DNV·GL

STATEMENT

Statement No.:
10000287935-Assessment Services-DNV GL-ITA

Initial date:
18 july 2019

This is to state that, as resulting from verification activities completed on the 9th of July 2019,

TRUST ITALIA S.p.A.

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

has been found to conform to the standard:
ETSI EN 319 411-1 (1.2.2)
ETSI EN 319 401 (2.2.1)

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

This statement is valid only if referred to full audit report:
"PRJN-96109-2019-AST-IT_Assessment Report, Rev. 1".

The audit activity covered the observation period from the 19th of May 2018 to the 18th of May 2019.

This declaration is not valid as and cannot be used to obtain the eIDAS Certification according to EU Regulation 910/2014.

Place and Date:
Vimercate (MB), 18 july 2019

For the Certification Body

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: 19/05/2018 – 18/05/2019

Audit Results

The audit object fulfills all applicable requirements from the audit criteria, as detailed in Full Audit report PRJN-96109-2019-AST-IT_Assessment Report, Rev. 1. 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 fulfillment. 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. Actually, the CA implements an Information Security Management System ISO/IEC 27001 Certified.

Root CA

VERISIGN CLASS 1 PUBLIC PRIMARY CERTIFICATION AUTHORITY - G3,
SHA256
fingerprint=CB:B5:AF:18:5E:94:2A:24:02:F9:EA:CB:C0:ED:5B:B8:76:EE:A3:C1:22:36:23:D0:04:47:E4:F3:BA:55:4B:65
C = US
O = VeriSign, Inc.
OU = VeriSign Trust Network
OU = © 1999 VeriSign, Inc. - For authorized use only
CN = VeriSign Class 1 Public Primary Certification Authority - G3

VERISIGN CLASS 2 PUBLIC PRIMARY CERTIFICATION AUTHORITY - G3
SHA256
Fingerprint=92:A9:D9:83:3F:E1:94:4D:B3:66:E8:BF:AE:7A:95:B6:48:0C:2D:6C:6C:2A:1B:E6:5D:42:36:B6:08:FC:A1:BB
C = US
O = VeriSign, Inc.
OU = VeriSign Trust Network
OU = © 1999 VeriSign, Inc. - For authorized use only
CN = VeriSign Class 2 Public Primary Certification Authority - G3

Intermediate CAs (issuing CAs)

TRUST ITALIA CLASS 1 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,
SHA256
Fingerprint=0A:64:82:B8:F3:D4:FB:08:57:86:A3:73:CB:F8:63:4E:EB:38:DA:F0:73:F2:53:34:0D:23:EB:27:70:FF:5C:6A
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

TRUST ITALIA CLASS 2 CONSUMER INDIVIDUAL SUBSCRIBER CA - G2,
SHA256
Fingerprint=89:62:A8:B1:82:87:07:1F:8E:95:81:83:2D:BD:2A:1B:9C:5F:45:61:03:99:81:AC:64:A1:5F:C7:46:80:BB:AC
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

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

SHA256
Fingerprint=1D:C2:DA:46:AD:E3:C1:E7:EB:BE:42:E0:2F:2E:1A:8E:3B:F7:B1:A3:A6:3A:BF:19:8F:D4:17:68:46:3E:42:9C
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

- Monte Titoli Client Auth CA – G2

SHA256
Fingerprint=84:AD:27:ED:A6:29:E7:5D:BF:C7:DB:EB:0C:05:E4:B0:49:D6:B3:90:F7:EB:DB:05:BB:04:AD:A9:6C:84:A5:EA
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

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 from 2019 Feb. Appropriate readable documentation made available promptly.
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 has defined its Information Security Risk Assessment and Treatment Framework, the Risk Model is based on assets; for what concerns the assessment scope last record for the Risk assessment for CA Perimeter is dated 01 of June 2018.

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: 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.
Certification Practice Statement [CPS] ver. 3.9 15-05-2019 based upon VeriSign Trust Network template specification, complies the ETSI 319 411 requirement CP identifier “NCP base”.
X.509 certificate include the statement “certificate policy” (ref RFC 3647 3.3): www.trustitalia.it/rpa “Relying Party Agreement” that links in contains links to other applicable CP and CPS 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).

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 sequences are documented in detail in Quality Management System procedures: PQ08 Certificate generation Practice, rev 2 09-05-2018 and PQ11 Delivery on site rev 2 09-05-2018
Applicable terms and condition are made readily and available 7day 24h at https://www.trustitalia.it/repository/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 tutorial 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 (ref. [CPS] par 3.2.5).
Identification and authentication for revocation: revocation conditions are described in [CPS] chap. 4.9. Maximum delay time for revocation is granted in 24h through CRL publication (ref [CPS] par 4.9). Clause for revocation are explicated to the subscriber in the contract Format: Digital Certificate Subscriber Agreement v 1.0 (April 2019) 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 on 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 for to generate subject key Pair, limited used to trigger the request of Certificate generation in the Symantec 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 Cerimony 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, and 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 23-04-2018 and SSI004 Physical Security Procedure ver. 7 of 27/02/2019 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) Infrastructures 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 2n 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
For CA perimeter Rome Datacenter is defined 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 16/01/2019"
Also, the document "Information Security context requirement and scope ver. 2 30/04/2018" 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 11/02/2019. 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 Jan 18,2012 (at activity level).

Audit Logging procedures:
Incident Management Process is already in place and documented in "SSI003.1 Gestione degli Incidenti ver. 2 28-01-2019" procedure. Incidents are recorded in internal WIKI tool Elenco incidenti. Every incident recorded in WIKI is correlated to "CRM Sugar" remediation task.
System activities concerning access to IT systems, use of IT systems, and service requests are stably monitored. The CA perimeter is protected from unauthorized 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 analyzed for investigation.
All events related to processing center registration including requests for certificate re-key or renewal are logged. Certificate Life cycle Operations and related Audit Trail have been sampled e.g.: Internal Code 227989 class2 of 24/04/2019 and 227663 class1 of 11/04/2019.
As per Digicert Policy constraint, log of all transactions are retained for 10 year plus 6 month after certificate validity cessation, 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 28-01-2019
TRUST DOC A17.2 Business continuity plan ver. 1 23-04-2018 – 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 documented in the WIKI platform section "Registro Prove Allarmi": DR Pilot cold activation restore test 24-01-2019 (RTO 8h) and 8-02-2019 (RTO 6h)

Technical Security Controls - Key Pair (ETSI EN 319 411-1 6.5, ETSI EN 319 401 7.5).

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 23-04-2018.
Key Pair generation practice is documented in [CPS] 4.5 and 7.1.3
Cryptographic algorithm used are: Signature SHA256 with RsaEncryption; public key RsaEncryption (2048)
Intermediate CA certificate is under current validity (expiration 2020 July)
relevant documents are:
a) TRUST DOC A10 Cryptographic Policy ver. 1 23-04-2018
b) PQ08 Certificate generation Practice, rev 2 09-05-2018
c) PQ11 Delivery on site rev 2 09-05-2018
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
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 in 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 (e.g. Ref docs MPQ11-06 for "managed PKI" service) have been examined
f) Video recording 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 19/04/2018" 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 segregated. 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.

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

Class 2: 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 Maggio 2019", that must be undersigned (also digitally) by the subscriber (both individual or client company referent person).
Digital Certificate Subscriber Agreement updated in v 1.0 2019 April" 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.
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 in 02/11/2015". 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