PKI Disclosure Statement – SSL CA

1 Introduction

This document is the PKI Disclosure Statement, as required by European norm ETSI EN 319 411-1, related to the SSL CA certification service offered by the Trust Service Provider **Actalis S.p.A.**, an Italian company with VAT number IT-03358520967 (henceforth, just "Actalis"). In particular, this document applies to the **SSL Server** certificates issued by Actalis in compliance with the CA/Browser Forum requirements and guidelines.

In the following, the acronym "CA" stands for Certification Authority (and thus refers to Actalis), while the certification service that this document relates to is also mentioned as "SSL CA service".

This document does not substitute or replace the Terms and Conditions nor the Certification Practice Statement (CPS) of the SSL CA service, published on the CA website (see further on).

2 CA contact information

The CA can be contacted at the following address:

Servizio di Certificazione
ACTALIS S.p.A
Via San Clemente 53
I-24036 Ponte San Pietro (BG)
ITALIA

Web site: https://www.actalis.it
Info mail: info@actalis.it
Tel. +39 0575 050.350
Fax +39 0575 862.350

For any queries regarding this PKI Disclosure Statement or other documents of the SSL CA service, please send email to ca-admin@actalis.it.

To request revocation of a certificate, follow the on-line procedure described in the CPS (requires authentication with the credentials provided at certificate issuance time). For further information, refer to the CPS published on the CA website.

3 Certificate types, validation procedures and usage

Within the SSL CA service, Actalis issues **SSL Server certificates** in compliance with CA/Browser Forum requirements and guidelines, related standards and best practices. **Code Signing** certificates are also issued.

Certificates are offered to the general public. Some classes of certificates can be issued to legal persons only.

All details on the supported certificate policies (e.g. their respective OIDs and other features) are found in the documentation published on the CA website at https://www.actalis.it/products/ssl-certificate.aspx.

To allow validation of certificates, the CA makes available both the Certificate Revocations List (CRL) and an on-line certificate status checking service based on the OCSP standard. The URLs of both services are found in the certificate themselves.

4 Reliance limits

Actalis does not set reliance limits for certificates issued by its SSL CA service.

5 Obligations of subscribers

The certificate subscriber has the obligations set forth in the CPS and the general Terms & Conditions of the SSL CA service. In particular, but not only, the following obligations:

- provide the CA with precise and true information in the certificate requests;
- adopt suitable measures to avoid compromise of their own private keys;
- install and start using the certificate only after having checked that it contains correct information;
- use the certificate only in the ways and for the purposes provided for in the CPS;
- in the event of confirmed compromise of any of their own private keys, immediately request revocation of the corresponding certificates and immediately stop using those certificates;
- immediately request revocation of the certificate in the case when any of the information contained in the certificate (i.e. company name, web site address etc.) is no longer valid;
- immediately inform the CA, after issuance and up to expiry or revocation of the certificate, of any changes in the information supplied during the application phase;
- upon revocation of their certificate(s), immediately stop using the revoked certificates;
- stop using certificates upon their expiration.

For the full list of subscriber obligations, refer to the CPS and the Terms & Conditions of the SSL CA service.

6 Certificate status checking obligations of relying parties

All those who rely on the information contained in certificates (in short, “Relying Parties”) must verify that certificates are not suspended or revoked. Such verification can be performed by consulting the list of revoked certificates (CRL) published by the CA or by querying the OCSP service provided by the CA, at the addresses (URLs) contained in certificate themselves.

7 Limited warranty and disclaimer/limitation of liability

For warranty and liability limitations, please refer to the Terms and Conditions of the SSL CA service published on the Actalis website at https://www.actalis.it/products/ssl-certificate.aspx.

8 Applicable agreements, CPS, CP

The agreements and conditions applying to the CA service are found in the following documents, published on the Actalis website at https://www.actalis.it/products/ssl-certificate.aspx:

- Certification Practice Statement (CPS) for SSL Server and Code Signing certificates
- General Terms and Conditions for SSL Server and Code Signing certificates

The supported Certificate Policies (CP) are described in the CPS; see also section 3 above.

The above-mentioned documentation is also published in Italian. In the event of any inconsistency between the Italian and the English versions, the Italian versions take precedence.

9 Privacy policy

Actalis complies with Italian law on privacy (D.Lgs. 196/2003 and subsequent), with the GDPR (UE Regulation No. 679/2016), and with the recommendations and provisions of the Italian Data Protection Authority. For further information, refer to the general Terms and Conditions of the SSL CA Service published on the Actalis website at https://www.actalis.it/products/ssl-certificate.aspx.

All records relating to certificates issued by the SSL CA service are retained by Actalis for 7 years after the expiry date of certificates. Event logs are retained for 20 years.

10 Refund policy

For the refund policy, please refer to the general Terms and Conditions of the SSL CA service published on the Actalis website at https://www.actalis.it/products/ssl-certificate.aspx.

11 Applicable laws, complaints and dispute resolution

All CA services provided by Actalis are subject to Italian and European law. The applicability, execution, interpretation and validity of the CPS are governed by Italian law and by directly applicable European laws, irrespective of the contract or other choice of legal provisions and without the need to establish a commercial contact point in Italy. This choice is intended to ensure uniformity of procedures and interpretations for all users, regardless of where they reside or use the service.

For all legal disputes related to the Actalis' SSL CA service, where Actalis is plaintiff or defendant, the Court of Bergamo shall have exclusive jurisdiction, with the exclusion of any other court and excluding any hypothesis wherein the law provides for the competence of Consumer's court.

12 TSP and repository licenses, trust marks, and audit

Since March 28, 2002, Actalis is a Certification Service Provided (Certification Authority) enlisted in the public registry of accredited CAs maintained by the national supervisory body Agenzia per l'Italia Digitale (AgID).

As of July 1st, 2016, Actalis is a Qualified Trust Service Provider of certification and electronic time-stamping services according to the eIDAS Regulation (EU Regulation No.910/2014), and therefore enlisted in the Italian List of Trust Service Providers (TSL) published by AgID.

Actalis' SSL CA service is subject to a compliance audit every 12 months, according to ETSI TS 102 042 or ETSI EN 319 411-1 (as mandated by the CA/Browser Forum Requirements and Guidelines), by an independent and qualified auditor.

* * *