N° ITSEC-02/13

CONFORMITY DECLARATION

WE HEREBY DECLARE THAT THE COMPANY:

ACTALIS S.p.A.

OPERATIVE UNIT:
Via San Clemente, 53
24036 - Ponte S. Pietro (BG)

For the following Certification Authority services:

- Issuing and management of SSL Server certificates of EV, OV, DV classes
- Issuing and management of Code Signing certificates

IS IN COMPLIANCE WITH THE TECHNICAL SPECIFICATION:

ETSI TS 102 042 V. 2.4.1 (2013-02)

WITH REFERENCE TO:

CA/BROWSER FORUM BASELINE REQUIREMENTS CERTIFICATE POLICY FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES, V.1.3.5

AND

CA/BROWSER FORUM GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES, V. 1.5.5

The present conformity declaration is only valid in combination with the respective audit report (Doc. N. ABACT1201A_04 V. 1.4)

Note:
During the Certification Authority audit it was also verified that the issuing and management of S/MIME certificates meets the LCP requirements of ETSI TS 102 042 V. 2.4.1 (2013-02).

FIRST ISSUE	CURRENT ISSUE	EXPIRY DATE
2013-10-18	2016-10-07	2017-10-18

IMQ S.p.A. - VIA QUINTILIANO, 43 - 20138 MILANO

mod. 1155/0 - 07/14 - 1000 - Med

ANNEX TO THE CONFORMITY DECLARATION N° ITSEC-02/13 ISSUED BY IMQ S.P.A.

AUDIT REPORT (DOC. CODE. IMQ ABACT1201A_04 V.1.4, 07/10/2016)

Audit Requirements

The audit requirements are defined in the technical specification ETSI TS 102 042: ETSI TS 102 042 V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates", Version 2.4.1, 2013-02, European Telecommunications Standards Institute, with reference to CA/BROWSER FORUM Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.5 and CA/BROWSER FORUM Guidelines for the issuance and management of Extended Validation Certificates, V. 1.5.5.

The applicable ETSI certification policy are: **EVCP, OVCP and DVCP**

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

- **Issuing and management of SSL Server certificates of EV, OV, DV classes**
- **Issuing and management of Code Signing certificates**

Audit result:

- The audit object fulfils all applicable requirements from the audit criteria, as detailed in Doc. Code IMQ ABACT1201A_08 V 1.0.
- All requirements for a CA Practice according to chapter 7 of the rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy (EVCP).
- The audited CA also takes the responsibility for the norm requirements fulfilment
- The CA provides the certification services according to the definitions of the Certificate Practice Statement.
- The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.

The Actalis's CA services for the issuing and management of S/MIME certificates meet the ETSI **LCP** certification policy.

Summary of the audit requirements

The ETSI specification ETSI TS 102 042 contains the following requirements:

1 Certification Practice Statement (CPS)

The CA has a presentation of its practices and policies.

2 Public Key Infrastructure – key management life cycle

The CA ensures that CA keys are created under controlled conditions.
The CA ensures that private CA keys are treated confidentially and that their integrity is maintained.
The CA ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved.

The CA does not generate nor store private signature keys of the certification owner (subject).

3 Public key infrastructure – certificate management life cycle

The CA ensures that the identification confirmation of a participant (subscriber) and of a certificate owner (subject) as well as the correctness of their names and their related data are either checked as part of the defined service or proved by attestations from appropriate and licensed sources. It also ensures that applications for a certificate take place in a correct and authorized way, completely according to the collected proofs respectively attestations.

The CA ensures that the certificates are handed out in a secure way so that their authenticity is maintained.

The CA ensures that the legal terms and conditions are made available to the participants (subscriber) and to the relying parties.

The CA ensures that certificates are made available to the participants (subscriber), certificate owners (subject) and relying parties to the extent necessary.

The CA ensures that certificates are blocked at short notice using authorized and verified blocking queries.

4 CA Management and Operation

The CA ensures that the applied administrative and management methods are appropriate and correspond to acknowledged standards.

The CA ensures that the objects and information worthy of protection receive an appropriate protection.

The CA ensures that the employees and the hiring procedures amplify and support the CA company's trustability.

The CA ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized.

The CA ensures that the CA systems are operated safely, according to specification.

The CA ensures that the access to the CA systems is restricted to appropriate, authorized persons.

The CA is to use trustworthy systems and products that are protected against modifications.

The CA ensures that in case of a catastrophe the operation is restored as soon as possible.

The CA ensures that in case of a cessation of the CA operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given.

The CA ensures that statutory requirements are met.

The CA ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

5 Organization

The CA ensures that its organization is reliable.

6 Additional requirements

The CA allows third parties to check and test their certificates.

The CA does not make use of Cross Certificates that identify the CA as the Subject.