

Manuale Operativo

Servizio di Validazione Temporale Elettronica Qualificata
Versione 1.1

Approvato da: **Andrea Sassetti**
Direttore dei Servizi di Certificazione

il **11/10/2016**

- Questa pagina è lasciata intenzionalmente bianca -

Indice

1	Introduzione	5
1.1	Scopo del documento e principali raccomandazioni ai lettori	5
1.2	Riferimenti agli standard	6
1.3	Riferimenti normativi	7
1.4	Definizioni ed acronimi	8
2	Dati identificativi - Pubblicazione Manuale Operativo	9
2.1	Dati identificativi del Prestatore di Servizi Fiduciari Qualificato	9
2.2	Identificativo della policy	9
2.3	Versione del manuale operativo	9
2.4	Pubblicazione del manuale	9
2.5	Responsabile del manuale operativo	9
3	Disposizioni generali	10
3.1	Obblighi del richiedente, del prestatore di servizi fiduciari e degli utenti	10
3.1.1	Obblighi di coloro che accedono alla verifica delle validazioni temporali elettroniche	10
3.2	Obblighi connessi al trattamento dei dati personali	11
3.2.1	Tutela e diritti degli interessati	11
3.2.2	Modalità del trattamento	11
3.2.3	Finalità del trattamento	11
3.2.4	Sicurezza dei dati	11
3.3	Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi	12
3.3.1	Conoscenza del manuale operativo	12
3.3.2	Forza Maggiore	12
3.3.3	Declinazioni e Limitazioni del Prestatore di servizi fiduciari qualificati	12
3.3.4	Manleva	12
3.3.5	Esclusione di risarcibilità di danni indiretti	13
3.3.6	Limitazioni di responsabilità	13
3.3.7	Attività pericolose	13
3.4	Tariffe del servizio	13
4	Operatività	14
4.1	Funzioni del personale addetto al Servizio di Validazione temporale elettronica qualificata	14
4.2	Rapporti con le organizzazioni esterne	14
4.2.1	Informazioni che il richiedente deve fornire	15
4.3	Modalità di protezione dei dati personali	15
4.3.1	Archivi contenenti dati personali	15
4.3.2	Misure di tutela della riservatezza	15
4.3.3	Informativa ai sensi del D.Lgs. 196/03	15
4.4	Modalità operative per l'apposizione e la definizione della validazione temporale elettronica qualificata	15
4.4.1	Validazione Elettronica Temporale Qualificata	15
4.4.2	Richiesta del servizio di validazione temporale elettronica qualificata	16
4.4.3	Sicurezza logica e fisica del sistema di validazione temporale elettronica qualificata	16
4.5	Modalità operative per l'utilizzo del sistema di verifica delle validazioni temporali elettroniche qualificate	17
4.6	Disponibilità del servizio	18
4.7	Conservazione dei log	18
4.8	Piano di Cessazione della TSA	19
5	Termini e condizioni generali	19
5.1.1	Obblighi degli Utenti	19

5.1.2	Nullità o inapplicabilità di clausole.....	20
5.1.3	Interpretazione.....	20
5.1.4	Nessuna rinuncia.....	20
5.1.5	Comunicazioni.....	20
5.1.6	Intestazioni e Appendici del presente Manuale Operativo.....	20
5.1.7	Modifiche del Manuale Operativo.....	20
5.1.8	Violazioni e altri danni materiali.....	20
5.1.9	Norme Applicabili.....	21
5.1.10	Foro competente.....	21

Storia delle modifiche apportate al documento

Data Modifica	Versione	Paragrafo	Tipo Modifica
24/05/2016	1.0	----	Prima emissione
11/10/2016	1.1	1.4	Aggiornata tabella definizioni
		2.3	Aggiornato indice versione
		4.4.3.1	Correzioni minori (refusi)
		4.4.3.2	Correzioni minori (refusi)
		4.5	Inserite modalità di qualifica applicazioni e rimosso riferimento ad appendice A
		4.6	Inserito significato acronimi
		4.7	Corretto periodo di conservazione log
		4.8	Aggiornato piano cessazione TSA
		5.1.8	Aggiornate le descrizione delle figure del presente paragrafo
		5.1.9	Aggiornati i riferimenti alle norme applicabili
	Appendice A	Rimossa del tutto	

1 Introduzione

1.1 Scopo del documento e principali raccomandazioni ai lettori

Questa sezione illustra lo scopo del manuale operativo e fornisce alcune raccomandazioni per il corretto utilizzo del servizio di validazione temporale.

Si prega di leggere l'intero testo del Manuale in quanto le raccomandazioni contenute nella presente sezione sono incomplete e molti altri importanti punti sono trattati negli altri capitoli. Per una più agevole e scorrevole lettura del Manuale Operativo si raccomanda la consultazione dell'elenco di acronimi e abbreviazioni posti alla fine della presente sezione. Il presente manuale operativo ha lo scopo di illustrare e definire le modalità operative adottate dalla Actalis S.p.A. nella attività di certificazione ai sensi del Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001, Decreto legislativo 7 marzo 2005, n. 82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93 "Codice dell'amministrazione digitale" e successive modifiche ed integrazioni e del Decreto del Presidente del Consiglio dei Ministri (DPCM) 30 Marzo 2009, "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.", pubblicato sulla Gazzetta Ufficiale 6 Giugno 2009, n. 129, nonché del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

In particolare, il presente documento illustra le modalità di richiesta, validazione, emissione, utilizzo delle marche temporali erogate nell'ambito del servizio di validazione temporale elettronica qualificata, nonché le responsabilità e gli obblighi del certificatore, dei richiedenti e di tutti coloro che accedono al servizio per la verifica delle firme marche temporale.

In ottemperanza all'obbligo di informazione (DPCM 22 febbraio 2013, art. 40 e successive modifiche ed integrazioni) richiesto dalla legge, Actalis S.p.A., come struttura di certificazione digitale, pubblica il presente manuale operativo in modo da permettere ad ogni singolo utente di valutare il grado di affidabilità del servizio offerto. Nel presente Manuale Operativo, si parte dal presupposto che il lettore abbia una adeguata conoscenza della materia relativa ai servizi fiduciari ed alla struttura PKI.

Actalis S.p.A., allo scopo di consentire un corretto utilizzo del servizio di validazione temporale elettronica qualificata, oltre a raccomandare all'utente una attenta lettura del presente documento, invita tutti coloro i quali dovranno fare affidamento su di una validazione temporale elettronica qualificata e/o sulle informazioni contenute nel certificato ad essa associato, di controllare preventivamente:

1. Che il certificato sia valido e non revocato o sospeso attraverso l'utilizzo delle apposite liste di certificati revocati o sospesi, disponibili per via telematica agli utenti (vedi definizioni di CRL e CSL).
2. Che la validazione temporale elettronica qualificata sia stata creata durante il periodo operativo del certificato stesso dalla chiave privata corrispondente alla chiave pubblica riportata nel certificato.
3. Che il messaggio associato alla validazione temporale elettronica qualificata non sia stato modificato.

Per ulteriori informazioni, vedi il sito web di Actalis S.p.A. <https://www.actalis.it> oppure contattare il servizio clienti all'indirizzo: assistenza@actalis.it.

1.2 Riferimenti agli standard

Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".

ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

PKCS. Public Key Cryptography Standards. Standard realizzati per assicurare l'interoperabilità delle tecniche crittografiche. Le componenti di questo standard sono numerate. Maggiori dettagli sugli standard PKCS implementati sono disponibili presso il sito <http://www.rsa.com>.

LDAP. Lightweight Directory Access Protocol. Protocollo per utilizzato per accedere online a servizi di directory (in particolare servizi directory X.500) che possono contenere informazioni riguardo ad utenti e ad i loro certificati digitali.

X.500. Insieme di standards ITU-T relativi a servizi di directory elettroniche.

X.509. Standards ITU-T T relativi a certificati digitali. X.509 v3 si riferisce a certificati contenenti o in grado di contenere estensioni.

Secure Sockets Layer (SSL). Protocollo originariamente sviluppato da Netscape, poi divenuto standard universale per l'autenticazione dei siti Web e per cifrare le comunicazioni tra i client (browsers) e i Web server.

IPSec. Insieme di standard aperti per assicurare comunicazioni private sicure nelle reti IP al livello network, che forniscono la crittografia a livello network.

SHA-1. Secure Hash Algorithm (SHA), algoritmo specificato nel Secure Hash Standard (SHS, FIPS 180), sviluppato dal NIST. SHA-1 è una revisione del algoritmo SHA pubblicata nel 1994.

Lo standard di riferimento è costituito dalla norma ISO/IEC 10118-3:2004.

SHA-256. Secure Hash Algorithm (SHA), algoritmo specificato nel Secure Hash Standard (SHS, FIPS 180), sviluppato dal NIST.

Lo standard di riferimento è costituito dalla norma ISO/IEC 10118-3:2004.

1.3 Riferimenti normativi

- [1] Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.
- [2] Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71.", pubblicato sulla Gazzetta Ufficiale del 21 maggio 2013 n. 117.
- [3] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- [4] Decreto Legislativo (DLGS 196) 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003.
- [5] Decreto 2 luglio 2004, "Competenza in materia di certificatori di firma elettronica" pubblicato nella Gazzetta Ufficiale n.199, 25 agosto 2004.
- [6] Decreto Legislativo (CAD) 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.
- [7] Deliberazione n. 45 del 21 maggio 2009, "Regole per il riconoscimento e la verifica del documento informatico" (Deliberazione n. 45/2009).
- [8] Legge 11 agosto 1991, "Istituzione del Sistema Nazionale di Taratura", Pubblicato nella Gazzetta Ufficiale 6 maggio 2002, n. 104.
- [9] Decreto legislativo 4 aprile 2006, n. 159 "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale", Pubblicato in Gazzetta Ufficiale 29 aprile 2006, n.99.
- [10] Decreto del Presidente del Consiglio dei Ministri (DPCM) 12/10/2007, "Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'articolo 13, comma 4, del decreto del Presidente del Consiglio dei Ministri", pubblicato sulla Gazzetta Ufficiale 30 Ottobre 2003, n. 13.

1.4 Definizioni ed acronimi

CA	Certification authority – Autorità di certificazione
CAD	Codice dell'Amministrazione Digitale
CRL	Certificate revocation list – lista dei certificati revocati
CSL	Certificate suspension list – lista dei certificati sospesi
CSR	Certificate signing request
AGID	Agenzia per l'Italia Digitale
DPCM	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 [2]
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol con SSL
ISO	International Standard Organization
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
NTP	Protocollo di accesso a servizi di data e ora certa
OCSP	Protocollo per il controllo on-line dello stato dei certificati digitali
OID	Object Identifier
POP	Point of Presence
PKCS	Public Key Cryptography Standards
PKI	Public key infrastructure – infrastruttura a chiave pubblica
RDN	Relative Distinguished Name
RPA	Relying Party Agreement
RSA	Sistema crittografico
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
TLS	Transport Layer Security
TSA	Time Stamping Authority (sistema di marcatura temporale)
SP	Security Procedures – procedure di sicurezza Actalis S.p.a
VTEQ	Validazione Temporale Elettronica Qualificata
WWW	World Wide Web
X.509	Specifica ITU-T in materia di certificazione e relativo framework di autenticazione
TSP	Trust Service Provider, Prestatore di Servizi Fiduciari

2 Dati identificativi - Pubblicazione Manuale Operativo

2.1 Dati identificativi del Prestatore di Servizi Fiduciari Qualificato

Denominazione Sociale : **Actalis S.p.A.**
Sede legale: **Via San Clemente, 53 – 24036 Ponte San Pietro (BG)**
Legale Rappresentante : **Simone Braccagni**
N° REA : **436479**
N° iscrizione al Registro delle imprese : **03358520967**
N° Partita IVA : **03358520967**
N° Telefono (centralino) : **+39 0575 050.350**
N° FAX : **+39 0575 862.350**
e-mail PEC : **direzione.ca@pec.actalis.it**
ISO OID: **1.3.159**
Web server principale: <https://www.actalis.it>
Web server servizi fiduciari: <https://portal.actalis.it>

2.2 Identificativo della policy

L'identificativo della politica di validazione temporale elettronica (time-stamp policy) descritta nel presente documento è **0.4.0.2023.1.1**, corrispondente alla "**Best practices Time-Stamp Policy**" (BTSP) definita nella norma **ETSI TS 319 421**. Includendo tale object identifier (OID) nelle marche temporali (time-stamp token), la TSA di Actalis attesta la propria conformità alla policy BTSP.

2.3 Versione del manuale operativo

Il presente Manuale Operativo è di proprietà di Actalis S.p.A., tutti i diritti sono ad essa riservati. Questo documento è la versione 1.1 del Manuale Operativo del Servizio di Validazione Temporale Elettronica Qualificata erogato da Actalis S.p.A. .

Il Manuale Operativo sarà aggiornato dal responsabile in presenza di significativi mutamenti tecnici o normativi che comportino una modifica del servizio. In caso di aggiornamento sostanziale verrà pubblicata una nuova versione del documento. In caso di aggiornamento minore sarà pubblicata una nuova release. Il numero di versione/release è riportato in copertina del documento ed in calce ad ogni pagina dello stesso.

2.4 Pubblicazione del manuale

Questo documento è pubblicato sulle pagine principali del web server dei servizi fiduciari indicato all'interno del paragrafo 2.1.

2.5 Responsabile del manuale operativo

Actalis è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Il soggetto responsabile del presente manuale operativo all'interno di Actalis è:

Andrea Sassetti
Direttore dei Servizi di certificazione
ArubaPEC S.p.A.

Tel. +39 0575 1939715
Fax. +39 0575 862022
E-mail: CPS-admin@actalis.it

3 Disposizioni generali

3.1 Obblighi del richiedente, del prestatore di servizi fiduciari e degli utenti

1. Il richiedente del servizio di Validazione Temporale Elettronica Qualificata è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
2. Il prestatore di servizi fiduciari qualificato è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
3. Il prestatore di servizi fiduciari qualificato che rilascia eroga il servizio di Validazione Temporale Elettronica Qualificata deve inoltre:
 - a. Garantire che la validazione temporale elettronica qualificata collega la data e l'ora ai dati elettronici in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati stessi;
 - b. si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato;
 - c. è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.
 - d. informare i richiedenti in modo compiuto e chiaro, sulla procedura di rilascio delle validazioni temporali elettroniche qualificate e sui necessari requisiti tecnici per accedervi;
 - e. predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio fiduciario validazione temporale elettronica qualificata, tra cui in particolare gli esatti termini e condizioni relative all'uso della validazione temporale elettronica qualificate le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore prestatore di servizi fiduciari qualificato.
4. Il prestatore di servizi fiduciari qualificato raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del servizio, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espreso consenso della persona cui si riferiscono.

3.1.1 Obblighi di coloro che accedono alla verifica delle validazioni temporali elettroniche

Coloro che intendono utilizzare documenti a cui sono associate delle validazioni temporali elettroniche qualificate dovranno:

1. verificare che le informazioni contenute nella validazione temporale elettronica qualificata corrispondano a quelle del prestatore di servizi fiduciari qualificato;
2. verificare che il messaggio associato non sia stato modificato e/o alterato.

3.2 Obblighi connessi al trattamento dei dati personali

3.2.1 Tutela e diritti degli interessati

In materia di trattamento dei dati personali Actalis S.p.A. garantisce la tutela degli interessati in ottemperanza al DLGS 196. In particolare:

1. Agli interessati sono fornite le necessarie informazioni ai sensi dell'art. 13 DLGS 196.
2. Nella suddetta informativa gli utenti sono informati sui diritti di accesso ai dati personali ed altri diritti. (art. 7 DLGS 196).

Agli interessati, qualora necessario, verrà chiesto il consenso scritto al trattamento dei propri dati personali da parte di Actalis S.p.A. .

3.2.2 Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza, come descritte nel presente manuale operativo, sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. I dati saranno gestiti elettronicamente, secondo le leggi in vigore e archiviati nei server ubicati presso la sede operativa di Actalis S.p.A., in Via San Clemente, 53– 24036 Ponte San Pietro (BG). I dati in formato cartaceo saranno conservati negli archivi cartacei di ACTALIS S.p.A., a tali dati avranno diritto di accesso solo gli incaricati a ciò espressamente autorizzati.

3.2.3 Finalità del trattamento

Erogazione del servizio:

- Richieste di validazioni temporali elettroniche qualificate:
I dati raccolti saranno utilizzati per l'erogazione di validazioni temporali elettroniche qualificate o per la validazione delle stesse. Actalis S.p.A., inoltre, utilizzerà le informazioni esclusivamente per lo svolgimento del servizio e di ogni altra attività connessa e derivante da tale servizio quale, a mero titolo esemplificativo, la gestione della fatturazione nonché l'effettuazione di eventuali controlli sulla qualità dei servizi e di sicurezza del sistema senza procedere, in alcun modo, alla sua profilazione.
- Scopi di natura commerciale:
Actalis S.p.A. potrà utilizzare le coordinate di posta elettronica fornite dal cliente per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati salva in ogni caso la possibilità dell'interessato di opporsi a tale trattamento.

Altre forme di utilizzo dei dati:

ACTALIS S.p.A. informa espressamente che per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i dati forniti dall'interessato potranno essere usati con altre finalità rispetto alla fornitura dei servizi ed essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria, per lo svolgimento delle attività di loro competenza.

3.2.4 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, Actalis S.p.A adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

I rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento risorse hardware su cui sono registrati ed i locali ove vengono custoditi; l'accesso non autorizzato ai dati stessi; le modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

1. l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;

2. la disponibilità dei dati da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi anche accidentale utilizzando un sistema di backup;
3. la riservatezza dei dati da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

3.3 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi

La sezione illustra le limitazioni di responsabilità assunte dal Certificatore nell'esercizio della propria attività.

3.3.1 Conoscenza del manuale operativo

Il richiedente il servizio di VTEQ e coloro i quali intendono accedere alla verifica delle VTEQ sono tenuti a consultare preventivamente ed a conoscere il presente Manuale Operativo, con particolare riferimento alle modalità in esso descritte per le operazioni di validazione temporale e di verifica. E' espressamente esclusa ogni responsabilità del Certificatore che sia derivante dalla non conoscenza o dal non corretto utilizzo delle procedure descritte nel presente manuale.

3.3.2 Forza Maggiore

Fatto salvo il caso di dolo o colpa grave, la responsabilità del prestatore di servizi fiduciari qualificato sarà esclusa nel caso di eventi che esulino dalla volontà dello stesso o da cause ad esso non imputabili. Il prestatore di servizi fiduciari qualificato quindi non sarà responsabile, eccettuate le ipotesi di dolo o colpa grave, per i danni di qualsiasi natura, da chiunque subiti e causati da caso fortuito o forza maggiore, impossibilità della prestazione, ordine o divieto dell'autorità quali, a titolo esemplificativo e non esaustivo, mancato funzionamento di reti o apparati tecnici al di fuori del controllo del Certificatore, interruzione nella fornitura di energia elettrica, allagamenti, scioperi, incendi, azioni di guerra, epidemie, colpi di stato, terremoti e altri disastri.

3.3.3 Declinazioni e Limitazioni del Prestatore di servizi fiduciari qualificati

Il prestatore di servizi fiduciari qualificati una volta terminata l'erogazione della validazione temporale elettronica qualificata non ha alcun ulteriore obbligo di verifica della validità dei dati e delle informazioni contenute nella richiesta né sul medesimo grava alcun obbligo, anche anteriormente all'erogazione della medesima validazione temporale elettronica qualificata, di verifica della validità, correttezza ed integrità dei documenti informatici a cui l'utente vuole associare la validazione; il prestatore di servizi fiduciari qualificato non assume alcun ulteriore obbligo, garanzia o responsabilità rispetto a quanto previsto nel presente Manuale Operativo o dalle vigenti disposizioni di legge, e non sarà responsabile per i danni di qualsiasi natura, da chiunque subiti, qualora tali danni derivino dalla violazione di quanto previsto e contenuto nel presente Manuale Operativo, ovvero dalle vigenti disposizioni di legge.

3.3.4 Manleva

Il richiedente il servizio di VTEQ e l'utente che procede alla verifica delle stesse manlevano e tengono indenne il prestatore di servizi fiduciari qualificato ed i suoi aventi causa da qualsiasi responsabilità, spesa, pregiudizio o danno, diretto o indiretto, derivante da pretese o azioni giudiziali da parte di terzi di cui esso prestatore di servizi fiduciari qualificato sia chiamato a rispondere nei confronti dei terzi per fatto imputabile al richiedente e/o all'utente del servizio di VTEQ, ivi espressamente incluse, a titolo esemplificativo e non esaustivo, le responsabilità e i danni derivanti dalla eventuale invalidità, erroneità o non attualità delle informazioni o dei dati trasmessi al prestatore di servizi fiduciari qualificato e/o dal non corretto utilizzo delle procedure descritte nel presente Manuale Operativo.

3.3.5 Esclusione di risarcibilità di danni indiretti

Salvo i casi di dolo o colpa grave il prestatore di servizi fiduciari qualificato non sarà responsabile di alcun danno indiretto o di qualsiasi perdita di profitto e/o perdita dei dati o altri danni indiretti e conseguenti derivanti o collegati all'utilizzo, consegna, licenze, prestazioni o mancate prestazioni di certificati, digitali validazioni temporali elettroniche qualificate o qualsiasi altra transazione digitale o servizio offerto o contemplato dal presente Manuale Operativo.

3.3.6 Limitazioni di responsabilità

Il prestatore di servizi fiduciari qualificato ha stipulato una polizza assicurativa per i danni eventualmente cagionati ai richiedenti, ai clienti ed agli utilizzatori nell'erogazione del servizio previsto dal presente Manuale Operativo.

Ciò premesso, il limite di indennizzo è pari ad € 1.000.000,00 per sinistro e in aggregato annuo

3.3.7 Attività pericolose

Il servizio di validazione temporale elettronica qualificata offerto da Actalis S.p.A. non è studiato, inteso o autorizzato per l'uso o la vendita come dispositivi di controllo in circostanze pericolose, o l'impiego in situazioni che richiedano un ambiente a prova di errore, come la gestione di impianti nucleari, sistemi di navigazione o comunicazione aerea, sistemi di controllo del traffico aereo o sistemi di comunicazione, sistemi di controllo d'armi, in cui un eventuale guasto comporterebbe direttamente decesso, danni alla persona, o gravi danni ambientali.

3.4 Tariffe del servizio

Per le tariffe del servizio si rimanda al form di richiesta informazioni presente sul sito web <https://www.actalis.it>.

4 Operatività

Questa sezione descrive le modalità con le quali opera il prestatore di servizi fiduciari qualificato ed in particolare le funzioni del personale addetto al servizio di certificazione validazione temporale elettronica qualificato, le modalità di richiesta delle validazioni e le modalità di comunicazione con il richiedente.

4.1 Funzioni del personale addetto al Servizio di Validazione temporale elettronica qualificata

Tutto il personale di Actalis S.p.A. è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità. Il personale addetto al Servizio di Validazione temporale elettronica qualificata, prevede, le seguenti figure responsabili:

- a) responsabile della sicurezza;
- b) responsabile del servizio di certificazione e validazione temporale;
- c) responsabile della conduzione tecnica dei sistemi;
- d) responsabile dei servizi tecnici e logistici;
- e) responsabile delle verifiche e delle ispezioni (auditing).

Non è possibile attribuire ad un medesimo soggetto più funzioni tra quelle citate.

Le funzioni sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di addetti ed operatori.

4.2 Rapporti con le organizzazioni esterne

Il prestatore di servizi fiduciari qualificato può avvalersi di terze parti, anche facenti parte del gruppo societario a cui appartiene Actalis, a cui possono essere demandate attività per la migliore erogazione del servizio.

In tali ipotesi il prestatore di servizi fiduciari qualificato vincola, a mezzo di appositi accordi, le organizzazioni esterne:

- a) al rispetto di quanto previsto nel presente Manuale Operativo;
- b) al rispetto della normativa tecnica e giuridica applicabile per l'esecuzione del servizio;
- c) al rispetto delle policy interne relative al trattamento dei dati personali dei clienti e degli utenti;
- d) al rispetto delle policy di sicurezza, logica e fisica, adottate dal prestatore di servizi fiduciari qualificato all'interno della propria struttura;
- e) al rispetto delle policy di qualità adottate dal prestatore di servizi fiduciari qualificato.

I soggetti esterni a cui possono essere demandate attività nell'ambito dei servizi fiduciari regolati dal presente Manuale Operativo sono scelti e selezionati tenuto conto di caratteristiche di esperienza, competenza e professionalità tali da assicurare il rispetto delle previsioni contenute nel presente documento e nelle normative in esso richiamate.

4.2.1 Informazioni che il richiedente deve fornire

L'utente che intende richiedere il servizio di validazione temporale elettronica qualificata deve obbligatoriamente fornire le seguenti informazioni:

- Nome e Cognome (*)
- Data di nascita
- Comune, provincia e stato di nascita
- Codice fiscale o analogo codice identificativo¹ (*)
- Indirizzo di residenza, eventualmente all'estero
- Indirizzo di posta elettronica (*)
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso
- Numero di cellulare.

4.3 Modalità di protezione dei dati personali

4.3.1 Archivi contenenti dati personali

Tutta la documentazione cartacea ed in formato elettronico raccolta durante le fasi di elaborazione delle richieste del servizio di VTEQ è conservata negli elaboratori del prestatore fiduciario di servizi qualificati in locali altamente sicuri.

4.3.2 Misure di tutela della riservatezza

Actalis è titolare dei dati personali raccolti di richiesta del servizio da parte degli utenti e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal DLGS 196.

4.3.3 Informativa ai sensi del D.Lgs. 196/03

Vale quanto indicato nel par. 3.2.

4.4 Modalità operative per l'apposizione e la definizione della validazione temporale elettronica qualificata

4.4.1 Validazione Elettronica Temporale Qualificata

La validazione elettronica temporale qualificata è un'informazione contenente la data e l'ora associata ad uno o più documenti informatici. Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un secondo rispetto alla scala UTC.

Il riferimento temporale usato da Actalis è ottenuto da un dispositivo di alta precisione che garantisce una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC (IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.

La validazione temporale elettronica qualificata è erogata da Actalis sulla base di quanto previsto dall'art. 42 del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE e relative norme di attuazione

4.4.2 Richiesta del servizio di validazione temporale elettronica qualificata

Il servizio di temporale validazione elettronica temporale qualificata offerto da Actalis S.p.A. è fruibile attraverso protocollo HTTPS.

I formati e la codifica delle richieste accettate e delle temporali validazioni temporali elettroniche qualificate restituite dal servizio sono conformi alle strutture dati descritte nella RFC 3161 e ETSI EN 319 422.

La richiesta viene accettata dal portale dei servizi fiduciari Actalis, specificamente all'indirizzo <https://portal.actalis.it/tsa/FrontEnd> (che deve essere configurato all'interno del client prescelto per l'interfacciamento al servizio) con le credenziali fornite da Actalis S.p.A. al momento dell'attivazione dell'account TSA (che devono essere inserite nel software prescelto per l'interfacciamento al servizio). Il servizio di TSA Actalis accetta solo ed esclusivamente richieste di marcatura temporale contenenti impronte dell'evidenza informatica da sottoporre a validazione temporale calcolate secondo l'algoritmo hash **SHA-256** (dedicated hash-function 4 definito nella norma ISO/IEC 10118-3:2004).

Dopo aver autenticato l'utente e verificato la correttezza della richiesta ricevuta, viene accertata la disponibilità di marche. In caso positivo, il sistema restituisce, come risposta, la TimeStampResp (RFC3161) contenente il TimeStampToken (RFC3161) relativo all'HASH incluso nella TimeStampReq (RFC3161) fornita in fase di richiesta

Nel caso in cui il sistema TSA riceva una richiesta di temporale validazione temporale elettronica qualificata non conforme al requisito di cui sopra viene restituito un messaggio di errore.

Sintesi operativa dell'utente :

1. Avviare l'applicazione di firma e verifica
2. Selezionare la funzione di apposizione della VTEQ
3. Selezionare il file;
4. Il software necessita di avere una connessione ad internet in quanto tenterà l'accesso a CRL e/o OCSP;
5. Il software mostra a video il risultato dell'apposizione della validazione temporale elettronica qualificata. Il contenuto del file potrà essere letto con programmi adeguati al formato del file stesso (esempio: i file in formato PDF saranno letti con Acrobat Reader).

La Time Stamping Authority Actalis, a seguito della ricezione di una richiesta conforme al formato sopra descritto restituisce un messaggio contenente un TimeStampToken (RFC3161) codificato in DER, così come previsto dall'RFC 3161.

4.4.3 Sicurezza logica e fisica del sistema di validazione temporale elettronica qualificata

Gli elaboratori che offrono il servizio di VTEQ collocazione sono fisicamente protetti in modo da dalla prevenire la possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

4.4.3.1 Sicurezza fisica

Il sistema di validazione temporale elettronica qualificata reso disponibile da Actalis ai propri titolari si basa su dei server web di Front-end che gestiscono le transazioni con i client, l'autenticazione, l'accounting e l'archiviazione delle validazioni temporali elettroniche qualificate ed dei server di Back-end che si occupano della creazione delle validazioni temporali elettroniche qualificate e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale.

I server del sistema di validazione temporale elettronica qualificata sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico.

Solo il personale autorizzato può accedere a tali sale. Questi ambienti, inoltre, sono protetti da allagamenti ed incendi mediante appositi presidi (sensori, spruzzatori, condizionamento, etc) e gli elaboratori sono alimentati con linea elettrica preferenziale, sorretta da gruppo di continuità.

4.4.3.2 Sicurezza logica

I server di Front-end e di Back-end del sistema di validazione temporale elettronica qualificata dialogano tra loro attraverso protocolli di comunicazioni sicuri e possono essere attivati solo da operatori autorizzati. In particolare, i server di Back-end firmano le validazioni temporali elettroniche qualificate mediante un dispositivo crittografico hardware (o "dispositivo di firma") di altissima qualità e sicurezza. L'algoritmo di sottoscrizione utilizzato è RSA con chiave di lunghezza 2048 bit e viene usato esclusivamente per il servizio di validazione temporale elettronica qualificata. La coppia di chiavi RSA è generata all'interno del dispositivo di firma. La chiave privata della coppia è usata all'interno del dispositivo di firma. Il dispositivo di firma può essere attivato solo da un operatore appositamente autorizzato e dotato della necessaria parola-chiave.

4.5 Modalità operative per l'utilizzo del sistema di verifica delle validazioni temporali elettroniche qualificate

Actalis ha qualificato, tramite una procedura interna di validazione del software, le applicazioni che fornisce alla propria clientela e che permettono la verifica delle validazioni temporali elettroniche qualificate apposte su documenti informatici sotto forma di "buste crittografiche" in standard PKCS#7 / CAdES, PAdES e XAdES. Tali applicazioni consentono di verificare:

1. L'integrità del documento a cui è applicata la validazione temporale elettronica qualificata;
2. L'autenticità e l'affidabilità della validazione temporale elettronica qualificata;
3. La data ed ora in cui la validazione temporale elettronica qualificata è stata associata al documento informatico.

Sintesi operativa dell'utente :

6. Avviare l'applicazione di firma e verifica
7. Selezionare la funzione di verifica della VTEQ
8. Selezionare il file;
9. Il software necessita di avere una connessione ad internet in quanto tenterà l'accesso a CRL e/o OCSP;
10. Il software mostra a video il risultato della verifica. Il contenuto del file potrà essere letto con programmi adeguati al formato del file stesso (esempio: i file in formato PDF saranno letti con Acrobat Reader).

I prodotti di verifica delle validazioni temporali elettroniche qualificate forniti da Actalis sono conformi a quanto indicato all'art. 42, commi 2 e 6 del DPCM ed ai requisiti di cui all'art.27 della DELIB. 45/09 [7].

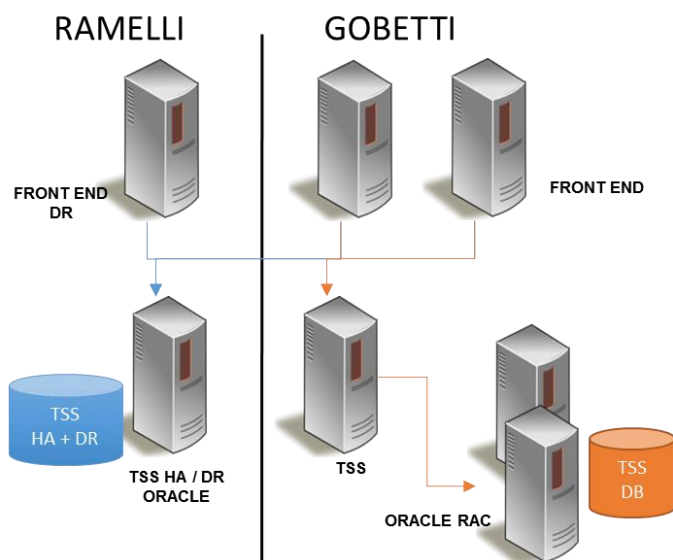
L'utente deve tenere ben presente il fatto che alcuni formati di file consentono di inserire del codice eseguibile (macro o comandi) all'interno del documento informatico senza che ciò vada ad modificarne la struttura binaria e tali da attivare funzionalità che possano alterare gli atti, i dati o i fatti rappresentati all'interno del documento stesso (Art. 4, comma 3 del DPCM [2]).

Tali file, seppur sottoposti a validazioni temporali elettroniche qualificate non producono gli effetti di cui all'articolo 21, comma 2 del CAD [6].

È unicamente responsabilità dell'utente accertarsi, attraverso le funzionalità tipiche di ciascun prodotto, che tale condizione sia soddisfatta.

4.6 Disponibilità del servizio

Il servizio è reso disponibile 24 ore su 24, tutti i giorni della settimana festivi inclusi tramite accesso Web Service (WS) con protocollo Secure Sockets Layer (SSL).



L'infrastruttura tecnologica, schematizzata nella figura a fianco, evidenzia come non vi siano Single Point Of Failure (SPOF) ed il sistema consenta di raggiungere un livello di servizio molto elevato.

Durante la normale operatività il Data Center principale eroga il servizio con due FRONT END ridondati richiedendo la marca temporale al Time Stamping Server (TSS) primario o, in alternativa, a quello secondario. I due TSS non hanno alcun componente in comune quindi è logico ipotizzare che il sistema sia assolutamente resiliente ai guasti.

Anche i singoli componenti hardware scelti hanno caratteristiche di durabilità estremamente elevate:

- gli HSM utilizzati nei TSS hanno inoltre un Mean Time Between Failure (MTBF) che si aggira intorno alle 200.000 ore
- le apparecchiature server hanno un MTBF, secondo standard consolidati per i servizi erogati, oltre le 80.000 ore di operatività.

4.7 Conservazione dei log

Il servizio di validazione temporale elettronica qualificata prevede che il prestatore di servizi fiduciari qualificato conservi i log (registri elettronici) delle validazioni temporali emesse per un periodo di 20 anni.

4.8 Piano di Cessazione della TSA

Di seguito si precisano le attività che saranno svolte qualora l'azienda decida, per qualsiasi ragione, di porre fine al servizio di marcatura temporale, ossia di cessare la propria attività di TSA.

Prima della effettiva cessazione:

- Almeno 60 giorni prima della data pianificata di cessazione del servizio, sarà inviata una informativa a tutti i clienti del servizio di TSA (o di altri servizi che includono i servizi di TSA), nonché al Supervisory Body nazionale e al Conformity Assessment Body.
- Sempre con preavviso di 60 giorni, sarà pubblicata in modo evidente una nota informativa anche sul sito web della TSA, al fine di rendere disponibile l'informazione anche alle Relying Parties.
- Sempre con preavviso di 60 giorni, la TSA invierà una comunicazione a tutti gli eventuali subappaltatori, informandoli che alla scadenza del termine non saranno più autorizzati ad eseguire attività collegate al processo di emissione di marche temporali.
- La responsabilità della conservazione delle evidenze (marche temporali, giornale di controllo, ecc.) sarà trasferita contrattualmente ad un altro soggetto affidabile che ne possa garantire la conservazione per un tempo pari ad almeno 20 anni. Sarà inoltre trasferita a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della TSA cessata nonché il mantenimento della URL della CRL.
- Si pianificherà la distruzione delle chiavi private di marcatura temporale nonché del materiale crittografico annesso (se presente) che ne consente il ripristino.

Alla data di cessazione:

- Saranno distrutte (per cancellazione logica) le chiavi private di marcatura temporale nonché il materiale crittografico annesso (se presente) che ne consente il ripristino, verbalizzando l'operazione.
- Saranno revocati i certificati di tutte le TSU facenti capo alla TSA cessata.

5 Termini e condizioni generali

Il presente capitolo presenta i termini e le condizioni generali del presente Manuale Operativo che non sono stati trattati nelle altre sezioni.

5.1.1 Obblighi degli Utenti

L'utente che, ai soli fini di verifica delle validazioni temporali elettroniche qualificate ha i seguenti obblighi:

- Conoscere l'ambito di utilizzo, e le eventuali limitazioni allo stesso, delle validazioni temporali elettroniche qualificate; le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel Manuale Operativo del Certificatore stesso;
- Verificare la validità del documento informatico a cui è associata una validazione temporale elettronica qualificata;
- Verificare i dati presenti nella validazione temporale elettronica qualificata ed, in particolare, che corrispondano ai dati previsti nel presente Manuale Operativo. Verificare che la validazione temporale elettronica qualificata sia correttamente sottoscritta dal prestatore di servizi fiduciari e che la chiave privata utilizzata per tale sottoscrizione non sia stata compromessa prima del momento della verifica della validazione temporale;
- Conoscere
- Adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- Conoscere e rispettare tutte quante le misure precauzionali previste nel presente Manuale Operativo e negli altri eventuali accordi intercorsi con il prestatore di servizi fiduciari, ivi comprese le limitazioni di responsabilità ed i limiti di indennizzo.

5.1.2 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizioni del presente Manuale Operativo, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale Operativo (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

5.1.3 Interpretazione

Salvo disposizioni diverse, questo Manuale Operativo dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù della legislazione italiana ed europea ad esso applicabile e degli usi commerciali internazionali.

5.1.4 Nessuna rinuncia

La mancata applicazione da parte di qualsivoglia persona di una delle disposizioni di cui al presente Manuale Operativo non sarà ritenuta rinuncia a future applicazioni di suddetta disposizione o di qualsiasi altra disposizione.

5.1.5 Comunicazioni

Qualora una persona desideri o sia tenuta ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale Operativo, tali comunicazioni dovranno avvenire attraverso messaggi PEC indirizzati alla seguente casella direzione.ca@pec.actalis.it oppure in forma scritta.

Le comunicazioni scritte dovranno essere consegnate da un servizio di posta che confermi la consegna per iscritto oppure tramite assicurata convenzionale, raccomandata a/r, indirizzate al seguente indirizzo:

Actalis S.p.A. - Via San Clemente 53 – 24036 Ponte San Pietro (BG)

5.1.6 Intestazioni e Appendici del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente Manuale Operativo sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta. Le appendici, comprese le definizioni del presente Manuale Operativo, sono parte integrante e vincolante del presente Manuale Operativo a tutti gli effetti.

5.1.7 Modifiche del Manuale Operativo

Modifiche Generali

Actalis S.p.A. si riserva il diritto di aggiornare periodicamente il presente Manuale Operativo in modo estensibile al futuro e non retroattivo.

Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale Operativo.

5.1.8 Violazioni e altri danni materiali

Gli utenti del servizio oggetto del presente manuale rappresentano e garantiscono che la loro presentazione al TSP qualificato (Actalis) e l'utilizzo delle informazioni relative alla richiesta del servizio di validazione temporale elettronica qualificata non interferiscano né danneggino i diritti di una qualsiasi terza parte di qualunque giurisdizione in merito a marchi, marchi di identificazione di servizio, nomi commerciali, nomi societari, o ogni altro diritto di proprietà intellettuale, e che non tenteranno di utilizzare il servizio per scopi illegali, ivi compresi interferenze illecite su vantaggi contrattuali o potenziali vantaggi aziendali, concorrenza sleale, azioni volte a ledere la reputazione di altra persona, pubblicità ingannevole, e ingenerare confusione su persone fisiche o giuridiche.

Gli utenti del servizio oggetto del presente manuale si obbligano a manlevare e indennizzare il TSP qualificato (Actalis) contro qualunque perdita o danno derivanti da una tale interferenza o infrazione.

5.1.9 Norme Applicabili

I servizi fiduciari qualificati oggetto del presente Manuale Operativo sono disciplinati dalle norme giuridiche dell'ordinamento Italiano e dell'Unione Europea.

Il fine è garantire uniformità di trattamento e mutuo riconoscimento all'interno dell'ordinamento Comunitario.

5.1.10 Foro competente

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta Actalis S.p.A e relative all'utilizzo del servizio di certificazione, alle modalità operative e all'applicazione delle disposizioni del presente Manuale sarà competente esclusivamente il Foro di Bergamo, con esclusione di qualsiasi altro foro competente e con esclusione delle ipotesi in cui la legge preveda la competenza del foro del consumatore.

(FINE DOCUMENTO)