DNV·GL

STATEMENT

Attestato No./Statement No.:
10000376189-MSC-DNV GL-ITA

Data di emissione/Initial date:
31 luglio 2020

This is to state that, as resulting from verification activities completed on the 2020-07-22,

TRUST ITALIA S.p.A.

Piazzale Bosco, 3/A – 05100 Terni (TR), Italy

has been found to conform to the standards:
ETSI EN 319 411-1 (1.2.2 - 2018/04);
ETSI EN 319 401 (2.2.1 - 2018/04);

for the Issuing and Management of "Digital Certification Service" provided by TRUST ITALIA S.p.A. as TSP CA.

The audit was performed as full annual audit at the TSP's location in Italy, Rome.
It took place from 2020-07-21 until 2020-07-22 and covered the period from 2019-05-19 to 2020-05-18.

This declaration is valid only referred to full audit report PRJN-96109-2019-AST-ITA – 2020-07-22.
This declaration is not valid and cannot be used to obtain the eIDAS Certification according to EU Regulation 910/2014.

Luogo e Data:
Vimercate (MB), 31 luglio 2020

Per l'Organismo

Zeno Beltrami
Management Representative

APPENDIX TO STATEMENT

Audit Requirements

The audit requirements are defined in the following technical specification:

- ETSI EN 319 411-1 (v 1.2.2 – 2018/04);
- ETSI EN 319 401 (v 2.2.1 – 2018/04);
- TRUST ITALIA Certification Practice Statement as per "cap 17 Audit".

The applicable ETSI certification policies are: NCP.

The audit object is the following TRUST ITALIA's Certification Authority services:

Issuing and management of NCP digital certificates;

Issuing and management of S/MIME certificates.

Observation period: 2019-05-19 – 2020-05-18.

Audit Results

The audit object fulfills all applicable requirements from the audit criteria, as detailed in Full Audit report PRJN-96109-2019-AST-ITA – 2020-07-22.

All requirements for a CA Practice according to rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy as detailed in "Audit Evidences Summary". The audited CA takes the responsibility for the requirements fulfilment.

The CA provides the certification service according to the definitions of the Certificate Practice Statement as detailed in "Audit Evidences Summary".

The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.

Currently the CA implements an Information Security Management System ISO/IEC 27001 Certified.

Root CA

- VERISIGN CLASS 1 PUBLIC PRIMARY CERTIFICATION AUTHORITY - G3,

SHA256 Fingerprint=CBB5AF185E942A2402F9EACBC0ED5BB876EEA3C1223623D00447E4F3BA554B65
OU = VeriSign Trust Network
OU = © 1999 VeriSign, Inc. - For authorized use only
CN = VeriSign Class 1 Public Primary Certification Authority - G3
O = VeriSign, Inc.
C = US
[Validity from 1999-10-01 to 2036-07-17]

- VERISIGN CLASS 2 PUBLIC PRIMARY CERTIFICATION AUTHORITY - G3

SHA256 Fingerprint=92A9D9833FE1944DB366E8BFAE7A95B6480C2D6C6C2A1BE65D4236B608FCA1BB
CN = VeriSign Class 2 Public Primary Certification Authority - G3
OU = VeriSign Trust Network
OU = © 1999 VeriSign, Inc. - For authorized use only
O = VeriSign, Inc.
C = US

[Validity from 1999-10-01 to 2036-07-17]

Intermediate CAs (issuing CAs)

- TRUST ITALIA CLASS 1 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=0A6482B8F3D4FB085786A373CBF8634EEB38DAF073F253340D23EB2770FF5C6A
CN = Trust Italia Class 1 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT
[expired 2020-07-08 - valid certificates are still present in the Audit Observation Period]

- TRUST ITALIA CLASS 2 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=8962A8B18287071F8E9581832DBD2A1B9C5F4561039981AC64A15FC74680BBAC
CN = Trust Italia Class 2 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT
[expired 2020-07-08 - valid certificates are still present in the Audit Observation Period]

- TRUST ITALIA CLASS 2 MANAGED PKI INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=1DC2DA46ADE3C1E7EBBE42E02F2E1A8E3BF7B1A3A63ABF198FD41768463E429C
CN = Trust Italia Class 2 Managed PKI Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT
[expired 2020-07-08 - valid certificates are still present in the Audit Observation Period]

- TRUST ITALIA CLASS 2 CA- G3

SHA256 Fingerprint=5040F179448145C3E9629D27343D3401DFF907C0D0807DA4AFDBB926D66A8C09
CN = Trust Italia Class 2 CA - G3
OU = Symantec Trust Network
O = Trust Italia S.p.A.
C = IT
[Validity from 2015-10-27 to 2025-10-27]

- Monte Titoli Client Auth CA – G2

SHA256 Fingerprint=84AD27EDA629E75DBFC7DBEB0C05E4B049D6B390F7EBDB05BB04ADA96C84A5EA
CN = Monte Titoli Client Auth CA - G2
OU = Class 2 Managed PKI Individual Subscriber CA
OU = Symantec Trust Network
O = Monte Titoli S.p.A.
C = IT

[Validity from 2015-10-27 to 2025-10-27]

- TRUST ITALIA CLASS 1 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=F6752416E6CBCF46EDB84EFFA2FCFAE4DC3A948482C2A491F238A94965189F20
CN = Trust Italia Class 1 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-06-27 to 2023-04-01]

- TRUST ITALIA CLASS 2 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=464EE6EB5DB42B918760EB6EA2D5EB378B399FD427674AE82E8D7A99602E1996
CN = Trust Italia Class 2 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-06-27 to 2023-04-01]

- TRUST ITALIA CLASS 2 MANAGED PKI INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=C2A2ECE5DF65100E84F8584F73576BCA4867392F9EA103A8FB85566E9408CF3F
CN = Trust Italia Class 2 Managed PKI Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-06-27 to 2023-04-01]

- TRUST ITALIA CLASS 1 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=3BF737ECFE51FABF337AD47D24735CE5EDE4C25408987F4BB90197F7E7461831
CN = Trust Italia Class 1 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-12-19 to 2023-04-01]

- TRUST ITALIA CLASS 2 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=F9CA60A90354D54EA235FC014FB1D44D6D943CACFCBDAA1D24167B52D4DF1223
CN = Trust Italia Class 2 Consumer Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-12-19 to 2023-04-01]

- TRUST ITALIA CLASS 2 MANAGED PKI INDIVIDUAL SUBSCRIBER CA - G2,

SHA256 Fingerprint=8FE44DD123EFE08A65D4A678E97B9A3846B3283148B065A692FDF52921E62A8F
CN = Trust Italia Class 2 Managed PKI Individual Subscriber CA - G2
OU = Terms of use at https://www.trustitalia.it/rpa (c)10
OU = VeriSign Trust Network
O = Trust Italia S.p.A.
C = IT

[Validity from 2019-12-19 to 2023-04-01]

Audit Evidences Summary

The ETSI specification contains the following:

General requirements - (ETSI EN 319 411-1 5.1)

The CA maintains compliant documentation and statement structure.

Effectiveness of trusted roles and responsibilities framework is based upon a Certified Quality Management System in place from several years and a Certified Information Security Management System is in place since 2019 February.

Appropriate readable documentation was promptly made available.

Adequate infrastructure is supporting Certificate Life cycle especially in terms of computer and network security controls.

Risk Assessment - (ETSI EN 319 401-5)

Trust Italia defined its Information Security Risk Assessment and Treatment Framework and the Risk Model is based on assets; with regards to the assessment scope, last record for the Risk Assessment for CA is dated 202-02-20 and related improvement plan is documented in Gannt project ISO 27001 tool (on line current version).

Certificate Policy e Certificate Practice Statement (ETSI EN 319 411-1: 4.1, 4.2, 5.2)

The CA maintains a compliant presentation of policies and practices, along with complete CA hierarchy, signature algorithms and parameters employed.

ETSI 319 411-1, applicable CP identifier is: NCP – Natural person CA certificates, issued both for single o under the management of a subscriber legal entity to which the natural person is affiliated. (ref. Digicert CP version 5.0 of 2020-02-06 par 1.2,1.4 and 3.2).

Certification Practice Statement [CPS] ver. 4.0 2020-03-31 is based upon DigiCert CP v5.0 (2020-02-06) and DigiCert CPS v5.0 (2020-02-06) referred above and complies the ETSI 319 411 requirement CP identifier "NCP base".

X.509 certificate include the statement "certificate policy" (rif RFC 3647 3.3): https://www.trustitalia.it/rpa "Relying Party Agreement" that links to all other applicable CP and CPS in any case available at https://www.trustitalia.it/cps

X.509 Key Usage allowed are: Digital Signature and Key Encipherment;

X.509 extended Key Usage : TLS web client Authentication, E-mail protection.

Certificate Policy name and identification (ETSI EN 319 411-1: 5.3)

The CA maintains certificates CP identifier. The identifiers for the certificate policies specified in the present document are listed above.

PKI participants (ETSI EN 319 411-1: 5.4)

The CA ensures specific roles to all involved parties (CA itself, subscribers, subjects, others identified by the CA). Specification of PKI are detailed in [CPS] par 1.3 and in [CPS] par 9, basically respecting the PKI Disclosure Statement Template proposed in ETSI 319-411-1 Annex A.

Certificate usage (ETSI EN 319 411-1: 5.5)

The CA ensures that the policies (listed above) place no constraints on the user community and applicability of the certificate.

Publication and repository responsibilities (ETSI EN 319 411-1: 6.1)

The CA ensures dissemination life cycle, that makes certificates available to subscribers, subjects and relying parties as per [CPS] cap 4; "Certificate Life Cycle Operational Requirements".

Operative sequence are documented in detail in Quality Management System procedures: PQ07 Certificate generation Practice, rev.2 2018-05-09 and PQ11 Delivery on site rev.2 2018-05-09.

Applicable terms and condition are made readily and available 7day 24h at https://www.trustitalia.it/rpa.

The CPS is published in the Repository at https://www.trustitalia.it/cps. Amendments to the CPS are also

posted at https://www.trustitalia.it/archivio/repository/updates/aggiornamenti-delle-procedure.pdf.

An additional downloadable tutorial document set is available at https://www.trustitalia.it/site/guide/030401/Download.html.

TSP Practices – Identification and authentication (ETSI EN 319 411-1: 6.2)

The CA ensures requirements for naming in certificates, verification of the identity of the subscriber and subject, updating due to change to the subject's attributes, revoking certificates.

Certificate naming compliant to X.509 including all required X.501 statements as described in [CPS] par 3.1.

Identification of subject identity:

For natural person combination of Identity national card hard copy plus recognized e-mail address (ref. [CPS] par 3.2.3).

For natural person under a "managed PKI" service is also required the verification of "legal identity" of the company (subscriber) that requires the service and a confirmation record of the person authorized to act on behalf of the organization/company (ref. [CPS] par 3.2.5).

Identification and authentication for revocation:

revocation conditions are described in [CPS] par. 4.9. CRLs is usually published every 24 hours. It is granted every seven days though (ref [CPS] par 4.9.7). Clause for revocation are explicated to the

subscriber in the contract Format: Digital Certificate Subscriber Agreement v.1.2 (May 2020) in Italian version [DCSA]. The legal responsibility for communication of a suspect compromised certificate is mainly deputed to the subscriber itself as stated [DCSA] "Art 7 Segnalazioni e Revoca".

TSP Practices - Certificate life cycle Operational Requirement (Generation and validation, dissemination, renewal, suspension and revocation) including Termination Plan (ETSI EN 319 411-1: 4.4, 6.1, 6.3, 6.4.9; ETSI EN 319 401: 7.12)

The CA ensures that certificate life cycle is maintained under controlled conditions.

Identity validation procedure for registration have been audited in field, key points highlighted are:

a) request and personal data submission is made directly from the subject or the subscriber (if a legal person) using a self-service procedure choosing and buying the certificate on the website https://trustitalia.it.

b) The CA require verification and order acceptance through a valid e-mail confirmation reply and request to attach a scan copy of a national ID-card.

c) secure procedure is granted to generate Certificate Key Pair. This is used to trig the request of Certificate generation in the Processing Center tool.

other relevant key points are:

a) CA public key used to generate the certificate are stored in HSM kept in physically secured environment (Terni Site) and subject to DR plan;

b) Re-key practice for valid certificates is not allowed for the intended scope. Certificates are ever revoked and then re-issued;

c) Suspension practices are not allowed for the intended scope;

d) Renew practice (validity extension) is not allowed (renew ever implies new key pair generation).

Due to Digicert CPS practices and platform constraint, Key escrow and recovery is provided just for HSM pre-generated key pairs using a dedicated backup equipment and managed with a special Key Ceremony procedure.

Termination Plan is described in [CPS] par 5.8. including: Termination condition; Preservation of archives; safeguard continuation of subscriber; handling of costs; SSCD device disposal.

In case of cessation of CA, continuation is granted by the CAroot Digicert, as per contract par.19.3 Terms and Termination (ref. CA root obligation to cover 1 year).

Facility, management, and operational controls (ETSI EN 319 411-1: 6.4; ETSI EN 319 401: 7.1, 7.2, 7.3, 7.4, 7.9, 7.10, 7.11)

The CA ensures physical, procedural, personnel, environmental and logical security conditions. Specific Computer and Network security controls have been found implemented.

Physical security:

A Physical Security Policy TRUST DOC A-11 2018-04-23 and SSI004 Physical Security Procedure ver. 7 of 2019-07-27 are issued.

It has been verified the perimeter layout of both sites (Rome and Terni). Different controls are in place to avoid damage, loss and interruption of business activities. Policy, procedure and both sites have been verified the current assessment.

In the Terni Data Center, that wards the CA infrastructure, the following evidences have been collected:

a) Physical access to the site is strictly controlled classifying the site areas in 7 security levels and providing safety barriers (doors and safe) protected by mixed physical (hard keys) and logical (badges; fingerprint devices and pin codes) measures. The access to each area is strictly limited to authorized personnel.

b) More protected areas concerned with certificate generation and revocation management services access and HSM infrastructures needs access credential of minimal two authorized persons used simultaneously.

c) Every entry and exit is logged, including the material picking of hard keys that is recorded in a paper register and written on a strip that seal the envelope that contains the Key.

d) Infrastuctures used for CA are doubled in HA mode

e) Infrastructures used for CA perimeter are protected from natural disaster, fire safety factors, structure collapse, plumbing leaks, theft, breaking and entering.

f) The 2nd redundancy criteria is applied to supporting utilities: power, UPS unit, Air conditioning system; telecommunications). An emergency electrical supply engine is available and monitored (30KW 200lt).

g) Business continuity and disaster recovery plan and exercises are provided; in CA perimeter Rome Datacenter is defined as the Disaster Recovery site. For further acknowledgment see the "Compromise and disaster recovery" section below.

Personnel security:

The TSP assures that employees engaged in CA practices possess the necessary expertise, reliability, experience, and qualifications and have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

In the Information Security Management System Framework all Roles Responsibility and authorities are documented (ref. doc ISMS Roles Responsibility and Authorities ver. 1 April 2018)

Roles and responsibilities are nominatively assigned in doc "Mansionario MPQ03-01 rev 4 of 2019-01-16".

Also the document "Information Security context requirement and scope ver.2 2018-04-30" refers details for functions appointed in the CA perimeter.

Personnel Screening and Management proceedings are referred in detail in the procedure "PQ03 – Gestione Risorse Umane rev.5 2019-02-11". A specific Non-Disclosure Agreement is requested to all employee (ref. doc. "MPQ03-12 Obbligo di fedeltà").

Segregation of duties guidelines has been verified. Applied VeriSign Processing Center SecAudit 2012-01-18 (at activity level).

Audit Logging procedures:

Incident Management Process is already in place and documented in "SSI003.1 Gestione degli Incidenti ver.2 2019-01-28" procedure. Incidents are recorded in internal WIKI tool "Elenco incidenti". Every incident recorded in WIKI is correlated to "CRM Sugar" remediation task.

In the observation period no incident was recorded impacting the CA.

System activities concerning access to IT systems, use of IT systems, and service requests are stably monitored. The CA perimeter is protected from unauthorised access using the IT intrusion detection system "Fail2ban" tool that automatically locks suspect malicious IP address and forward an alert to IT security staff.

Abnormal system activities are also monitored in same way, with specific focus on the availability and utilization of needed services with the TSP's network. Log are collected in real time and can be on-demand exported and analysed for investigation.

All events related to processing centre registration including requests for certificate re-key or renewal are logged. Certificate Life cycle Operations and related Audit Trail availability have been sampled e.g: Certificate issuing - Internal code number 270427 of 2020-04-16; Certificate Issuing - Internal Code 849011279 class2 of 2020-04-20; class2 certificate revoking for key compromise (wrong subject email) of 2020-05-18.

As per Digicert Policy constraint, log of all transaction are retained for 10 year plus 6 month after certificate validity cessation (above the minimum requirement for ETSI 319-411 par. 6.4.6), as documented in [CSP] par. 5.5.

Compromise and disaster recovery:

TSP's systems data necessary to resume CA operations are backed up and stored in safe places in Terni Site, making suitable to allow the TSP to timely go back to operations in case of incident/disasters.

Backup policies are documented in procedure "SSI003 ver.2 – Continuità Operativa 2019-01-28".

TRUST DOC A17.2 Business continuity plan ver.1 2018-04-23 – It consider disruptive scenario of total unavailability of primary Data Center. Disaster recovery strategy has the following key points: Cold devices (HSM and host servers) already available in the DR site Rome; daily synchronization of production platform and database in DR infrastructure in Rome; the acceptable RTO is considered 24h; Recovery team is permanently appointed.

Business continuity exercises are executed at least once per year and documented in the WIKI platform section "Registro Prove Allarmi": DR Pilot cold activation test on 2020-01-20 (RTO 8h) and restore test on 2020-02-06 (RTO 6h).

Technical Security Controls - Key Pair (ETSI EN 319 411-1: 6.5; ETSI EN 319 401: 7.8).

The CA ensures that key pairs life cycle is maintained under controlled conditions, including all technical conditions for network and computer security. A specific Cryptographic Policy is documented in "TRUST DOC A10 Cryptographic Policy ver.1 2018-04-23".

Key Pair generation practice is documented in [CPS] 4.5 and 6.1.

Cryptographic algorithm used are: Signature SHA256 with RsaEncryption; public key RsaEncryption (2048) [CPS] 7.1.3.

Intermediate CA certificate have been re-issued and are under current validity.

Relevant documents are:

a) TRUST DOC A10 Cryptographic Policy ver.1 2018-04-23;

b) TRUST DOC A13-1 Network Security Policy ver 1 2018-04-23;

c) PQ07 Certificate generation Practice, rev.2 2018-09-05;

d) PQ11 Delivery on site rev.2 2018-09-05.

Key Points verified are the following:

a) HSM are kept in physically secured environment in Terni Site, the HSM module used is Luna SA 5.2.

b) HSM activation modules safekeeping procedure have been examined (ref. docs: PQ15 - Data Center Access; SSI004 - Physical Security)

c) Subject Private keys are held by TRUST ITALIA just in the case of sub CA generation request (managed PKI service).

d) A Key ceremony procedure is available (ref. doc. PQ11) the whole sequence is documented on an hardcopy and each step submitted for signature to the involved persons coordinated by the Key Manager (at least two trusted employee plus the KM). The installation and recovery of the CA's key pairs in a secure cryptographic device require simultaneous control of at least two trusted employees.

e) Templates (script) repository for record the key ceremony (eg. Ref. docs "MPQ11-06 for "managed PKI" service) have been examined.

f) Video recording of the Key Ceremony is needed in case of recovery of HSM.

Specific Computer and Network security controls:

The CA ensures that user access of operators, administrators and system auditor to critical application related to the service is managed under an access policy strictly restricted for trusted role in the certificate life cycle. The Policy is documented in "PQ15 Gestioni accessi of 2018-04-19" and "PQ21 Lista autorizzati" and its application assessed during the audit.

Local network components (e.g. routers) are kept in a physically and logically secure environment inside the highest level (7) of secure area in Terni site.

For what concerns access to critical application for services, strong authentication SSH2 is applied. People are driven to the correct use of password and other internal policies into the procedure "IQ25 Indicazioni per utilizzo risorse aziendali".

It is at all no possible for Certificate Processing Center Users to modify any certificate status without a justified reason.

The entire local network, including the specific CA service dedicated and segregated segment, is mapped in a Configuration Management Data Base documented in "Generic High lever Network Diagram – Pilot & Production" managed by IT administrators.

Certificate management infrastructure physically and logically separated. In particular, the front-end used for to collect subjects and subscribers request is firewalled vs the back-end platform and information are transferred using SSL/TSL strong encryption

A network Intrusion Detection professional tool "Fail2ban" is used to protect services over internet (ref Network security policy TRUST DOC A-13). Also, for unauthorized access attempts coming from inside the local network the CA perimeter is protected through "Fail2ban". The monitoring tool Nagios is active on the Local Network basically for to detect any kind of unproper traffic behavior.

For security purposes, wireless network is forbidden in whole company.

Capacity demand are monitored within the Information Security Management System practices and regularly reviewed during Management Review.

As per ETSI 319-401 req.7.8-13 a regular (yearly based) vulnerability scan on all public and private IP addresses of CA network infrastructure is performed by an independent professional company (Ref HEMMELER PARTNERS agreement signed on 2019-05-27) and a reliable report and record evidence that each vulnerability scan has shown (ref Security penetration test performed in 2019 June and reported on 2019-06-23).

Certificate, CLR and OCSP Profile (ETSI EN 319 411-1: 6. 6)

Certificate profile meets the requirements specified in Recommendation ITU-T X.509

As per X.509 requirement the CLR link is embedded in the Certificate statement. The "distribution point" is declared, as specified below, for each "SubCA" certificates type as well as "End User" type as declared in the audit scope (see Audit Results section):

SubCA

TRUST ITALIA CLASS 1 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2: URL=http://s.symcb.com/pca1-g3.crl

TRUST ITALIA CLASS 2 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2: URL=http://s.symcb.com/pca2-g3.crl

TRUST ITALIA CLASS 2 MANAGED PKI INDIVIDUAL SUBSCRIBER CA - G2: URL=http://s.symcb.com/pca2-g3.crl

Monte Titoli Client Auth CA – G2: URL=http://onsitecrl.trustitalia.it/offlineCA/Class2CAG3.crl

End User:

Classe 1: URL=http://onsitecrl.trustitalia.it/TrustItaliaSpAConsumerServiceCenterClass1G2/LatestCRL.crl

Classe2: URL=http://onsitecrl.trustitalia.it/TrustItaliaSpAConsumerServiceCenterClass2G2/LatestCRL.crl

MPKI: URL=http://onsitecrl.trustitalia.it/OnSitePublic/LatestCRL

Monte Titoli Client Auth CA – G2:

URL=http://onsitecrl.trustitalia.it/MonteTitoliSpAMonteTitoliClientAuthG2/LatestCRL.crl

CRL is maintained updated on 24h based at 12 am, but after decision, the revocation of a single certificate is made effective immediately (few seconds latency).

OCSP is available as feature but not implemented by default (ref. [CPS] par. 4.9.10), but it can be contractually requested paying a supplementary fee.

The server used for CRL and OCSP has been verified NTP synchronized in real time (ref. TRUST DOC A12-6 par. 2.5).

Compliance audit and other assessment (ETSI EN 319 411-1: 6.7)

The CA ensures full availability to third-party CB auditing activities and ensures full collaboration at all stages.

Other Business and Legal Matter including Privacy (ETSI EN 319 411-1: 6.8; ETSI EN 319 401: 7.13; EU 679/2016)

Compliance for applicable legal matter has been audited.

Contractual legal issues are addressed in the document "Condizioni Generali di Contratto Trust Italia S.p.A ver.1.3 2019 May", that must be undersigned (also digitally) by the subscriber (both individual or client company referent person).

Digital Certificate Subscriber Agreement updated in v.1.2 2019 May has been verified in detail. Warranties are described in sec. 3 of this document. Disclaimers of Warranty and Limitations of liability in sec 5. Intellectual Property Rights are described in sec 4. Dispute resolution Procedures and compliance with applicable law are both covered by sec 9 General Provisions. Privacy of Personnel information is described in sec 7. and in the actual CPS.

Proper information related to PKI Disclosure Statement Template proposed in ETSI 319-411-1 Annex A are also detailed in [CPS] par 9.

The document has been verified with respect addressing all specific ETSI EN 319 411 obligations.

Specific ticks on the on-line service requesting form assure full taking charge of contractual obligations (ref https://www.trustitalia.it/enroll/clientcsc.php?cod_prodotto=193 – form on line)

For what concerns Financial Responsibility it has been verified documentation that confirms the adequate financial ranking level declared by the bank "Banco Popolare on 2015-11-02". Besides, company maintains different type of Insurance policies e.g.: 30217091 – Professional Services; 60118825 Civil Responsibility to third parties; 6593958, 5788231, A23/00185 – Facilities and Infrastructures.

6.9 Other provisions (ETSI EN 319 411-1: 6.9; ETSI EN 319 401: 7.1, 7.13)

Internal organization reliability has been Audited vs. ETSI EN 319 401 7.1 requirements.

As per applicable [CPS] the CA organization area concerned with certificate life cycle is independent of other organizations for its decision relating to certificate provision service, and the audit has no revealed any commercial, financial and other pressures which might adversely influence trust in the services it provides.

As per Digicert contractual requirement, the CA can provide the capability to allow third parties to check and test all the certificate types.

The use of services provided are, where feasible, made accessible for person with disabilities.