statement (electronic seal).
 - The qcStatements extension of the certificate (OID 1.3.6.1.5.5.7.1.3), as well as the verification that it corresponds to the values established in the Practices Statement under which the certificate is issued.
 - That the issuing Certification Entity is on the Trust Services List (TSL) issued by the National Accreditation Body⁷.
- Communicate to VinCAsign and to any person that the subscriber believes may trust the certificate, without unjustifiable delay:
 - The loss, theft, or potential compromise of your private key.
 - Inaccuracies or changes in the content of the certificate known or could be known by the corporate subscriber.

⁷ Accesible at <https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

- Transfer to the natural persons identified in the certificate the fulfillment of their specific obligations and establish mechanisms to guarantee the effective fulfillment of the same.
- Do not monitor, manipulate, or carry out acts of reverse engineering on the technical implementation of VinCAsign certification services, without prior written permission.
- Not to compromise the security of the certification services of the VinCAsign certification service provider, without prior written permission.

4.5.2.2. Individual Subscriber Obligations

VinCAsign contractually obligates the individual subscriber to:

- Provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Trust Practices Statement, especially about the registration procedure.
- Express your consent prior to the issuance and delivery of a certificate.
- Use the certificate in accordance with the provisions of section 1.4 of this CPS.
- Check the following aspects before using the certificate:
 - That the obtained certificate is valid (as well as any of the certificates of the hierarchy under which it has been issued) using any of the certificate validation methods exposed by VinCAsign.
 - That the key uses for which the certificate has been issued are correct and coincide with those specified in the corresponding Practices Statement (electronic signature).
 - The qcStatements extension of the certificate (OID 1.3.6.1.5.5.7.1.3), as well as the verification that it corresponds to the values established in the Statement of Practices under which the certificate is issued.
 - That the issuing Certification Entity is on the Trust Services List (TSL) issued by the National Accreditation Body⁸.
- Communicate to VinCAsign and to any person that the subscriber believes may trust the certificate, without unjustifiable delay:
 - The loss, theft, or potential compromise of your private key.
 - The inaccuracies or changes in the content of the certificate that you know or could know.
- Do not monitor, manipulate, or carry out acts of reverse engineering on the technical implementation of VinCAsign certification services, without prior written permission.

⁸ Accesible en <https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

- Not to compromise the security of the certification services of the VinCAsign certification service provider, without prior written permission.
- Be accountable for:
 - That all statements made in the application are correct.
 - That all the information provided contained in the certificate is correct.
 - o That the certificate is used exclusively for legal and authorized uses, in accordance with the CPS.
 - That no unauthorized person has ever had access to the private key of the certificate, and that they are solely responsible for the damages caused by their breach of the duty to protect the exclusive control of access to the private key.
 - That it is a final recipient and not a certification service provider, and that it will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), or Revocation List of Certificates, or title of certification service provider or in any other case.

4.5.2.3. Registration Entity obligations

VinCAsign contractually obliges the Registration Entity to:

- Provide the Certification Authority with complete and adequate information, in accordance with the requirements of this Trust Practices Statement, especially regarding the registration procedure.
- Notify VinCAsign without unjustifiable delay:
 - The loss, theft, or potential compromise of the private key.
 - The inaccuracies or changes in the content of the certificate that you know or could know.
- Transfer to the natural persons identified in the certificate the fulfillment of their specific obligations and establish mechanisms to guarantee the effective fulfillment of the same.

- Not monitor, manipulate, or carry out acts of reverse engineering on the technical implementation of VinCAsign certification services, without prior written permission.
- Not to compromise the security of the certification services of the VinCAsign certification service provider, without prior written permission.

4.5.2.4. Signatory civil liability

VinCAsign requires the signer to be responsible of:

- That all statements made in the application are correct.
- That all the information provided by the signatory contained in the certificate is correct.
- That the certificate is used exclusively for legal and authorized uses, in accordance with the CPS.
- That no unauthorized person has ever had access to the private key of the certificate, and that they are solely responsible for the damages caused by their breach of the duty to protect the exclusive control of access to the private key.
- That the signatory is a final recipient and not a certification service provider, and that it will not use the private key corresponding to the public key listed in the certificate to sign any certificate (or any other format of certified public key), nor List of Revocation of Certificates, or title of certification service provider or in any other case.

4.5.3. Relying party public key and certificate usage

4.5.3.1. Obligations of the third party that trusts in the certificates

VinCAsign requires the third party that trusts certificates to:

- Obtain independent advice as to whether the certificate is appropriate for its intended use.
- Verify the validity or revocation of the issued certificates, for which it will use information on the status of the certificates.

- Verify all the certificates in the hierarchy of certificates, before trusting the digital signature or any of the certificates in the hierarchy, as well as that the issuing Certification Authority is on the Trust Services List (TSL) issued by the National Accreditation Body⁹.
- Recognize that verified electronic signatures produced on a Qualified Signature Creation Device (QSCD) are legally considered qualified electronic signatures; that is, equivalent to handwritten signatures, as well as the fact that the certificate allows the creation of other types of electronic signatures and encryption mechanisms.
- Be aware of any limitation on the use of the certificate, regardless of whether it is in the certificate itself or in the contract of a third party that trusts the certificate.
- Consider any precaution established in a contract or in another instrument, regardless of its legal nature.
- Do not monitor, manipulate, or carry out acts of reverse engineering on the technical implementation of VinCAsign certification services, without prior written permission.
- Do not compromise the security of VinCAsign certification services, without prior written permission.

4.5.3.2. Civil liability of the third party that relies on certificates

VinCAsign contractually obliges the third party to express:

- That you have enough information to make an informed decision to trust the certificate or not.
- That he is solely responsible for trusting or not the information contained in the certificate.

That it will be solely responsible if it fails to comply with its obligations as a third party that trusts the certificate.

⁹ Accessible at <https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx>

4.6. Certificate renewal

The renewal of the certificates requires the renewal of the keys, so the provisions of section 4.7 of this document.

4.6.1. Circumstance for certificate renewal

Not stipulated.

4.6.2. Who may request renewal

Not stipulated.

4.6.3. Processing certificate renewal requests

Not stipulated.

4.6.4. Notification of new certificate issuance to subscriber

Not stipulated.

4.6.5. Conduct constituting acceptance of a renewal certificate

Not stipulated.

4.6.6. Publication of the renewal certificate by the CA

Not stipulated.

4.6.7. Notification of certificate issuance by the CA to other entities

Not stipulated..

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

Current certificates can be renewed through a specific and simplified application procedure, to maintain the continuity of the certification service. When this procedure is performed electronically, the NebulaSUITE platform is used exclusively.

4.7.2. Who may request certification of a new public key

Prior to the issuance and delivery of a renewed certificate, there must be a certificate renewal request, which can be made ex officio or at the request of an interested party.

Likewise, for corporate certificates, an authorization from the subscriber is contemplated so that the applicant can make the request, which is legally implemented through a certificate renewal sheet signed by the company, entity, or organization.

For its part, VinCAsign informs the holder requesting the renewal, of the existence, if applicable, of new CPS, PDS or other legal documents.

4.7.3. Processing certificate re-keying requests

Not stipulated.

4.7.3.1. Requesting

VinCAsign, in relation to corporate certificates, receives requests for renewal of certificates, made by entities, companies or organizations of public or private law.

VinCAsign, in relation to individual certificates, receives requests for renewal of certificates, made by the holders of the certificates.

There is a document, either on paper or in electronic format, referring to the request for renewal of certificates, which will include the data of the persons to whom certificates will be issued.

When it is in electronic format, the request is made exclusively through the NebulaSUITE platform.

4.7.3.2. Execution of identification and authentication functions

Upon receipt of a certificate renewal request, VinCAsign ensures that certificate requests are complete, accurate, and properly authorized before processing them.

4.7.3.3. Approval or rejection of the request

In case the data is verified correctly, VinCAsign must approve the certificate renewal request (if the certificate has not yet expired, it must be revoked to approve the issuance of the new certificate or else this approval will be carried out the same way). expiration date of the current certificate) and proceed to its issuance and delivery.

VinCAsign notifies the applicant of the approval or denial of the application.

VinCAsign will be able to automate the verification procedures of the correctness of the information that will be contained in the certificates, and of the approval of the requests.

4.7.3.4. Deadline to resolve the request

VinCAsign attends to certificate renewal requests in order of arrival, within a reasonable period prior to the expiration of the certificates to be revoked, and a maximum term guarantee may be specified in the certificate issuance agreement.

Renewal requests remain active until approved or rejected.

4.7.4. Notification of new certificate issuance to subscriber

VinCAsign notifies the issuance of the certificate to the subscriber and to the natural person identified in the corporate certificate, and to the subscriber of the individual certificate.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

The acceptance of the certificate occurs through the signature, written or electronic, of the delivery and acceptance sheet before the person responsible for certification of the entity, company, or organization of public or private law or Registration Entity.

When the signature is produced electronically, it is done through the NebulaSUITE platform.

4.7.6. Publication of the re-keyed certificate by VinCAsign

VinCAsign publishes the renewed certificate in the Repository referred to in the section 2 *Publication* and Repository Responsibilities

, with the pertinent security controls.

4.7.7. Notification of certificate issuance by VinCAsign to third parties

VinCAsign does not make any notification of the issue to third parties.

4.8. Certificate modification

The modification of certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new certificate issuance, applying what is described in epigraphs 4.1, 4.2, 4.3 and 4.4 of this document.

4.8.1. Circumstance for certificate modification

Not stipulated.

4.8.2. Who may request certificate modification

Not stipulated.

4.8.3. Processing certificate modification requests

Not stipulated.

4.8.4. Notification of new certificate issuance to subscriber

Not stipulated.

4.8.5. Conduct constituting acceptance of modified certificate

Not stipulated.

4.8.6. Publication of the modified certificate by VinCAsign

Not stipulated.

4.8.7. Notification of certificate issuance by VinCAsign to other entities

Not stipulated

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

VinCAsign revokes a certificate when any of the following causes occur:

- 1) Circumstances that affect the information contained in the certificate:
 - a) Modification of any of the data contained in the certificate, after the corresponding issuance of the certificate that includes the modifications.
 - b) Discovery that some of the data contained in the certificate request is incorrect.
 - c) Discovery that some of the data contained in the certificate is incorrect.
- 2) Circumstances that affect the security of the key or certificate:
 - a) Compromise of the private key, of the infrastructure or of the systems of the certification service provider that issued the certificate, if it affects the reliability of the certificates issued from that incident.
 - b) Violation, by VinCAsign, of the requirements set forth in the certificate management procedures, established in this Trust Practices Statement.
 - c) Compromise or suspected compromise of the security of the key or of the issued certificate.
 - d) Unauthorized access or use by a third party of the private key corresponding to the public key contained in the certificate.
 - e) The irregular use of the certificate by the natural person identified in the certificate, or the lack of diligence in the custody of the private key.
 - f) The CA knows a proven method that can simply and easily calculate the private key of the subscriber based on the public key of the certificate.
- 3) Circumstances that affect the subscriber of the individual certificate or the natural person identified in the corporate certificate:

- a) Termination of the legal relationship for the provision of services between vinCAsign and the subscriber (corporate or individual).
 - b) Modification or termination of the underlying legal relationship or cause that led to the issuance of the certificate to the natural person identified in the corporate certificate.
 - c) Violation by the applicant of the certificate of the pre-established requirements for the application of the same.
 - d) Violation by the corporate or individual subscriber, or by the person identified in the certificate, of their obligations, responsibilities and guarantees, established in the corresponding legal document or in this CPS.
 - e) The supervening incapacity or the death of the signatory of the corporate certificate or of the holder of the individual certificate.
 - f) In corporate certificates, the termination of the legal person subscribing the certificate, as well as the end of the authorization of the subscriber to the key holder or the termination of the relationship between the subscriber and the person identified in the certificate.
 - g) Request from the subscriber to revoke the certificate, in accordance with the provisions referred to in section 3.4.
- 4) Other circumstances:
- a) The termination of the certification service of the VinCAsign service, in accordance with the provisions detailed in 5.8.
 - b) The use of the certificate that is harmful and continued for VinCAsign. In this case, a use is harmful based on the following criteria:
 - The nature and number of complaints received.
 - The identity of the entities filing the complaints.
 - The relevant legislation in force at any given time.
 - The response of the subscriber or the person identified in the certificate to the complaints received.
 - c) By judicial or administrative resolution ordering its revocation.
 - d) For any other reason contained in this CPS.

4.9.2. Who can request revocation

Certificates can be requested by:

- The natural person (signatory) identified in the corporate certificate.
- The subscriber of the corporate or web authentication certificate, through the person responsible for the certification service.
- The subscriber of the individual certificate, through the Registration Entity.
- Any person who is aware of any of the causes detailed in 4.9.1.

4.9.3. Procedure for revocation request

The corporate subscriber entity or an individual subscriber who needs to revoke a certificate must request it from VinCAsign.

The revocation request can be requested through the NebulaSUITE platform or by email to info@vincasign.net or through the form available at:

- <https://www.vincasign.net/>(Spanish)
- <https://www.vincasign.net/> (English)
- <https://www.vincasign.net/> (Catalonian)

The revocation request will include the following information:

- Date of revocation request.
- Subscriber identity.
- Detailed reason for the revocation request.
- Name and title of the person requesting the revocation.
- Contact information of the person requesting the revocation.

The request must be authenticated, by VinCAsign, in accordance with the requirements established in section 3.4, before proceeding with the revocation.

VinCAsign may include any other requirements for confirmation of revocation requests.

¹⁰.

¹⁰ Sec. REV-6.2.4-01, c) of ETSI EN 319 411-1

The revocation service can be found on the VinCAsign website at the address: <https://www.vincasign.net>.

If the recipient of a revocation request is the subscribing entity or the Registration Entity, once the request has been authenticated, it must send a request in this regard to vinCAsign.

The revocation request will be processed upon receipt, and the subscriber (corporate or individual) and, if applicable, the natural person identified in the certificate, will be informed about the change in status of the revoked certificate.

VinCAsign does not reactivate the certificate once it has been revoked.

Both the revocation management service and the query service are considered critical services and thus appear in VinCAsign Contingency Plan and Business Continuity Plan.

4.9.4. Revocation request grace period

Revocation requests will be sent immediately as soon as the reason for revocation is known, 24x7 and will not exceed 24 hours¹¹.

4.9.5. Time within which VinCAsign must process the revocation request

The revocation will take place immediately when it is received, 24x7.

In case that the identity of the requester could not be validated within 24 hours following the receipt of the request, it will be disregarded and will not be processed

4.9.6. Revocation checking requirement for relying parties

Third parties must check the status of those certificates they wish to trust.

One method by which the status of certificates is verified is by querying the VinCAsign OCSP service.

VinCAsign validates the status of all certificates before performing a signature.

The Certificate Revocation Lists are published in the Deposit of the Vintegris Certification Entity, as well as in the following web addresses, indicated inside the certificates:

¹¹ Sec REV-6.2.4-01, d) of ETSI EN 319 411-1

For certificates issued by the qualified CA “vinCAsign nebulaSUITE2 Authority”:

- <http://crl1.vincasign.net/canebula2.crl>
- <http://crl2.vincasign.net/canebula2.crl>

For certificates issued by the CA “vinCAsign nebulaSUITE3 Authority”:

- <http://crl1.vincasign.net/canebula3.crl>
- <http://crl2.vincasign.net/canebula3.crl>

For certificates issued by the qualified CA “vinCAsign nebulaSUITE4 Authority”:

- <http://crl1.vincasign.net/canebula4.crl>
- <http://crl2.vincasign.net/canebula4.crl>

For certificates issued by the qualified CA “vinCAsign nebulaSUITE5 Authority”:

- <http://crl1.vincasign.net/canebula5.crl>
- <http://crl2.vincasign.net/canebula5.crl>

For certificates issued by the qualified CA "CA Vintegris TrustServices":

- <http://crl1.vincasign.net/catrustservices.crl>
- <http://crl2.vincasign.net/catrustservices.crl>

For certificates issued by the qualified CA "CA Vintegris SSL TrustServices":

- <http://crl1.vincasign.net/cassltrustservices.crl>
- <http://crl2.vincasign.net/cassltrustservices.crl>

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

For certificates issued by VinCAsign CAs:

- <http://ocsp.vincasign.net/>

4.9.7. CRL issuance frequency

VinCAsign issues a CRL at least every 24 hours.

The CRL indicates the scheduled time of issuance of a new CRL, although, to reflect revocations, a CRL may be issued before the deadline indicated in the previous one.

The CRL compulsorily maintains the revoked certificate until it expires.

4.9.8. Maximum latency for CRLs

CRLs are published in the Repository in an immediate and reasonable period after their generation, which in no case does not exceed a few minutes.

4.9.9. On-line revocation/status checking availability

Alternatively, third parties that rely on certificates may consult VinCAsign Certificate Repository, which is available 24/7 on the web:

<https://validator.vincasign.net/>

To check the last CRL issued in each CA you must download the issuing CA CRL, as it is shown in the epigraph 4.9.6 of this document.

For certificates issued by the root CA “vinCAsign QUALIFIED Authority”:

In the event of failure of the certificate status verification systems due to causes beyond vinCAsign's control, vinCAsign must make its best efforts to ensure that this service remains inactive for the shortest time possible, which may not exceed one day.

VinCAsign provides information to third parties that trust certificates about the operation of the certificate status information service.

Certificate health check services are free to use¹².

VinCAsign maintains the revocation information of expired certificates in the OCSP service from the date of the issuing certificate¹³.

¹² Sec CSS-6.3.10-01 of ETSI EN 319 411-2

¹³ Sec CSS-6.3.10-08 of ETSI EN 319 411-2

In case of discrepancy regarding the validation status of a certificate due to temporary differences between the publication of CRLs and OCSP, the one provided by the latter should be considered as the prevailing value.

VinCAsign keeps the revocation status information available after the validity period of the certificate ¹⁴, through the OCSP service. This availability is maintained if the PKI services are terminated by VinCAsign, transferring this obligation to another provider.

If the CA issues the last CRL, the “nextUpdate” field should be set¹⁵ to “99991231235959Z”, as defined in IETF RFC 5280¹⁶.

In case that this last CRL would be issued due to a CA private key compromise, its SHA256 hash will be kept with the corresponding CRL file in the vinCAsign website (<https://www.vincasign.net>).

4.9.10. On-line revocation checking requirements

It is mandatory to check the status of the certificates before trusting them.

As specified in RFC 6960 and in the latest version of the Baseline Requirements document (CA/B Forum), the online revocation checking service complies with the following requirements specified in its definitions.

4.9.11. Other forms of revocation advertisements available

VinCAsign also informs about the revocation status of the certificates, through the OCSP protocol, which allows knowing the validity status of the certificates online from the following addresses:

For certificates issued by VinCAsign <http://ocsp.vincasign.net/>

4.9.12. Special requirements for re-key compromise

The compromise of the VinCAsign private key is notified to all participants in the certification services, to the extent possible, by publishing this fact on the VinCAsign

¹⁴ Sec CSS-6.3.10-12, c) of ETSI EN 319 411-2

¹⁵ Sec 6.3.9 of ETSI EN 319 411-2 -> Sec CSS-6.3.9-06 of ETSI EN 319 411-1

¹⁶ Sec 4.1.2.5 (validity) of IETF RFC 5280

website, as well as, if deemed necessary, in other communication mediums, including on paper.

To prove that a private key has been compromised, the following methods can be used:

- Provide evidence of security breaches or incidents or vulnerabilities where key compromise can be verified.
- Send a signed CSR, compromised private key, or other challenge response signed by that private key and verifiable by your public key.

Other mediums may be tested for key compromise, and if approved by VinCAsign, they will be included in this section.

The communication will be carried out as provided in 1.4.2.

VinCAsign considers the compromise of its private key as a significant security incident. As a result, it will apply its internal procedures for managing such incidents.

4.9.13. Circumstances for suspension

Not applicable, as VinCAsign does not support certificate suspension.

4.9.14. Who can request suspension

Not stipulated.

4.9.15. Procedure for suspension request

Not stipulated.

4.9.16. Limits on suspension period

Not stipulated.

4.10. Certificate status services

4.10.1. Operational characteristics

Certificate status checking services are provided through a web query interface, available at <http://www.VinCAsign.net>.

4.10.2. Service availability

Certificate status checking services are available 24x7, except for scheduled outages.

VinCAsign has 24x7 services to attend internally to high priority certificates, through the web form, being able to send the information of the complaint or problem to the police, where appropriate, and revoking the certificate subject of the problem.

The certificate status validation services (CRL or OCSP) have the necessary resources to provide a response time of less than 10 seconds.

4.10.3. Optional features

Not stipulated.

4.11. End of subscription

Upon certificate expiration, the subscription to the service will be terminated.

As an exception, the subscriber can keep the service in force by requesting the renewal of the certificate in advance as determined by this Statement of Trust Practices.

VinCAsign may issue a new certificate ex officio if subscribers maintain such status.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

VinCAsign does not provide key deposit and recovery services.

4.12.2. Session key encapsulation and recovery policy and practices

Not stipulated.

5. Management, operational and physical controls

Víntegris, which supports VinCAsign certificate management operations, is subject to the annual validations of the ISO/IEC 27001 standard, which regulates the establishment of appropriate processes to ensure proper security management of information systems.

5.1. Physical security controls

Based on the results of its risk assessments, vinCAsign has established physical and environmental security controls aligned with Regulation (EU) 910/2014 and with the provisions of Article 21 of Directive (EU) 2555/2022 and its Implementing Regulation of October 17, 2024, in order to protect the resources of the facilities where the systems are located, the systems themselves, and the equipment used for the registration and approval of requests, the technical generation of certificates, and the management of cryptographic hardware.

Specifically, the physical and environmental security policy applicable to certificate generation, cryptographic devices and revocation management services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Fire protection measures.
- Failure of support systems (electrical power, telecommunications, etc.).
- Collapse of the structure.
- Flooding.
- Theft protection.
- Unauthorized removal of equipment, information, media, and applications related to components used for the certification service provider's services.

These measures apply to the facilities where the certificates are produced under the full responsibility of vinCAsign, from its high-security facilities, both primary and, if applicable, contingency operation facilities. These are duly tested, reviewed, and, when necessary,

periodically updated or following significant incidents, or in the event of major changes in operations or risks.

The facilities have preventive and corrective maintenance systems with 24x7 support, and technical assistance within 24 hours of notification.

5.1.1. Site location and construction

Physical protection is achieved by creating clearly defined security perimeters around the facilities. The quality and solidity of the construction materials of the facilities guarantee adequate levels of protection against intrusions by brute force, while being in a low disaster risk area and allowing quick access.

The room where cryptographic operations are performed in the Datacentre:

- It has redundancy in its infrastructure.
- It has several alternative sources of electricity and cooling in case of emergency.
- Maintenance operations do not require the Datacentre to be offline at any time.
- It has an availability of 99.982%.

VinCAsign has facilities that physically protect the provision of certificate request approval and revocation management services from compromise caused by unauthorized access to systems or data, as well as from disclosure.

5.1.2. Physical access

VinCAsign has three levels of physical security (entrance to the building where the Datacentre is located, access to the server room and access to the rack) for the protection of the certificate generation service, being necessary to access from the lower floors to the upper ones.

Physical access to the VinCAsign premises where certification processes are carried out is limited and protected by a combination of physical and procedural measures. Thus:

- It is limited to expressly authorized personnel, with identification at the time of access and registration, including CCTV filming and archiving.

- Access to the rooms is done with badge readers and is managed by a computer system that keeps an automatic log of entries and exits.
- Access to the rack where the cryptographic processes are located requires prior authorization from VinCAsign to the administrators of the hosting service, who have the key to open the cage.

5.1.3. Power and air conditioning

The VinCAsign facilities are equipped with power stabilizers and a power supply system for the equipment, which is duplicated with a generator set.

The rooms housing computer equipment have temperature control systems with air conditioning equipment.

5.1.4. Water exposures

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

The rooms housing computer equipment are equipped with a humidity detection system.

5.1.5. Fire prevention and protection

VinCAsign facilities and assets are equipped with automatic fire detection and suppression systems.

5.1.6. Media storage

Only authorized personnel have access to the storage media.

The highest level of classification information is stored in a safe deposit box outside the Data Processing Centre facilities.

5.1.7. Waste disposal

The removal of media, both in paper and magnetic format, is carried out by means of mechanisms that guarantee the impossibility of recovering the information.

In the case of magnetic media, formatting, permanent erasure, or physical destruction of the media is carried out by means of specialized software that performs a minimum of 3 erasure passes and with variable erasure patterns.

In the case of paper documents, by means of shredders or in paper garbage cans provided for this purpose to be destroyed later, under control.

5.1.8. Off-site backup

VinCAsign uses a secure off-site storage facility for the custody of documents, magnetic and electronic devices that are independent of the operations centre.

At least two specifically authorized persons are required for access, deposit, or removal of devices.

5.2. Procedural controls

VinCAsign ensures that its systems are operated securely and has established and implemented procedures for the functions that affect the provision of its services.

The VinCAsign staff executes administrative and management procedures in accordance with the security policy.

The VinCAsign PKI system consists of the following modules:

- Management component/module for SubCA
- Management component/module for RA
- Management component/module for request handling
- Management component/module for key generation and storage (HSM)
- Management component/module for databases
- Management component/module for CRL handling
- Management component/module for OCSP

5.2.1. Trusted roles

VinCAsign has identified, in accordance with its security policy, the following functions or roles with the trusted status:

- **Internal auditor:** Responsible for compliance with operating procedures. This is a person external to the Information Systems department. The tasks of Internal Auditor are incompatible in time with the tasks of Certification and incompatible with Systems. These functions will be subordinated to the Head

of Operations, reporting both to the Head of Operations and to the Technical Management.

- **System administrator:** Responsible for the correct operation of the hardware and software supporting the certification platform.
- **CA administrator:** Responsible for the actions to be performed with the cryptographic material, or with the performance of any function that involves the activation of the private keys of the certification authorities described in this document, or of any of its elements.
- **CA operator:** Responsible jointly with the CA Administrator for the custody of cryptographic key activation material, also responsible for the backup and maintenance operations of the CA.
- **Registry administrator:** Person responsible for approving certification requests made by the subscriber.
- **Security manager:** In charge of coordinating, controlling, and enforcing the security measures defined by VinCAsign security policies. He/she must oversee the aspects related to information security: logical, physical, network, organizational, etc.

Persons occupying the above positions are subject to specific investigation and control procedures. These persons shall perform their duties based on the principle of least privilege.

5.2.2. Number of Individuals Required per Task

VinCAsign guarantees that at least two people perform the tasks detailed in the corresponding Certification Policies. Especially in the manipulation of the device for the custody of the keys of the Root and Intermediate Certification Authorities.

5.2.3. Identification and authentication for each role

The people assigned to each role are identified by the internal auditor who will ensure that each person performs the operations assigned to him/her.

Each person only controls the assets required for his role, thus ensuring that no person accesses unassigned resources.

Access to resources is done depending on the asset by means of cryptographic cards and activation codes.

5.2.4. Roles requiring separation of duties

The following tasks are performed by at least two people:

- Issuance and revocation of certificates, and access to the repository.
- Generation, issuance, and destruction of certificates of the Certification Entity.
- Putting the Certification Entity into production.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

All staff that performs tasks qualified as reliable, have been working at the production centre for at least one year and have permanent employment contracts.

All personnel are qualified and have been suitably instructed to perform the operations assigned to them.

Personnel in positions of trust do not have personal interests that conflict with the development of the function entrusted to them.

VinCAsign ensures that the registration staff is reliable to perform the registration tasks.

The Registry Administrator has completed a preparation course for the performance of request validation tasks.

In general, VinCAsign will remove an employee from a position of trust when it becomes aware of the commission of a criminal act that could affect the performance of his or her duties.

VinCAsign will not assign to a position of trust or management a person who is not suitable for the position, especially if he/she has been convicted of a crime or misdemeanour that affects his/her suitability for the position. For this reason, an investigation is carried out beforehand, **to the extent permitted by applicable law**, concerning the following aspects:

- Studies, including alleged degree.

- Previous work, up to five years, including professional references and verification that the alleged work was performed.
- Default (payments)

5.3.2. Background check procedures

VinCAsign, before hiring a person or before he/she enters the job, performs the following checks:

- References from recent years' work
- Professional references
- Studies, including claimed qualifications.

VinCAsign performs such checks in strict observance of 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

The investigation will be repeated with suitable regularity.

All checks are carried out to the extent permitted by the applicable legislation in force. The reasons that may lead to the rejection of the candidate for a reliable position are as follows:

- Misrepresentations in the job application, made by the candidate.
- Very negative or very unreliable professional references in relation to the candidate.

The application for the position informs about the need to undergo a prior investigation, warning that refusal to undergo the investigation will result in the rejection of the application.

5.3.3. Training Requirements and Procedures

VinCAsign trains staff in reliable and managerial positions until they reach the required qualification, keeping records of such training.

Training programs are periodically updated and improved.

Training includes at least the following contents:

- Principles and security mechanisms of the certification hierarchy, as well as the user environment of the person to be trained.
- Tasks to be performed by the person.
- VinCAsign security policies and procedures. Use and operation of installed machinery and applications.
- Management and handling of security incidents and compromises.
- Business continuity and emergency procedures.
- Management and security procedures in relation to the processing of personal data.

Additionally, vinCAsign develops cybersecurity training programs for employees, members of the management bodies, as well as for direct suppliers and other service providers. In particular, the training covers:

- Relevant cyber threats and applied risk management measures.
- Points of contact and available resources for obtaining additional information and advice on cybersecurity.
- Basic cybersecurity hygiene practices.

5.3.4. Retraining frequency and requirements

VinCAsign, updates staff training according to their needs, and with sufficient frequency to perform their duties competently and satisfactorily, especially when substantial changes are made to certification tasks.

5.3.5. Job rotation frequency and sequence

No stipulated.

5.3.6. Sanctions for unauthorized actions

VinCAsign has a sanctioning system in place to determine responsibilities arising from unauthorized actions in accordance with applicable work legislation and coordinated with the sanctioning system of the collective bargaining agreement applicable to the staff.

Disciplinary actions include suspension and removal of the person responsible for the harmful action, proportional to the severity of the unauthorized action.

5.3.7. Independent contractor controls

Employees hired to perform reliable tasks sign in advance the confidentiality clauses and operational requirements employed by VinCAsign. Any action that compromises the security of accepted processes could, upon evaluation, result in termination of employment.

If all or part of the certification services are operated by a third party, the controls and provisions made in this section, or in other parts of the DPC, shall be applied and complied with by the third party that performs the functions of operation of the certification services, notwithstanding which, the certification entity shall be responsible in any case for the effective execution. These aspects are specified in the legal instrument used to agree the provision of certification services by a third party other than VinCAsign.

In any case, these third parties must meet the same requirements for VinCAsign employees, both in terms of prior training and skills qualification, for the performance of specific operator or validation specialist functions.

5.3.8. Documentation supplied to personnel

The TSP shall supply the documentation strictly always required by its personnel, to perform its work in a competent and satisfactory manner.

5.4. Audit logging procedures

VinCAsign is subject to the annual validations of the ISO/IEC 27001 standard, which regulates the establishment of adequate processes to ensure proper security management in the information systems that support electronic certification processes.

Additionally, vinCAsign has implemented the security requirements and basic principles of the National Security Scheme (ENS), obtaining a High Level certification in accordance with the provisions of Royal Decree 311/2022, of May 3, which regulates the National Security Scheme.

5.4.1. Types of events recorded

VinCAsign produces and keeps record of at least the following events related to the entity's security:

- System start and shutdown.

- Attempts to create, delete, set passwords, or change privileges.
- Login and logout attempts.
- Attempted unauthorized access to the CA system through the network.
- Attempted unauthorized access to the file system.
- Physical access to logs.
- System configuration and maintenance changes.
- CA application logs.
- CA application start and shutdown.
- Changes to CA details and/or keys.
- Changes in the creation of certificate policies.
- Generation of own keys.
- Certificate creation and revocation.
- Records of the destruction of media containing keys and activation data.
- Events related to the lifecycle of the cryptographic module, such as receiving, using, and uninstalling it.
- The activities of firewalls and routers.
- The key generation ceremony and key management databases.
- Physical access logs.
- System maintenance and configuration changes.
- Personnel changes.
- Commitment and discrepancy reports.
- Records of the destruction of material containing key information, 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 organizational certificates.
- Possession of activation data, for operations with the private key of the Certification Entity.

- Complete reports of physical intrusion attempts in the infrastructures that support the issuance and management of certificates.
- Use of system resources, as well as its performance.
- Access and use of its network equipment and devices.
- Activation, shutdown, and pause of various logs.
- Environmental events.

Registry entries include the following items:

- Date and time of entry.
- Serial number or sequence of the entry, in automatic records.
- Identity of the entity entering the record.
- Type of entry.

5.4.2. Frequency of processing audit log

VinCAsign reviews its logs when a system alert is triggered by an incident.

The processing of audit records consists of a review of the records that includes verification that the records have not been tampered with, a brief inspection of all log entries, and further investigation of any alerts or irregularities in the records. Actions taken from the audit review are documented.

VinCAsign maintains a system that guarantees:

- Enough space for log storage
- That the log files are not rewritten.
- That the information stored includes at least: type of event, date and time, user executing the event and result of the operation.
- The log files shall be stored in structured files that can be incorporated into a database for later exploration.

5.4.3. Retention period for audit log

VinCAsign stores audit log information for at least 15 years.

5.4.4. Protection of audit log

System logs:

- They are protected against possible manipulation, erasure, or deletion by signing the files that contain them.
- They are stored in fireproof devices.
- Their availability is protected by storing them in facilities outside the centre where the CA is located.

Access to the log files is reserved for authorized persons only. Likewise, the devices are always handled by authorized personnel.

There is an internal procedure detailing the management processes for devices containing audit log data.

5.4.5. Audit log backup procedures

VinCAsign has an adequate backup procedure in place so that, in case of loss or destruction of relevant files, corresponding backup copies of the logs are available within a short period of time.

VinCAsign has implemented a secure backup procedure for audit logs, making a weekly copy of all logs on an external medium. Additionally, a copy is kept in an external custody centre.

5.4.6. Audit collection System (internal vs external)

Event audit information is collected internally and in an automated manner by the operating system, network communications and certificate management software, in addition to manually generated data, which will be stored by duly authorized personnel. All of this makes up the audit trail accumulation system.

5.4.7. Notification to event-causing subject

When the audit log accumulation system records an event, a notification does not need to be sent to the individual, organization, device, or application that caused the event.

5.4.8. Vulnerability assessments

Vulnerability scanning is covered by VinCAsign auditing processes.

Vulnerability scans must be run, reviewed, and revised through a review of these monitored events. These scans are run on a quarterly basis.

The systems audit data is stored to be used in the investigation of any incidents and to locate vulnerabilities.

5.5. Records archival

VinCAsign ensures that all information relating to certificates is retained for an appropriate period, as set out in section 5.5.2 of this policy.

5.5.1. Types of records archived

The following documents involved in the certificate lifecycle are stored by VinCAsign (or by the registration entities):

- All system audit data (PKI, TSA and OCSP).
- All data relating to certificates, including contracts with signatories and data relating to their identification and location.
- Requests for issuance and revocation of certificates, including all reports related to the revocation process.
- Any specific choices made by the signer or subscriber during the subscription agreement.
- Type of document presented in the certificate request.
- Identity of the Registration Entity accepting the certificate request.
- Unique identification number provided by the above document.
- All issued or published certificates.
- Issued CRLs or records of the status of generated certificates.
- History of generated keys.
- Communications between PKI elements.
- Certification Policies and Practices

- All audit data identified in section 5.4.
- Certification request information.
- Documentation provided to support certification requests.
- Certificate lifecycle information.

VinCAsign is responsible for the proper archiving of all this material.

5.5.2. Retention period for archive

VinCAsign stores the information records specified above for at least 15 years.

5.5.3. Protection of archive

VinCAsign protects the file so that only authorized persons can access it. The file is protected against viewing, modification, deletion, or any other manipulation by storing it in a reliable system.

VinCAsign ensures the proper protection of the archives by assigning qualified personnel to handle them and storing them in fireproof safes and off-site facilities.

5.5.4. Archive backup procedures

VinCAsign has an external storage centre to guarantee the availability of copies of the electronic file archive. Physical documents are stored in secure locations with access restricted to authorized personnel only.

VinCAsign at a minimum performs daily incremental backups of all its electronic documents and performs weekly full backups for data recovery purposes.

In addition, VinCAsign (or the organizations performing the registry function) keeps copies of paper documents in a secure location other than the Certification Authority own premises.

5.5.5. Requirements for time-stamping of records

The records are dated with a reliable source via NTP from the ROA.

VinCAsign has a procedure describing the time configuration of the equipment used in the issuance of certificates.

This information does not need to be digitally signed.

5.5.6. Archive collection system (internal or external)

VinCAsign has a centralized system for collecting information on the activity of the teams involved in the certificate management service.

5.5.7. Procedures to obtain and verify archive information

VinCAsign has a procedure that describes the process for verifying that archived information is correct and accessible.

5.6. Key changeover

Before the use of the CA private key expires, a key exchange will be performed. The old CA and its private key will only be used for signing CRLs if there are active certificates issued by that CA. A new CA will be generated with a new private key and a new DN.

The change of the subscriber's keys is materialized by performing a new issuance process.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

Backups of the following information are stored in storage facilities external to VinCAsign, which are made available in case of compromise or disaster: technical certificate request data, audit data and database records of all issued certificates.

Backups of VinCAsign private keys are generated and maintained in accordance with section 6.2.4. of this document.

5.7.2. Recovery Procedures if Computing resources, software and/or data are corrupted

When a resource, application or data corruption event occurs, the incident will be reported to security, and appropriate management procedures will be initiated, including escalation and incident investigation and response. If necessary, VinCAsign key compromise or disaster recovery procedures will be initiated.

5.7.3. Recovery procedures after key compromise

In case of suspicion or knowledge of VinCAsign compromise, the key compromise procedures will be activated, led by a response team that will evaluate the situation and develop an action plan, which will be executed under the approval of the Certification Entity's management.

In case of compromise of the VinCAsign private key, certificate statuses and revocation processes using this key may not be valid.¹⁷

In case of compromise of the CA private key, VinCAsign:

1. Inform its subscribers, users, and other CA with which it has agreements or other types of relationship of the key commitment. Such information may be made by posting a notice on its website <https://www.VinCAsign.net/>.
2. Shall indicate that certificates and revocation status information signed using this key or algorithms are invalid.

¹⁷ Section OVR-6.4.8-13 from ETSI EN 319 411-1

3. The last CRL for this CA shall be generated and published.
4. Shall notify browsers and software manufacturers that rely on its certificates, within the deadlines established in the respective CA admission policies.
5. Shall notify the National Supervisory Body and the reference security incident response team (CSIRT), or, where applicable, the competent authority in cybersecurity, within 24 hours after becoming aware of the compromise.

VinCAsign has developed a Contingency Plan to recover critical systems, if necessary, in an alternative data centre.

The case of root key compromise should be taken as a separate case in the contingency and business continuity process. This incident affects, in case of key replacement, the recognition by different private and public applications and services. A recovery of the effectiveness of the keys in terms of business will depend mainly on the duration of these processes. The contingency and business continuity document will address the purely operational terms for making the new keys available, but not their recognition by third parties.

Any failure to achieve the goals set by this Contingency Plan will be treated as reasonably unavoidable unless such failure is due to a breach of the CA obligations to implement these processes.

5.7.4. Business continuity capabilities after a disaster

VinCAsign will restore critical services (revocation and publication of revoked certificates) in accordance with the existing contingency and business continuity plan restoring the normal operation of the previous services within 24 hours after the disaster.

There is a Contingency Plan that defines the actions to be taken, resources to be used and personnel to be employed in the event of an intentional or accidental event that disables or degrades the certification resources and services provided by VÍNTEGRIS.

The main objectives of the Contingency Plan are:

- Achieve the greatest effectiveness of recovery operations through the establishment of three phases:
 - Assessment/Activation Phase, to detect, evaluate impacts and activate the plan.

- Recovery Phase, to restore services temporarily and partially until the damage caused to the original system has been recovered.
- Resumption Phase, to restore the system and processes to their normal operation.
- Identify the activities, resources, and procedures necessary for the efficient and effective completion of the three phases.

VinCAsign has alternatives, if necessary, for the implementation of the certification systems described in the business continuity plan.

5.8. VinCAsign termination

VinCAsign ensures that potential disruptions to subscribers and third parties are minimized because of the termination of the certification service provider's services and ensures continued maintenance of records required to provide evidence of certification in the event of civil or criminal investigation, by transferring them to a notarial repository.

Prior to termination of its services, VinCAsign develops a termination plan with the following provisions:

- Provide the necessary funds (through liability insurance and provision of own funds) to continue the termination of the revocation activities.
- It shall inform all Signatories/Subscribers, Relying Third Parties and other CAs with which it has agreements or other types of relationships, about the termination of the service:
 - If the service does not have issued certificates or does not have active or productive use, the notice may be reduced to the minimum period of 2 months established by the Current Regulations (Law 6/2020).
 - If the service has certificates or active productive use, the advance notice shall be done at least in 6 months.
- It shall revoke any authorization to subcontracted entities to act on behalf of the CA in the certificate issuance procedure.
- Transfer its obligations regarding the maintenance of registry information and logs for the indicated period to subscribers and users.
- Destroy or disable for use the CAs private keys.

- Maintain the active certificates and the verification and revocation system until the expiration of all issued certificates.
- Issue the last CRL before termination of service.
- Execute the necessary tasks to transfer the obligations of maintaining the registration information and event log files for the respective periods of time indicated to the subscriber and third parties relying on the certificates.
- It shall communicate to the Spanish Ministry of Industry, Energy and Tourism, at least 2 months in advance, the cessation of its activity and the destination of the certificates specifying whether their management is transferred and to whom or whether their validity will be extinguished.
- It shall also communicate to the competent Ministry regarding the opening of qualification of trusted electronic services any bankruptcy proceedings against VinCAsign as well as any other relevant circumstance that may prevent the continuation of the activity.

6. Technical security controls

VinCAsign uses reliable systems and products that are protected against tampering and guarantee the technical and cryptographic security of the certification processes they support.

6.1. Key pair generation and installation

6.1.1. Key pair generation

6.1.1.1. CA Key Pair Generation

The key pair of the intermediate certification authorities are created by the root certification authority "VinCAsign Qualified Authority" or by the root certification authority "CA Vintegris ROOT TrustServices", according to VinCAsign ceremony procedures, within the high security perimeter destined to this task.

The activities performed during the key generation ceremonies have been recorded, dated, and signed by all individuals participating in them, in the presence of a Notary or an Auditor. These records are kept for auditing and monitoring purposes for an appropriate period determined by VinCAsign.

Devices with FIPS 140 level 3 or Common Criteria EAL 4+ certifications (with ALC_FLR.1 enhancement) are used to generate the key for root and intermediate certification authorities.

VinCAsign QUALIFIED Authority	4.096 bits	25 year(s)
VinCAsign NEBULASUITE2 Authority	4.096 bits	13 year(s)
- End-entity certificates	2.048 bits	3 year(s)

CA Vintegris ROOT TrustServices	4.096 bits	25 year(s)
CA Vintegris TrustServices	4.096 bits	10 year(s)
- End-entity certificates	2.048 / 4.096 bits	3 year(s): 2048 bits 4 year(s): 4096 bits
Timestamp Unit	4.096 bits (RSA) 256 bits (ECDSA)	5 year(s)

More information in:

<https://policy.VinCAsign.net>

If VinCAsign qualified device is likely to lose its qualification as a Qualified Signature Creation Device (QSCD), VinCAsign will discontinue use of such device, seek alternative qualified devices for replacement, and notify Subscribers whose keys are current on such device. VinCAsign will revoke all those certificates that are in force at the time such device loses its qualification.

6.1.1.2. RA Key Pair generation

Not stipulated.

6.1.1.3. Subscriber Key Pair Generation

Signer's keys can be created by the Signer using hardware or software devices authorized by VinCAsign or can be created by VinCAsign.

The keys are generated using the RSA public key algorithm with a minimum length of 2048 bits.

In case of using secure signature creation device the device used for key generation shall be certified in accordance with the requirements of Annex 2 of Regulation (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

To maintain the above point, VinCAsign establishes the internal procedure "**VinCAsign Device Validity Management**".

6.1.1.3.1. *Signers' key generation in Remote Signature Service*

Signer's keys in the remote signature service (nebulaSIGN) are created by VinCAsign and are generated under the signer's unique control using a multifactor authentication scheme (it may include the signatory signature activation PIN).

Signers' keys are generated using the RSA public key algorithm with a length of 2048 bits, although the system is prepared to generate keys of longer length.

They are protected by the signature activation PIN, on which the PBKDF2 algorithm for key derivation is applied.

The keys are generated using FIPS 140-2 L3 and Common Criteria EAL4+ AVA_VAN.5 certified HSMs (see section 6.2.12 *Cryptographic storage for signer's keys*) that act as cryptographic hardware or QSCD, and a SAM appliance (Common Criteria certified) to allow the key activation on electronic signatures.

6.1.2. **Private key delivery to subscriber**

In certificates in a qualified signature creation device, the private key is duly protected inside the device.

In software certificates, the signer's private key is created either in the signature creation device and managed under the exclusive control of the holder from the NebulaSUITE platform, or in PKCS#12 format files, which contain the keys and certificates in duly encrypted files.

6.1.3. **Public key delivery to certificate issuer**

The method of forwarding the public key to the certification service provider is PKCS#10, another equivalent cryptographic proof or any other method approved by VinCAsign.

When keys are generated in a QSCD, VinCAsign ensures that the public key that is forwarded to the certification service provider comes from a key pair generated by that QSCD¹⁸.

¹⁸ Sections SDP-6.5.1-03, SDP-6.5.1-04, SDP-6.5.1-05 and SDP-6.5.1-06 from ETSI EN 319 411-2

6.1.4. CA public key delivery to relying parties

The VinCAsign keys are communicated to third parties that trust the certificates, ensuring the integrity of the key and authenticating its origin by publishing it in the Repository.

Users can access the Repository to obtain the public keys, and additionally, in S/MIME applications, the data message may contain a chain of certificates, which are then distributed to users.

The certificate of the root and subordinate CAs will be available to users on the VinCAsign web page.

6.1.5. Key sizes

The key length of the root Certification Authorities "VinCAsign Qualified Authority" and "CA Vintegris ROOT TrustServices" is 4096 bits.

The key length of the subordinate Certification Authorities "VinCAsign nebulasuite2 Authority", "CA Vintegris TrustServices" is 4096 bits.

The keys of the end-entity certificates are 2048 or 4096 bits.

6.1.6. Public key parameters generation and quality checking

The public key of the Root CA, Subordinate CA and Subscriber certificates are encrypted in accordance with RFC 5280.

The keys of the Root CA and Subordinate CAs are created with the RSA algorithm.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

The uses of the keys of the Certification Authorities' certificates are exclusively for signing certificates and CRLs.

The uses of keys for end-entity certificates for natural persons are exclusively for digital signature and non-repudiation.

The uses of keys for end-entity certificates for electronic seals are exclusively for digital signature, non-repudiation and encryption.

The uses of keys for web authentication certificates are for digital signature and encryption.

Supported Key Uses (KeyUsage field of X.509v3)

The parameters defined in the cryptographic suite 001 specified in the ETSI document TS 001 176-1 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" are used. ModLen=1024 is defined.

- Module length = 4096
- Key generation algorithm: rsagen1
- Padding method: emsa-pkcs1-v1_5
- Summary cryptographic functions: SHA256.
- Private Keys corresponding to ROOT Certificates shall not be used to sign Certificates except in the following cases:
 - a) Self-signed certificates to represent the ROOT CA itself.
 - b) Certificates for subordinate CAs and cross certificates.
 - a) Certificates for OCSP response verification

6.1.7.1. Signer key usage within remote signature service

The algorithms allowed in the remote signature service (SSASC) for use by the keys generated through this service are¹⁹:

- RSA-PKCS#1v1_5
- RSA-PSS
- sha256-with-rsa
- sha512-with-rsa

6.1.8. Key generation in software applications or capital assets

All keys are generated in capital assets, as indicated in section 6.1.1 of this document.

¹⁹ Following ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

In relation to the modules that manage VinCAsign and electronic signature certificate subscribers' keys, the level required by the standards indicated in the previous sections is ensured.

The European reference standard for qualified devices used as a secure signature creation device is the Commission Decision (EU) 2016/650 of April 25, 2016, which sets the standards for the evaluation of the security of the qualified devices for creating signatures and seals in accordance with article 30, section 3, article 39, section 2, and article 51.1 of Regulation (EU) n.° 910/2014 of the European Parliament and of the Council, relative to electronic identification and trust services for electronic transactions in the internal market

6.2.2. Private key (n out of m) multi-person control

Multi-person control is required for CA private key activation. In the case of this CPS, specifically there is a **2 out of 5** user policy for key activation.

The cryptographic devices are physically protected as determined in this document.

The CA facilities are equipped with continuous monitoring systems and alarms to detect, record and be able to act immediately in the event of an unauthorized and/or irregular access attempt to its resources.

6.2.3. Private key escrow

VinCAsign does not store copies of signer private keys.

6.2.4. Private key backup

VinCAsign makes a backup copy of the private keys of the Certification Authorities that make possible their recovery in case of disaster, loss, or damage. Both the generation of the copy and its recovery require, at least, the participation of two people.

These recovery files are stored in fireproof cabinets and in the external custody centre.

The subscriber keys in software can be stored for possible recovery in case of contingency in an external storage device separate from the installation key.

Signer keys in hardware cannot be copied as they cannot leave the cryptographic device.

6.2.5. Private key archival

The private keys of the Certification Authorities are archived for a period of **10 years after the issuance of the last certificate**. They will be stored in secure fireproof archives and in the Vintegris data centre. The collaboration of at least two people will be necessary to recover the private key of the CAs in the initial cryptographic device.

6.2.6. Private key transfer into or from a cryptographic module

The private keys of VinCAsign internal components are generated directly in the VinCAsign production cryptographic modules.

6.2.7. Private key storage on cryptographic module

6.2.7.1. CA private key storage

The CA private keys are stored encrypted in VinCAsign production cryptographic modules.

6.2.7.2. Signer's private key storage

- Keys generated in Nebula.

With the entry into operation of the electronic platform NebulaSuite²⁰ the private keys for the qualified electronic signature and the qualified electronic seal are generated exclusively on the cryptographic²¹ hardware provided for this function.

²⁰ Section 1.3.1.3 nebulaSUITE

²¹ Section 6.2.12 Cryptographic storage for signer's keys

- Keys generated in other certification authorities and imported into Nebula by its holder

With the entry into operation of the electronic platform NebulaSuite²² the private keys of the certificates of signatories/creators of seals of certification authorities other than VinCAsign can be imported by their holder into the NebulaSuite program, in which case they are stored in the cryptographic²³ hardware.

The possibility is only applicable in the case of advanced electronic signature or advanced electronic seal, and is carried out by the certificate holder himself, so that VinCAsign does not know the corresponding private key. The certificate holder must only proceed with this import if this action is not prohibited, or can be understood to be prohibited, by the trust service provider that issued the certificate being imported.

In any case it is not possible to import private keys of qualified electronic signature or qualified electronic seal to NebulaSuite.

This complies with Article 26(c) of EU Regulation 910/2014 which states that advanced electronic signatures must "have been created using electronic signature creation data that the signatory can use, with a high level of confidence, under his exclusive control," and with Article 36(c) of EU Regulation 910/2014 which states that advanced electronic seals must "have been created using electronic seal creation data that the seal creator can use, with a high level of confidence, under his exclusive control."

Likewise, and for the case of qualified electronic signature, the generation of the keys by the qualified provider enables compliance with Recital 51 of EU Regulation 910/2014 which indicates that it must be possible for the signatory to entrust qualified electronic signature creation devices to a third party provided that adequate procedures and mechanisms are in place to ensure that the signatory has exclusive control over the use of its electronic signature creation data and that the use of the device meets the requirements of the qualified electronic signature.

Finally, this reliable key generation environment complies with the generation of signature creation data on behalf of the signatory indicated in article 9.1.b) of Law 6/2020, of November 11, regulating certain aspects of trusted electronic services.

²² Section 1.3.1.3 nebulaSUITE

²³ Section 6.2.12 Cryptographic storage for signer's keys

It is confirmed that the private keys for signature or seal certificates are under the exclusive control of the signatory or the creator of the stamp.

6.2.8. Activating Private Keys

The VinCAsign private key is activated by the execution of the corresponding secure start procedure of the cryptographic module, by the persons indicated in section 6.2.2. of this document.

The CA keys are activated with a process of m of n (2 of 5).

The activation of the Intermediate CA private keys is handled with the same m of n process as the root CA keys.

6.2.9. Deactivating Private Keys

To deactivate the VinCAsign private key, follow the steps described in the corresponding cryptographic equipment administrator's manual.

On the other hand, the signer must enter the PIN for the new activation (if required).

6.2.10. Destroying Private Keys

Prior to the destruction of the private keys, a certificate revocation of the public keys associated with them will be issued.

Devices that have stored any part of the VinCAsign private keys will be physically destroyed or rebooted at a low level. For deletion, follow the steps described in the cryptographic equipment administrator's manual.

Finally, the backup copies will be securely destroyed.

The signer keys in software can be destroyed by deleting them, following the instructions of the application that hosts them.

The signer's keys in hardware can be destroyed by means of a special software application at the RA or VinCAsign premises.

6.2.11. Cryptographic Module Capabilities

The cryptographic modules are subjected to the engineering controls specified in the standards indicated throughout this section.

The key generation algorithms used are commonly accepted for the use of the key for which they are intended.

All VinCAsign cryptographic operations are performed on modules with FIPS 140 level 3 or Common Criteria EAL 4+ certifications (with ALC_FLR.1 enhancement).

6.2.11.1. Cryptographic storage of Root CA “VinCAsign QUALIFIED Authority” private key

The certificate key of the Root Certificate Authority "VinCAsign Qualified Authority" is stored in the Realsec HSM "Cryptosec 2048 by Realia Technologies S.L".

6.2.11.2. Cryptographic storage of SubCA “VinCAsign nebulaSUITE2 Authority” private key

The certificate key of the Subordinate Certificate Authority "VinCAsign nebulaSUITE2 Authority" is stored in the Primekey HSM "SafeGuard® CryptoServer Se of Utimaco IS GmbH".

6.2.11.3. Cryptographic storage of Root CA “CA Vintegris ROOT TrustServices” private key

The certificate key of the subordinate certificate authority "CA Vintegris ROOT TrustServices" is stored in the Primekey HSM "SafeGuard® CryptoServer Se of Utimaco IS GmbH".

6.2.11.4. Cryptographic storage of SubCA “CA Vintegris TrustServices” private key

The certificate key of the subordinate certificate authority "CA Vintegris TrustServices" is stored in the Primekey HSM "SafeGuard® CryptoServer Se of Utimaco IS GmbH".

6.2.12. Cryptographic storage for signer’s keys

The private keys of the centralized qualified certificates issued to subscribers, in the subordinate authorities are generated in the "nShield Connect XC" HSMs belonging to the "nShield Connect XC v12.60.15" family by using a SAM “Entrust Signature Activation Module v.1.0.4”.

6.3. Other aspects of key pair management

6.3.1. Public key archival

VinCAsign archives its public keys on a routine basis, in accordance with section 5.5 of this document.

6.3.2. Certificate operational periods and key pair usage periods

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, the private decryption key can continue to be used even after the expiration of the certificate.

6.4. Activation data

6.4.1. Activation data generation and installation

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

The creation and distribution of such devices is registered.

VinCAsign also securely generates the activation data.

6.4.2. Activation data protection

The activation data of the devices protecting the private keys of the root and subordinate Certification Authorities are protected by the holders of the cryptographic module administrator cards, as stated in the key ceremony document.

The signer of the certificate is responsible for the protection of his private key, with a password as complete as possible. The signer must remember this password.

6.4.3. Other aspects of activation data

Not stipulated.

6.5. Computer security controls

VinCAsign uses reliable systems to offer its certification services. VinCAsign has carried out IT controls and audits to establish a management of its IT assets adequate to the level of security required in the management of electronic certification systems.

About information security, VinCAsign follows the ISO 27001 certification scheme for information management systems.

The equipment used is initially configured with the appropriate security profiles by VinCAsign systems staff, in the following aspects:

- Security configuration of the operating system.
- Application security configuration.
- Correct sizing of the system.
- Configuration of users and permissions.
- Log events configuration.
- Backup and recovery plan.
- Antivirus configuration.
- Network traffic requirements.

6.5.1. Specific computer security technical requirements

Each VinCAsign server includes the following functionalities:

- Access control to SubCA services and privilege management.
- Imposition of separation of duties for privilege management.
- Identification and authentication of roles associated with identities.
- Archiving of subscriber and SubCA history and audit data.
- Security-related event auditing.
- Self-diagnosis of security related to SubCA services.
- SubCA system and key recovery mechanisms.

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

Verification of the certification of qualified devices (QSCD) is performed throughout the validity period of the certificate²⁴. Should the QSCD lose its certification as such, VinCAsign will notify users of this fact and execute a renewal plan for these devices (including the revocation of all affected certificates).

6.5.2. Computer security rating

The Certification Authority and registry applications used by VinCAsign are reliable.

6.6. Life cycle technical controls

6.6.1. System development controls

The applications are developed and implemented by VinCAsign according to development and change control standards.

The applications have methods for the verification of integrity and authenticity, as well as the correctness of the version to be used.

VinCAsign annually reviews its systems and applications involved in the management of the certificate issuance service and, in any case, whenever there is any relevant change that affects the applications or systems indicated.

6.6.2. Security management controls

VinCAsign develops the necessary activities to train and raise the security awareness of its employees. Training materials and process descriptions are updated after approval by a security management group. VinCAsign has an annual training plan for this function.

VinCAsign requires, by contract, the equivalent security measures from any external supplier involved in certification work.

In addition, VinCAsign will review its Security Policy at planned intervals and at least annually or whenever significant changes occur in the organization to maintain its suitability, adequacy and effectiveness.

²⁴ Section SDP-6.5.1-07 from ETSI EN 319 411-2

6.6.2.1. Classification and management of information and assets

VinCAsign maintains an inventory of assets and documentation and a procedure for the management of this material to ensure its use.

VinCAsign security policy details information management procedures where information is classified according to its level of confidentiality.

Documents are categorized into three levels: UNCLASSIFIED, INTERNAL USE, CONFIDENTIAL and SECRET/RESERVED.

6.6.2.2. Management operations

VinCAsign has an adequate incident management and response procedure, through the implementation of an alert system and the generation of periodic reports.

In the VinCAsign security document, the incident management process is developed in detail.

VinCAsign has documented the entire procedure related to the roles and responsibilities of the personnel involved in the control and handling of elements contained in the certification process.

6.6.2.3. Treatment of media and safety

All media are treated securely in accordance with information classification requirements. Media containing sensitive data are securely destroyed if they are no longer required.

6.6.2.3.1. System planning

The VinCAsign Systems department keeps a record of equipment capacities. In conjunction with the resource control application of each system, a possible resizing can be anticipated.

6.6.2.3.2. Incident reporting and response

VinCAsign has a procedure for the follow-up of incidents and their resolution, in which responses are recorded and an economic evaluation is carried out for the resolution of the incident.

6.6.2.3.3. Operational procedures and responsibilities

VinCAsign defines activities assigned to persons in a trusted role other than the persons in charge of day-to-day operations, which are not confidential.

6.6.2.4. Access system management

VinCAsign makes every effort reasonably within its power to confirm that system access is limited to authorized persons.

Particularly:

6.6.2.4.1. CA (general)

- It has controls based on firewalls, antivirus, and IDS (in high availability mode).
- Sensitive data is protected by cryptographic techniques or access controls with strong identification.
- VinCAsign has a documented procedure for managing user registrations and cancellations and access policy detailed in its security policy.
- VinCAsign has procedures to ensure that operations are performed in compliance with the role policy.
- Each person has an associated role to perform certification operations.
- VinCAsign staff is responsible for their actions through the confidentiality commitment signed with the company.

6.6.2.4.2. Certificate generation

Authentication for the issuance process is performed by a system m of n operators for the activation of the VinCAsign private key.

6.6.2.4.3. Revocation management

The revocation will be performed by strong authentication to the applications by an authorized administrator. The log systems will generate the evidence that guarantees the non-repudiation of the action performed by the VinCAsign administrator.

6.6.2.4.4. Revocation status

The revocation status application has access control based on certificate or two-factor authentication to prevent attempts to modify revocation status information.

6.6.2.5. Cryptographic hardware lifecycle management

VinCAsign ensures that the cryptographic hardware used for signing certificates is not tampered with during transport by inspecting the delivered material.

The cryptographic hardware is transported on prepared carriers to avoid any tampering.

VinCAsign records all relevant information from the device and adds to the asset catalogue.

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

VinCAsign performs periodic test runs to ensure the correct functioning of the device.

The cryptographic hardware device is only handled by trusted personnel.

The VinCAsign private signing key stored in the cryptographic hardware will be deleted once the device has been removed.

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

VinCAsign has a device maintenance contract. Changes or updates are authorized by the security manager and are recorded in the corresponding work logs. These configurations are performed by at least two reliable persons.

6.6.3. Life-cycle technical controls

As stated in section 6.6 of this document.

6.7. Network security controls

VinCAsign protects physical access to network management devices and has an architecture that sorts the generated traffic based on its security characteristics, creating clearly defined network sections. This division is done by firewalls.

Confidential information transferred over unsecured networks is encrypted using SSL protocols or VPN with two-factor authentication.

VinCAsign network security is tested and verified through annual eIDAS compliance assessment audits. In addition, VinCAsign is constantly striving to improve and use best practices to secure its networks.

VinCAsign considers the best practices and requirements specified by the industry, adhering, among others, to those established by CA/B Forum in the document Network and Certificate System Security Requirements²⁵.

6.8. Time-stamping

VinCAsign has its own time source, an NTP Stratum 1 in the facilities of the CPD of ATLASEdge Barcelona (Meinberg LANTIME M200/GPS model) with which it synchronizes all its services.

In addition, VinCAsign has a time synchronization procedure coordinated with the ROA Real Instituto y Observatorio de la Armada in San Fernando via NTP.

²⁵ Última versión accesible en <https://cabforum.org/network-security-requirements/>

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profile

All qualified certificates issued under this policy comply with X.509 version 3, RFC 3739, ETSI EN 319 412-1, ETSI EN 319 412-2, and ETSI EN 319 411-1, ETSI 319 411-2 and ETSI EN 319 401.

7.1.1. Version number(s)

VinCAsign issues X.509 Version 3 Certificates

7.1.2. Certificate Content and Extensions; Application of RFC 5280

The certificate extensions are detailed in the profile documents that are accessible from the VinCAsign website (<https://www.VinCAsign.net>).

This allows more stable versions of the CPS to be maintained by decoupling them from frequent adjustments to the profiles.

The value of the *commonName* field of the end-entity certificate subject will also be included in the *subjectAlternativeNames* extension.

7.1.3. Algorithm object identifiers

The signature algorithm object identifier is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- 1.2.840.113549.1.1.13 sha512WithRSAEncryption

The object identifier of the public key algorithm is:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Name forms

The certificates must contain the information necessary for their use, as determined by the corresponding policy.

7.1.5. Name constraints

The names contained in the certificates are restricted to "Distinguished Names" X.500, which are unique and unambiguous.

Additionally, name restrictions may be established in relation to certificates in the corresponding authentication, electronic signature, encryption or electronic evidence policy, provided that they are objective, proportionate, transparent and non-discriminatory.

7.1.6. Certificate policy object identifier

All certificates include a certificate policy identifier under which they have been issued, according to the structure indicated in section 1.2.1 of this document.

7.1.7. Usage of Policy Constraints extension

Not stipulated.

7.1.8. Policy Qualifiers syntax and semantics

Two PolicyQualifiers are used in the Certificate Policy extension:

- id-qt-cps: Contains the URL where the CPS can be found.
- id-qt-unotice: Certificate type identification.

7.1.9. Processing semantics for the critical Certificate Policies extension

The Certificate Policy extension allows you to identify the policy that VinCAsign associates with the certificate and where these policies can be found.

7.2. CRL profile

7.2.1. Version number(s)

CRLs issued by VinCAsign are version 2.

7.2.2. CRL and CRL entry extensions

This CPS supports and uses X.509 compliant CRLs.

7.3. OCSP profile

7.3.1. Version number(s)

According to the IETF RFC 6960 standard

7.3.2. OCSP extensions

Not stipulated.

8. Compliance audit and other assessments

VinCAsign as a certification service provider by the competent Ministry in the field of trusted electronic services will be subject to the control reviews that this body deems necessary.

VinCAsign is a company committed to the security and quality of its services by obtaining and maintaining the ISO/IEC 27001:2022 certification.

8.1. Frequency or circumstances of assessment

VinCAsign is being audited annually (in terms of compliance), in addition to the internal audits it performs at its own discretion or at any time due to a suspected breach of any security measure.

8.2. Identity/qualifications of assessor

The audits are performed by an external independent auditing firm that demonstrates technical competence and experience in computer security, information systems security and public key certification services compliance audits, and related elements.

8.3. Assessor's relationship to assessed entity

The auditing firms are of recognized prestige with departments specialized in the performance of computer audits, so there is no conflict of interest that could distort their performance in relation to VinCAsign.

8.4. Topics covered by assessment

The audit verifies with relation to VinCAsign:

- a) That the entity has a management system that guarantees the quality of the service provided.
- b) That the entity complies with the requirements of the CPS and other documentation related to the issuance of the different digital certificates.

- c) That the CPD and other related legal documentation is in accordance with what has been agreed by VinCAsign and with what is established in the current regulations.
- d) That the entity adequately manages its information systems.

In particular, the elements to be audited shall be the following:

- a) CA processes, RAs, and related elements.
- b) Information systems.
- c) Protection of the data processing centre.
- d) Documents

8.5. Actions taken as a result of deficiency

Once management has received the report of the compliance audit performed, the deficiencies found are analysed with the firm that performed the audit and a corrective plan is developed and implemented to address such deficiencies.

If the VínTEGRIS Certification Entity is unable to develop and/or implement such a plan or if the deficiencies found pose an immediate threat to the security or integrity of the system, it must immediately notify the VínTEGRIS Corporate Security Committee, which may take the following actions:

- Cease operations temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate CA service.
- Other complementary actions that may be necessary.

8.6. Communication of results

The audit results reports are delivered to the Corporate Security Committee of VínTEGRIS within a maximum of 15 days after the execution of the audit.

8.7. Self-Audits

VinCAsign performs an annual revision of its policies as procedures (following what is specified in section 1.5.3), and self-audits as stated in section 8.1.

9. Other business and legal matters

9.1. Fees

9.1.1. Certificate issuance or renewal fees

VinCAsign may establish a fee for the issuance or renewal of certificates, of which, if applicable, subscribers will be informed in a timely basis.

9.1.2. Certificate access fees

VinCAsign has not established any fees for access to certificates.

9.1.3. Revocation or status information access fees

VinCAsign has not established any fees for accessing certificate status information.

9.1.4. Fees for other services

Not stipulated.

9.1.5. Refund policy

Not stipulated.

9.2. Financial responsibility

VinCAsign has sufficient financial resources to maintain its operations and meet its obligations, as well as to address the risk of liability for damages, as set out in section 7.12.c) of ETSI EN 319 401-1, in relation to the management of the termination of services and cessation plan.

9.2.1. Insurance coverage

VinCAsign has a sufficient guarantee of coverage of its civil liability, through a professional liability insurance that complies with the provisions of Article 24.2.c) of Regulation (EU) 910/2014, with a minimum insured amount of €5,000,000.

9.2.2. Other assets

Not stipulated.

9.2.3. Insurance or warranty coverage for end-entities

VinCAsign has a guarantee of coverage of its civil liability sufficient, through professional indemnity insurance in accordance with Article 24.2.c) of REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014, with a minimum insured amount of €5,000,000.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The following information is kept confidential by VinCAsign:

- Certificate requests approved or denied, as well as all other personal information obtained for the issuance and maintenance of certificates, except for the information indicated in the following section.
- Private keys generated and/or stored by the certification service provider.
- Transaction records, including complete records and audit trails of transactions.
- Internal and external audit records created and/or maintained by the Certification Authority and its auditors.
- Business continuity and emergency plans.
- Security policy and plans.
- Documentation of operations and other operational plans, such as archiving, monitoring and other similar.
- All other information identified as "Confidential".

9.3.2. Information not within the scope of confidential information

The following information is considered non-confidential:

- Certificates issued or in the process of issuance.

- The binding of the subscriber to a certificate issued by the Certification Entity.
- The name and surname of the natural person identified in the certificate, as well as any other circumstance or personal data of the holder, if it is significant in terms of the purpose of the certificate.
- The e-mail address of the natural person identified in the certificate, or the e-mail address assigned by the subscriber, if it is significant in terms of the purpose of the certificate.
- The uses and economic limits outlined in the certificate.
- The period of validity of the certificate, as well as the date of issue and the expiration date of the certificate.
- The serial number of the certificate.
- The different statuses or situations of the certificate and the start date of each one of them, specifically: pending generation and/or delivery, valid, revoked, expired and the reason for the change of status.
- Certificate revocation lists (CRLs), as well as other revocation status information.
- The information contained in the certificate repositories.
- Any other information not indicated in the previous section.

9.3.3. Responsibility to protect confidential information

In accordance with Article 19.2 of the eIDAS Regulation, VinCAsign shall, upon any breach of security or loss of integrity that has a significant impact on the trust service provided or the personal data concerned, notify the competent national supervisor for electronic trust services no later than 24 hours after becoming aware of the breach and the relevant Data Protection Authority no later than 72 hours after becoming aware of the facts.

Legal disclosure of information

VinCAsign discloses confidential information only in the cases provided for by law.

In particular, the records that support the reliability of the data contained in the certificate, as well as records related to the reliability of the data and those related to the

operation²⁶, will be disclosed if required to provide evidence of the certification in a legal proceeding, even without the consent of the subscriber of the certificate.

The Certification Entity shall indicate these circumstances in the privacy policy provided in section 9.4 of this document.

Disclosure of information by request of its owner

VinCAsign includes, in the privacy policy provided for in section 9.4 of this document, prescriptions to allow the disclosure of the Subscriber's information and, if applicable, of the natural person identified in the certificate, directly to the Subscriber or to third parties.

9.4. Privacy of personal information

9.4.1. Privacy plan

VinCAsign has developed a privacy policy, and documented in this Statement of Trusted Practices the corresponding security aspects and procedures in accordance with *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (RGPD - General Data Protection Regulation) and the Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights (LOPDGDDD)*.

VinCAsign has a Register of Personal Data Processing Activities, where the "Certificate Management" processing is included, the purpose of which is the management of the certificates issued and the provision of associated certification services.

Likewise, VinCAsign has adopted the technical and organizational measures appropriate to the risk analysis carried out in relation to this treatment, ensuring the lawfulness and proportionality of the treatment, as well as that the principles of privacy by design and by default have been respected.

²⁶ Section REQ-7.10-04 from ETSI EN 319 401

9.4.2. Information treated as private

In accordance with the provisions of Article 4 of the General Data Protection Regulation (GDPR), personal data is any information relating to identified or identifiable natural persons.

To provide the service, VinCAsign needs to collect and store certain information, including personal data.

In corporate certificates, such information is collected through the subscribers, based on the corporate relationship that binds them to the signers (employees, positions, partners...), or in the rest of the certificates, directly from the affected parties, or through the Registration Entities, always in strict compliance with the conditions for legitimate processing referred to in Article 6 of the General Data Protection Regulation, and concordant of the LOPDGDD.

VinCAsign collects the data exclusively necessary for the issuance and maintenance of the certificate.

VinCAsign does not disclose or transfer personal data, except in the cases provided for in sections 9.3.2 to 9.3.6, and in section 5.8 of this document, in case of termination of the certification service.

Confidential information in accordance with the regulations on personal data protection is protected from loss, destruction, damage, falsification and unlawful or unauthorized processing, in accordance with the requirements set forth in this document in compliance with the General Data Protection Regulation, and the LOPDGDD.

In any case, the data collected by the Certification Service Provider, acting as data controller, must be treated with the level of security appropriate to the risk presented by its processing.

9.4.3. Information not deemed private

The following information is not qualified as private:

- a) The information contained in the certificates, since for their issuance the subscriber previously grants his consent, including the different states or situations of the certificate.
- b) Certificate revocation lists (CRLs), as well as other revocation status information.

9.4.4. Responsibility to protect private information

In accordance with Article 23 of Directive (EU) 2555/2022 and Article 24.2 f) ter of the eIDAS Regulation, vinCAsign, in the event of any security breach or loss of integrity that significantly impacts the trust service provided or the related personal data, will notify the competent national supervisory authority for trust services, the reference security incident response team (CSIRT), or, where applicable, the designated competent authority for cybersecurity, within 24 hours of becoming aware of the breach, and the relevant data protection authority within 72 hours of becoming aware of the incident.

9.4.5. Notice and consent to use private information

The user's authorization for the automated processing of the personal data provided for the provision of agreed services, as well as for the offer and contracting of other VinCAsign products and services, will be required by signing and accepting the binding legal instrument. Explicit consent will be obtained from the applicant for the processing of his/her biometric data in the case of using VinCAsign video identification system for the issuance of the certificate.

The information obtained is used both for the following purposes:

- The correct identification of users requesting customized services, necessary for the performance of a contract to which the data subject is a party or for the application at his request of pre-contractual measures, as well as compliance with a legal obligation applicable to the controller.
- The retention of the files and audit trails set out in 5.4.1 and 5.5.1 of this document, necessary for the fulfilment of a legal obligation applicable to the controller.
- The performance of statistical studies of registered users to design improvements in the services provided, carry out basic administrative tasks and to communicate incidents, offers and news to subscribers and users, necessary for the satisfaction of legitimate interests pursued by VinCAsign as data controller.

The personal information collected from registered users is stored by VinCAsign, which assumes the necessary technical and organizational security measures to ensure the confidentiality and integrity of the information, appropriate to the risks identified and in accordance with the provisions of the RGPD and the LOPDGDD.

The user will be responsible, in any case, for the accuracy and veracity of the data provided, VinCAsign reserves the right to exclude from the registered services to any user who has provided inaccurate or untruthful data or, without prejudice to other legal actions.

Any registered user may at any time exercise the rights of access, rectification and deletion of their personal data provided to VinCAsign, as well as those of opposition and limitation to its processing by written communication with reference "data processing" and proof of identity or representation.

The right to portability in relation to the information necessary for the issuance of certificates is limited to the provisions of point 5.8 regarding the termination of the service.

However, if the user considers that his right to the protection of personal data may have been violated, he may complain to the Spanish Data Protection Agency.

The data will be kept for the time necessary to fulfil the purpose for which they were collected, to determine the possible responsibilities that may arise from that purpose and from the processing of the data and to comply with legal obligations. In this regard, at a minimum, they shall be kept for the time necessary to comply with the record retention requirements set forth in section 5.5.2 of this document and the audit trails set forth in section 5.4.3 of this document.

9.4.6. Disclosure pursuant to judicial or administrative process

Personal data may be disclosed by VinCAsign without the prior consent of the subscriber in the context of legal proceedings, in compliance with a legal obligation and under formal court order.

9.4.7. Other information disclosure circumstances

Those described in paragraph 1 of Article 6 of the General Data Protection Regulation (GDPR).

No international data transfers are foreseen.

The provision of certification services by VinCAsign may involve the use of technological infrastructures located in external data centres, without this implying in any case an access or commissioning of processing of personal data by these providers. In such a case,

this relationship would be governed by a contract or other equivalent legal act that determines the conditions and guarantees of the processing assignment.

9.5. Intellectual property rights

9.5.1. Certificate ownership and revocation information

Only VinCAsign has intellectual property rights over the certificates it issues, without prejudice to the rights of subscribers, key holders and third parties, to whom it grants a non-exclusive license to reproduce and distribute certificates, free of charge, provided that the reproduction is complete and does not alter any element of the certificate, and is necessary in connection with digital signatures and/or encryption systems within the scope of use of the certificate, and in accordance with the documentation that binds them.

Additionally, certificates issued by VinCAsign contain a legal notice regarding the ownership of the certificate.

The same rules apply to the use of certificate revocation information.

9.5.2. Ownership of Certificate Practice Statement

Only VinCAsign has intellectual property rights over this Statement of Trust Practices.

This document is public and freely accessible. However, it is prohibited to modify, copy, reproduce, publicly communicate, transform, or distribute, by any means and in any form, all or part of the contents, for public or commercial purposes, without the prior and express written authorization of VinCAsign.

9.5.3. Ownership of the information related to names

The subscriber and, if applicable, the natural person identified in the certificate, retains all rights, if any, to the trademark, product or trade name contained in the certificate.

The subscriber is the owner of the distinguished name of the certificate, consisting of the information specified in section 3.1.1 of this document.

9.5.4. Key ownership

The key pairs are owned by the signatories, the natural persons who exclusively own the digital signature keys.

When a key is split into parts, all these parts of the key are owned by the owner of the key.

9.6. Representations and warranties

9.6.1. VinCAsign representations and warranties

VinCAsign guarantees, under its full responsibility, that it complies with all the requirements set out in the CPD, being solely responsible for compliance with the procedures described, even if part or all the operations are outsourced externally.

VinCAsign provides certification services in accordance with this Statement of Trust Practices.

Prior to the issuance and delivery of the certificate to the subscriber, VinCAsign informs the subscriber of the terms and conditions relating to the use of the certificate, its price, and limitations of use, by means of a subscriber agreement.

This information requirement is also fulfilled by a PDS document²⁷, also called disclosure text, which incorporates the contents of Annex A of the technical standard ETSI EN 319 411-1 v1.2.2 (2018-04), a document that can be transmitted by electronic means, using a durable means of communication over time, and in understandable language.

VinCAsign permanently communicates changes²⁸ in its obligations by publishing new versions of its legal documentation on its website to subscribers, key holders and third parties who trust certificates through this PDS, in written and understandable language, with the following minimum contents:

- Requirements to comply with sections 4.5.2, 4.5.3, 9.2, 9.13, 9.14, 9.15 and 9.16 of this document.

²⁷ “PKI Disclosure Statement”, or any applicable PKI disclosure document.

²⁸ Section REG-6.2.3-08 from ETSI EN 319 411-1

- Indication of the applicable policy, stating that the certificates are not issued to the public.
- A statement that the information contained in the certificate is correct, unless otherwise notified by the subscriber.
- Consent to the publication of the certificate in the repository and third-party access to it.
- Consent to the storage of the information used for the subscriber's registration and for the transfer of such information to third parties, in case of termination of operations of the Certification Entity without revocation of valid certificates.
- Limits of use of the certificate, including those established in section 1.4.2 of this document.
- Information on how to validate a certificate, including the requirement to check the status of the certificate, and about the conditions under which the certificate can be reasonably trusted, which is applicable when the subscriber acts as a third party relying on the certificate.
- How the liability of the Certification Entity is guaranteed.
- Applicable limitations of liability, including the uses in which the Certification Entity accepts or excludes its liability.
- Archiving period for certificate request information.
- Period for archiving audit records.
- Applicable dispute resolution procedures.
- Applicable law and competent jurisdiction.
- Whether the Certification Entity has been declared compliant with the certification policy and, if so, according to what system.

9.6.2. RA representations and warranties

The Registration Authorities are also obliged under the terms defined in this CPS for the issuance of certificates, primarily to

- a) Comply with the provisions of this CPS and the CPs corresponding to the type of certificate issued.

- b) Comply with the provisions of the contracts signed with the CA.
- c) Respect the provisions of the contracts signed with the Subscriber or signer.

Regarding life cycle of the certificates:

- a) Verify the identity of certificate applicants as described in this CPS or through another procedure that has been approved by VinCAsign.
- b) Verify the accuracy and authenticity of the information supplied by the subscriber or applicant.
- c) Inform the applicant, prior to the issuance of a certificate, of the obligations assumed, the manner in which the signature creation data must be stored, the procedure to be followed to report the loss or misuse of the signature creation and verification data or devices, its price, the precise conditions for the use of the certificate, its limitations of use and the manner in which it guarantees its possible liability, and the web page where any information from VinCAsign, the CPS, PDSs and CPs corresponding to the certificate may be consulted.
- d) To process and deliver the certificates as stipulated in this CPS.
- e) Formalize the certification contract with the subscriber as established by the applicable Certification Policy.
- f) Pay the established fees for the certification services requested.
- g) Archive the documents provided by the subscriber, for the period established in the current legislation.
- h) Inform the CA of the causes of revocation at the time it was aware of.
- i) Carry out communications with the subscribers or signers, by the means they consider appropriate, for the correct management of the certificate life cycle. Specifically, to carry out communications regarding the approaching expiration of the certificates and their suspensions, reinstatements, and revocations.

As Data Processor on behalf of the CA, the RA shall comply with all the obligations set forth in Article 28 of the General Data Protection Regulation (GDPR).

9.6.3. Subscriber representations and warranties

VinCAsign, in the documentation binding it to Subscribers and third parties relying on certificates, sets forth and disclaims applicable warranties and limitations of liability.

VinCAsign, at a minimum, warrants to Subscriber:

- That there are no factual errors in the information contained in the certificates, known, or made by the Certification Entity.
- That there are no factual errors in the information contained in the certificates, due to lack of due diligence in the management of the certificate request or in the creation of the certificate.
- That the certificates comply with all material requirements established in the Declaration of Trust Practices.
- That the revocation services and the use of the Repository comply with all material requirements set forth in the Statement of Trust Practices.

VinCAsign shall, at a minimum, guarantee to the third party relying on the certificate

- That the information contained or incorporated by reference in the certificate is correct, except where otherwise indicated.
- In the case of certificates published in the Repository, that the certificate has been issued to the subscriber identified therein and that the certificate has been accepted, in accordance with section 4.4 herein.
- That all material requirements set forth in the Statement of Trust Practices have been met in the approval of the certificate application and in the issuance of the certificate.
- The speed and security in the provision of the services, especially the revocation and Deposit services.

In addition, VinCAsign guarantees the subscriber and the third party that trusts the certificate:

- That the certificate contains the information that a qualified certificate must contain, in accordance with Annex 1 of REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.
- That, if it generates the private keys of the subscriber or, where appropriate, natural person identified in the certificate, its confidentiality is maintained during the process.

The responsibility of the Certification Entity, within the limits established.

9.6.4. Relying party representations and warranties

As provided in section 9.6.3 of this document.

9.6.5. Representations and warranties of other participants

Not stipulated.

9.7. Disclaimers of warranties

VinCAsign disclaims all other warranties that are not legally enforceable, except those referred to in section 9.6.3 of this document.

9.8. Limitations of liability

VinCAsign limits its liability to the issuance and management of certificates and subscriber key pairs supplied by the Certification Entity and may reject all guarantees that are not linked to obligations derived from current regulations (currently Law 6/2020, regulating certain aspects of electronic trust services and the eIDAS Regulation).

9.9. Indemnities

9.9.1. Subscriber compensation clause

VinCAsign includes in the contract with the subscriber a clause whereby the subscriber agrees to indemnify the Certification Entity from any damage arising from any action or omission resulting in liability, damage or loss, expenses of any kind, including legal and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occur:

- Falsity or misrepresentation made by the user of the certificate.
- Error by the user of the certificate when providing the application data, if the action or omission has involved fraud or negligence with respect to the Certification Entity or any person relying on the certificate.
- Negligence in the protection of the private key, in the use of a reliable system or in maintaining the necessary precautions to prevent the compromise, loss, disclosure, modification or unauthorized use of the private key.

- Use by the subscriber of a name (including common names, e-mail address and domain names), or other information in the certificate, that infringes intellectual or industrial property rights of third parties.

9.9.2. Relying certificate third-party indemnity clause

VinCAsign includes in the corresponding PDS a clause whereby the third party relying on the certificate agrees to indemnify the Certification Entity from any damage arising from any action or omission that results in liability, damage or loss, expenses of any kind, including legal and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes occur:

- Breach of the obligations of the third party relying on the certificate.
- Reckless reliance on a certificate, under the circumstances.
- Failure to check the status of a certificate to determine that it is not revoked.

9.10. Term and termination

9.10.1. Term

The CPS will enter into force at the time of its publication.

9.10.2. Termination

This CPS will be repealed when a new version of the document is published.

The new version will replace the previous document in its entirety.

9.10.3. Effect of termination and survival

Under the survival clause, certain rules will continue in force after the termination of the legal relationship between the parties. Until termination, the Certification Entity ensures that, at least the requirements contained in sections 9.6, 8 and 9.3 of this document, remain in force after the termination of the service and the general conditions of issuance/use.

9.11. Individual notices and communications with participants

Not stipulated.

9.12. Amendments

9.12.1. Procedure for amendment

All proposed changes to this CPS that may materially affect Subscribers, Users or third parties will be notified immediately to interested parties by publication on the VinCAsign website.

ARs may be notified directly by email or by telephone depending on the nature of the changes made.

9.12.2. Notification mechanism and period

The notification clause shall establish the procedure by which the parties notify each other of events or modifications.

9.12.3. Circumstances under which OID must be changed

Not stipulated.

9.13. Dispute resolution provisions

Víntegris establishes, in the subscriber contract and in the PDS, the applicable mediation and dispute resolution procedures. The procedure to be followed is described in the internal document "VINCASIGN proc disputes v1r1.pdf".

VinCAsign establishes, in the subscriber contract and in the PDS, a competent jurisdiction clause, indicating that international jurisdiction corresponds to Spanish judges.

Territorial and functional jurisdiction shall be determined by virtue of the rules of private international law and rules of procedural law that may be applicable.

9.14. Governing law

VinCAsign establishes, in the subscriber contract and in the PDS, that the legislation applicable to the provision of services, including the certification policy and practices, is the Spanish Law.

VinCAsign assumes the application of the following regulations:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 999/93/EC (eIDAS Regulation), as amended by Regulation (EU) 1183/2024 of the European Parliament and of the Council, of April 11, 2024, regarding the establishment of the European digital identity framework.
- REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)
- COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting minimum technical specifications and procedures for security levels of electronic identification means as referred to in Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (SRI2 Directive) (NIS 2).
- Implementing Regulation of Directive (EU) NIS2, of October 17, 2024, establishing the technical and methodological requirements for cybersecurity risk management measures and specifying in greater detail the cases in which an incident is considered significant in relation to trust service providers and other obligated entities.
- Law 6/2020, November 11, regulating certain aspects of electronic trust services.

- Law 39/2015, of October 1, 2015, on the Common Administrative Procedure of Public Administrations.
- Law 40/2015, of October 1, 2015, on the Legal Regime of the Public Sector.
- Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and Guarantee of Digital Rights (LOPD).
- Latest version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published at <http://www.cabforum.org> by the CA/Browser Forum.
- Order ETD/743/2022 of July 26, modifying the Order ETD/465/2021, of May 6, regulating the methods of remote video identification for the issuance of qualified electronic certificates.

9.15. Compliance with applicable law

VinCAsign declares compliance with Law 6/2020, of November 11, regulating certain aspects of electronic trust services, Regulation (EU) 910/2014 (eIDAS) as well as the regulations related to the previous point.

Should there be a discrepancy between the requirements published by Spanish laws and the requirements established by CA/B Forum (by any BR or EV Guidelines), this CPD may be brought in line with the national requirements, but VinCAsign shall be obliged to communicate such compliance to CA/B Forum.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

VinCAsign establishes, in the subscriber contract, and in the PDS the full agreement clause, it being understood that the legal document regulating the service contains the complete will and all the agreements between the parties.

9.16.2. Assignment

Not stipulated.

9.16.3. Severability

VinCAsign establishes, in the subscriber contract and in the PDS, the severability clause, by virtue of which the invalidity of a clause does not affect the rest of the contract.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Not stipulated.

9.16.5. Force Majeure

VinCAsign provides, in the subscriber contract and in the PDS, clauses limiting its liability in the event of unforeseeable circumstances and in the event of force majeure.

9.17. Other provisions

Not stipulated.