TSP Disclosure Statement

CA service

Statement types	Statement descriptions	Specific requirements
Entire agreement	A statement indicating that the disclosure statement is not the entire agreement, but only a part of it.	This document is an abstract of qualified certificate policy and practice statement documents and is intended to assist users of Notartel Qualified Electronic Signature CA in making informed trust decisions. This document is compliant with Annex A of ETSI EN 319 411-3.
CA contact info	The name, location and relevant contact information for the CA/PKI.	**Notartel S.p.A – S.B.** Qualified Trust Service Provider Via Flaminia 162 00196 - Roma Organization identifier 05364151000 Operating sites: Via Flaminia 162, 00196 Roma Via Giovanni Vincenzo Gravina 4, 00196 Roma Via Flaminia 133/135, 00196 Roma Phone: +39-0636769306 Fax: +39-0632650077 Mail: notartel@postacertificata.notariato.it esercizio@postacertificata.notariato.it Web: https://ca.notartel.it https://www.notartel.it
Certificate type, validation procedures and usage:	A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage	This statement applies to Qualified certificates for electronic signatures service provided by the Public Key Infrastructure (PKI) of Notartel. Public key qualified certificates are issued only to citizens by the qualified certification authority “Notartel Qualified Electronic Signature CA” (Notartel CA). Certificate Profiles and any other limitations of certified public keys issued by the Notartel CA are compliant with the ETSI EN 319 411-2.

Statement types	Statement descriptions	Specific requirements
		Qualified certificates are issued to citizens after verification of their identity. Verification of the individual and certificate request is carried out by the notary and his operators that that acts as Local Registration Authority (LRA). Qualified certificates are issued by Notartel CA and shall be used only in accordance with REGULATION (EU) No 910/2014 of the European Parliament.
Reliance limits	The reliance limits, if any.	Certificates issued and logs are preserved for at least 20 years in a preservation system, according to Italian law.
Obligations of subscribers	The description of, or reference to, the critical subscriber obligations.	Certificate users shall keep safe their credentials to sign, their PIN and their private key are intended only for personal use. Users must protect their tools to sign and to verify signatures from malware and any malicious code. If users want to disable their certificate, they must send a signed request to revoke the certificate. By applying for the certificate issuance, a subscriber agrees this Certificate Policy and the terms and conditions stated in the agreement. ✓ control of the access to devices containing his private key; ✓ immediately inform Primary Registration Authority when a private key, has been, or there is a reason to strongly suspect it would be compromised; ✓ do not create any electronic signature with its private key if the validity period of certificate has expired and certificate has been revoked or suspended; ✓ control the access to this software, media, and devices on which the keys or passwords are stored; ✓ make his private keys inaccessible to other persons; ✓ start a procedure of revocation in the case of security violation or security violation suspicion of his private key; ✓ apply qualified certificate and the corresponding private key only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in this document.
Certificate status checking obligations of relying parties	The extent to which relying parties are obligated to check certificate status, and references to further explanation.	Certificate status can be checked on the CRL available at http://crl.notartel.it/pki/crls/ca_notartel_2021.crl or through the OCSP Service (online certificate status protocol) at http://ocsp.notartel.it/

Statement types	Statement descriptions	Specific requirements
Limited warranty and disclaimer/Limitation of liability	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	The TSP is liable for the content of the certificate and for the issuance of the signature credentials to the users. The TSP is not responsible for the use of certificate made by the user, for the content of the signed document, for any incorrect usage of the personal credentials, and for any other liability not mentioned in CPS or Terms and Conditions.
Applicable agreements, certification practice statement, Certificate:	Identification and references to applicable agreements, certification practice statement, certificate policy and other relevant documents.	Terms and Conditions and the CPS are available from the URL https://ca.notartel.it/03_manuali.html
Privacy policy	A description of and reference to the applicable privacy policy.	The data protection policies adopted by the TSP are compliant with the Italian law about privacy and include the personal data of users, employees and sub-contractors. The systems are protected to ensure the integrity, availability and confidentiality of the personal data.
Refund policy	A description of and reference to the applicable refund policy.	Subscribers can complain about service issues by email, phone or fax to: ▪ Phone: +39 0636209306 ▪ Fax: +39 0632650077 ▪ Email: customercare@notartel.it Customer Care hours: Monday to Friday from 9:00 a.m. to 1:30 p.m. and from 2:30 p.m. to 6:00 p.m.
Applicable law, complaints and dispute resolution	Statement of the choice of law, complaints procedure and dispute resolution mechanisms.	For every other matter or thing, not specified or provided for in CPS or Terms and Conditions, the Italian Civil Code is applied. Every dispute or complaint regarding the execution of the service of the qualified certificates supply shall be under the exclusive jurisdiction of the Court of Rome.
CA and repository licenses, trust marks, and audit	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	The service is qualified according to the Regulation (EU) No 910/2014 and is accredited by "Agenzia per l'Italia Digitale" (AgID). The qualified service and TSP are audited, at least every 24 months, to confirm that they fulfil the requirements laid down in the Regulation. The qualified trust service provider submits the resulting conformity assessment report to the AgID to keep the accreditation.