DNV·GL

STATEMENT

Statement No.:
266517-2018-OTH-ITA-DNV

Initial date:
18 may 2018

Valid:
18 may 2018 - 18 may 2019

We hereby declare that

TRUST ITALIA S.p.A.

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

Is compliant to the following European Standards:

ETSI EN 319 411-1 (1.1.1)
ETSI EN 319 401 (2.1.1)

for issuing and management of:

“Digital Certification Service” provided by TRUST ITALIA S.p.A. as TSP CA

This declaration is valid only if referred to full audit report:
PRJC-566736-2017-MSC-AUT – 1- 1.1, on date 18th may 2018

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

Place and date:
Vimercate (MB), 18 may 2018

For the Certification Body

Zeno Beltrami

Zeno Beltrami
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.

Annex to Statement

Audit Report
Report N. PRJC-566736-2017-MSC-AUT – 1 – 1.1
Date 12th june 2018

Audit Requirements
The audit requirements are defined in the following technical specification:
ETSI EN 319 411-1 (v 1.1.1 – 2016/02)
ETSI EN 319 401 (v 2.1.1 – 2016/02)

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

TRUST ITALIA Certification Practice Statement as per "Summary of the Audit requirements"
Certificate Policy for S/MIME as per "Summary of the Audit requirements"
Observation period: 04/24/2018 – 05/18/2018

Audit result
The audit object fulfills all applicable requirements from the audit criteria, as detailed in Full Audit report PRJC-566736-2017-MSC-AUT 05/18/2018
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 per "Summary of the Audit requirements"
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 per "Summary of the Audit requirements".
The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.

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

- 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

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

- 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

- 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

Summary of the audit requirements

The ETSI specification contains the following requirements and related assessment evidences:

5.1 General requirements

The CA maintains compliant documentation and statement structure
Effectiveness of trusted roles and responsibilities framework based upon a Certified Quality Management System in place from several years
Appropriate readable documentation made available promptly
Adequate infrastructure supporting Certificate Life cycle especially in terms of computer and network security controls

5.2 Certification Practice Statement requirements

The CA maintains a compliant presentation of policies and practices, along with complete CA hierarchy, signature algorithms and parameters employed.
Scope perimeter – Natural person CA certificates issued both for single o under the management of a subscriber legal entity to which the natural person is affiliated.
ETSI 319 411-1, applicable CP identifier: NCP
[CPS] Certification Practice Statement ver. 3.8 24-10-2011 based upon VeriSign Trust Network template specification, has been integrated by a [TSPS] Trust Service Practice Statement ver. 1 13-04-2018 to comply 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 another applicable CP and CPS
X.509 Key Usage allowed are: Digital Signature and Key Encipherment
X.509 extended Key Usage: TLS web client Authentication, E-mail protection

5.3 Certificate Policy name and identification

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

5.4 PKI participants

The CA ensures specific roles to all involved parties (CA itself, subscribers, subjects, others identified by the CA).

5.5 Certificate usage

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

6.1 Publication and repository responsibilities

The CA ensures dissemination life cycle, that makes certificates available to subscribers, subjects and relying parties.
[CPS] par 4; “Certificate Life Cycle” described in detail in Quality Management System procedures:
PQ08 Certificate Generation Practice, rev 2 09-05-2018
PQ11 Delivery on site rev 2 09-05-2018
Applicable terms and condition are made readily and available 7day 24h
https://www.trustitalia.it/repository/rpa (also in Certificate policy statement)
https://www.trustitalia.it/site/guide/030401/Download.html
and linked documents

6.2 Identification and authentication

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 email address (ref [CPS] par 3.2.1).
- for natural person under a "managed PKI" service is also required the verification od legal identity of the company (subscriber) that requires the service (ref. [CPS] par 3.2.5).
- Identification and authentication for revocation: revocation conditions described in [CPS] par 4.9.
- Maximum delay time for revocation is granted in 24h (ref [TSPS] par 4.9)
- Digital Certificate Subscriber Agreement v 1.0 (June 2011) [DCSA]
- The legal responsibility for communication of a suspect compromised certificate is mainly deputed to the subscriber itself as stated [DCSA] Art 2 Revocation

6.3 Certificate Life-Cycle operational requirements

The CA ensures that certificate life cycle is maintained under controlled conditions.
Identity validation procedure for registration have been audited in field, key point highlighted:

- request and personal data submission directly from the subject or the subscriber (if a legal person) using a self-service procedure on https://trustitalia.it
- request verification and order acceptance through email confirmation and request to deliver a scan copy of a national ID-card
- secure procedure for to generate subject key Pair, limited used to trigger the request of Certificate generation in the Symantec processing center tool

6.4 Facility, management, and operational controls

The CA ensures physical, procedural, personnel, environmental and logical security conditions.
Specific Computer and Network security controls:

- 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 is used to protect services over internet (ref Network security policy TRUST DOC A-13)
- Local network components are kept in a both physically and logically secure environment (ref Network security policy TRUST DOC A-13)
- For security purposes, wireless networks are forbidden in whole company
- Logging policies and practices have been examined

Physical Security Policy issued on 23/04/2018. It has been verified the layout of both sites (Rome and Terni). Different controls are in place to avoid damage, loss and interruption of business activities. A structured ISO 27001 approach on the definition of controls has been approved and will be verified during the ISO27001 certification process that is initiated.

Datacenter Access Policy applied for Terni site has been, recently, adopted by Rome site too.

- PQ15 Gestioni accessi on 19/04/2018 has been reviewed.
- PQ21 Lista autorizzati and Procedura accesso fisico. With regards to access to critical services strong authentication SSH2 is applied.
- IQ25 Indicazioni per utilizzo risorse aziendali is the reference document for the communication of Password Management rules and other internal Policies.
- Verified the Generic High Level NW diagram – Pilot & Production
- Verified the documentation where all LOG types have been listed. ELENCO LOG 2014. This document is rarely modified because the service is unchanged from
- Some logs have been verified as LOG ADMIN Secure.
- LOGWATCH is the monitoring tool verified every morning.

6.5 Technical security controls

The CA ensures that key pairs life cycle is maintained under controlled conditions, including all technical conditions for network and computer security.
Key Points:

- HSM kept in physically secured environment (Terni Site) and subject to DR plan - HSM module used Luna SA
- HSM activation modules safekeeping procedure have been examined

- Subject Private keys are held by TRUST ITALIA just in the case of sub CA generation request (managed PKI service).
- Ref docs MPQ11-06, examined Templates (script) repository for record the key ceremony (e.g. "managed PKI" service.
- Key ceremony sequence is documented in a hardcopy and each step submitted for signature to the involved persons coordinated by the Key Manager (at least two trusted employees plus the KM).
- Videorecording the KC is needed in case of recovery of HSM

Key Pair generation practice [CPS] 4.5 and 7.1.3, cryptographic algorithm used:

- Signature SHA256 with RsaEncryption
- Public key RsaEncryption (2048)

Intermediate CA certificate under current validity expiration 2020 July, relevant documents:

- TRUST DOC A10 Cryptographic Policy ver. 1 23-04-2018
- PQ08 Certificate Generation Practice, rev. 2 09-05-2018
- PQ11 Delivery on site rev 2 09-05-2018

TRUST DOC A17.2 Business continuity plan ver. 1 23-04-2018 – It consider disruptive scenario of total unavailability of primary Data Center. Key points:

- Cold devices already available in the DR site
- daily backup of production platform and DB assured in DR site
- acceptable RTO – 24h
- Recovery team appointment

6.6 Certificate, CRL, and OCSP profiles

The CA ensures that certificates, CRL profile and OCSP profile meet the specified requirements.
As per X.509 CLR link is embedded in the Certificate statement:

- "distribution point" - full name http://onsitecrl.trustitalia.it/TrustItaliaSpAConsumerServiceCenterClass2G2/latestCRL.crl

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

OCSP 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 is NTP synchronized real time (ref. TRUST DOC A12-6 par 2.5)

6.7 Compliance audit and other assessment

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

6.8 Other business and legal matters

The CA ensures that all applicable organizational, financial and legal topics are fulfilled.
Digital Certificate subscriber agreement updated in June 2011 as per Symantec Request 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. For what concerns Financial Responsibility it has been verified documentation that confirms the high-level reference declared by Banco Popolare in 02/11/2015. Generally the document defines policies for other issues as revocation, change of terms etc..

6.9 Other provisions

The CA provides the capability to allow third parties to check and test all the certificate types; the CA allows use of such capability even to visual impaired people. The CA ensures impartiality and privacy compliance where applicable for all certificate life cycle activities.