Certification Practice Statement

Certificati SSL Server e Code Signing

Versione: 5.6

Data: 22 Gennaio 2020

Certification Practice Statement

Certificati SSL Server e Code Signing

Redatto da: Adriano Santoni

Verificato da: Marco Menonna
Approvato da: Andrea Sassetti

Codice documento: MGA_A_93

Distribuzione: PUBBLICA

Storia delle modifiche

DATA	VERS.	PARAGRAFI	MODIFICHE	AUTORE
14 dicembre 2005	1	-	Prima versione del documento	FP
24 giugno 2009	2	tutti	Revisione dell'intero documento; ristrutturazione secondo RFC 3647	FP, AS
19 novembre 2009	2.0.1	1.3.1	Cambiato il nome del Presidente	AS
13 maggio 2010	2.0.2	3.4	Rimossa la frase relativa all'eventuale inserimento di indirizzi IP privati nei certificati (possibilità non prevista)	AS
18 maggio 2010	2.0.3	4.2, 8.1, 8.2, 8.4, 8.5, 8.6, 9.5.2, 9.8	Precisazioni e integrazioni relative alle RA	AS
18 maggio 2010	2.0.3	1.3.1	Aggiornato l'indirizzo di Actalis; corretto il nome del Presidente	AS
23 giugno 2011	2.0.4	1.3.1, 3.1, 4.1	Modificato il rappresentante legale di Actalis. Aggiunti chiarimenti relativi a I&A e verifiche per i certificati wildcard e multi-SAN	AS
28 settembre 2011	2.1.0	Tutti	Introdotta PKI a due livelli. Aggiunti dettagli sulla gestione delle chiavi di Root CA e Sub CA. Necessità di autenticazione a due fattori per le utenze che consentono l'emissione dei certificati. I numeri di serie devono includere almeno 8 byte random. SHA256 usato per la firma dei certificati e delle CRL. Aggiornate lunghezze minime delle chiavi.	AS
19 settembre 2013	2.2.0	Tutti	Aggiornato frontespizio secondo l'attuale organizzazione. Precisato in §5.1 che il data center di Actalis è gestito da Aruba. Diverse revisioni e precisazioni per conformità alle linee guida del CAB Forum (BR+EVGL) e alla norma ETSI TS 102 042.	AS
8 ottobre 2013	2.2.1	Tutti	Dichiarazione esplicita di rispetto dei [BR] e delle [EVGL]. Integrazione elenco delle circostanze per la revoca. Revoca immediata per attività criminali svolte col certificato. Dual control nell'emissione dei certificati. Altre precisazioni.	AS
16 ottobre 2013	2.2.2	3.6, 7.1, 6.10.3	Correzione refusi. La massima durata dei certificati SSL Server EV è 24 mesi. Il titolare deve assicurare la riservatezza del PIN o password di attivazione della propria chiave. Policy OID = "anyPolicy" nel certificato della SubCA.	AS
21 ottobre 2013	2.2.3	4.9.4, 9.5.3	Precisazioni sulla revoca. Precisazioni sugli obblighi del titolare.	AS
13 novembre 2013	2.2.4	Diversi	Aggiornato il nome dell'Amministratore di Actalis nel par 1.3.1. Nuovo par 4.13 su segnalazione problemi sui certificati e relativa gestione. Modifica al par 1.3.2 per introduzione Enterprise RA.	AS

			Introdotti profili OV nel par 1.4 e nel capitolo 7. Modificato il 3.1 per maggiore chiarezza. Precisazioni nel par 3.3 sulle verifiche. Precisazioni sull'uso di CNames per l'accesso a CRL e al servizio OCSP.	
14 febbraio 2014	2.2.5	Diversi	Precisazione sulla conformità ai requisiti del CAB Forum all'inizio del capitolo 3. Precisazione sugli IDN.	AS
03 settembre 2014	2.2.6	3.1.1, 4.13, 6.3.3	Precisato che gli hostname non sono ammessi nei certificati per Code Signing e che un certificato per Code Signing emesso erroneamente con un hostname all'interno sarà revocato. Possibilità di inviare segnalazioni ad Actalis anche per telefono. La lunghezza chiavi utente di 1024 bit non è più consentita.	AS
20 ottobre 2014	2.2.7	Diversi	Supporto per i certificati di classe DV (Domain Validated). Firma digitale accettata come mezzo per verificare l'identità individuale. Correzione di refusi e alcune precisazioni.	AS
9 dicembre 2014	2.3	Diversi	Correzione refusi.	AS
13 marzo 2015	2.4	Diversi	Nuovo paragrafo 1.3.5 (rivenditori). Correzioni e precisazioni nel §1.4 (uso dei certificati), nel §4.1 (richiesta del certificato) e nel 4.9.6 (procedura per la sospensione o revoca).	AS
1 aprile 2015	2.4.1	Diversi	Precisazioni sugli URL delle CRL e del servizio OCSP. Precisazioni su Comunicazioni e assistenza. Ampliate le possibilità per la verifica di controllo del dominio. Spostato o rinominati alcuni paragrafi per maggior chiarezza.	AS
23 giugno 2015	2.5	Diversi	SubCA dedicata per i certificati di classe EV. Informazioni di Certificate Trans-parency nei certificati di classe EV. Aggiunti policy OID del CAB Forum ai certificati delle varie classi.	AS
22 marzo 2016	2.6	1.3.1, 4.13	Cambiati l'indirizzo di Actalis e i numeri di telefono. Modifiche nel frontespizio a seguito dei cambiamenti organizzativi. Cambiato n. telefono per segnalazione problemi sui certificato.	AS
5 ottobre 2016	2.7	3.4, 1.4	Precisazione sui CAA records. Precisazione sui domini .onion.	AS
6 ottobre 2016	2.8	1.3, 7	Precisazioni sulle CA. Introduzione cAIssuers nella estensione AIA. SubCA dedicata per SSL Server di classe DV.	AS
24 Luglio 2017	2.9	1.7, 3.2, 4.3	Cambiato da ETSI 102 042 a 319 411 nei Riferimenti. Aggiunto controllo dei CAA Record. Per certificati EV, firma autografa accettabile se autenticata da notaio. Chiarimenti sulla verifica di autenticità e sulle informazioni non verificate.	AS
28 Agosto 2017	3.0	4.3, 7.3	Correzione refusi. Nuovo paragrafo 7.3 con il profilo delle risposte OCSP.	AS

22 Gennaio 2018	4.0	Tutti	Completa ristrutturazione e revisione del documento per un più agevole confronto con la RFC 3647 e con i CABF Baseline Requirements. Documentazione di una nuova CA subordinata per certificati OV. Eliminati i riferimenti ai certificati Code Signing EV in quanto ad oggi non offerti.	AS
27 aprile 2018	4.1	3.1.1, 3.2.2.5, 4.3.1, 7.1.2.3	Precisato che nei certificati SSL Server di classe EV non sono ammessi indirizzi IP. Introdotta la CT obbligatoria, dopo il 30 Aprile 2018, su tutte le classi di certificati SSL Server.	AS
23 maggio 2018	5.0	1.4, 1.5, 1.7, 4.6, 7.1.2.3, 5, 6, 8, 9	Ampliamento del cap. 4 per maggior chiarezza. Revisione dei capp. 5, 6, 8, 9 per allineamento con altri CPS di Actalis. Introdotti i certificati SSL Server qualificati (QWAC). Aggiornati i riferimenti normativi.	AS
28 febbraio 2019	5.1	1.3.1	Aggiornamento Legale Rappresentante	AS
23 maggio 2019	5.2	1.3.1.2, 3.2.2.5, 4.9.1.1, 7.1.2.3, 7.1.4.2.1 9.13	Allineamento alle versioni correnti dei [BR] e delle [EVGL]. Aggiornamento elenco delle CA subordinate. Precisazioni sul profilo dei certificati. Correzione refusi. Aggiornamento paragrafo 9.13 “Foro competente”	AS
29 agosto 2019	5.3	7.1	Inserite indicazioni sull’applicazione delle raccomandazioni emanate dall’Agenzia con Det. AgID n.121/2019	FC
26 settembre 2019	5.4	4.9.1.1, 7.1.2.3	Precisazioni sulla revoca da parte della CA nel caso di qualsiasi non-conformità dei certificati ai BR e/o EVGL. Previste anche le chiavi di tipo ECC (P256/P384) nei certificati dei Titolari	AS
08 ottobre	5.5	7.1.2.2	Precisazioni sulla EKU dei certificati di CA subordinata per conformità alla Mozilla Root Store Policy	AS
22 gennaio 2020	5.6	1.3.1.2, 1.5.2, 3.2.2.4, 4.2.2, 4.10.3, 4.12.1, 4.12.2, 4.13, 5.6.2, 6.2.3, 7.1.4.2, 7.1.2.3	Aggiornata tabella delle SubCA. Precisazioni nel §3.2.2.4. Spostato il testo del precedente §4.13 nel §1.5.2 per conformità ai BR e rimosso il §4.13. Ribadito nel §4.2.2 che non sono ammessi gli internal names. Aggiunti §4.10.3, §4.12.1, §4.12.2 per conformità alla RFC3647. Revisioni e correzione refusi nel profilo dei certificati. Precisato che non si fa key escrow.	AS

Sommario

1 Introduzione

1.1 Scopo del documento

Actalis S.p.A., società del gruppo Aruba S.p.A., è un primario certificatore attivo dal 2002, accreditato presso l'AgID ai sensi della Direttiva Europea sulle Firme Elettroniche, quindi secondo il Regolamento (EU) n.910/2014 ("eIDAS"). Actalis offre diverse tipologie di certificati e relativi servizi di gestione, oltre a diversi altri servizi fiduciari e soluzioni (www.actalis.it).

Un certificato lega una chiave pubblica ad un insieme d'informazioni che identificano un soggetto (individuo od organizzazione). Tale soggetto, titolare del certificato, possiede ed utilizza la corrispondente chiave privata. Il certificato viene generato e fornito al titolare da una terza parte fidata detta **Certification Authority** (CA). Il certificato è firmato digitalmente dalla CA.

L'affidabilità di un certificato, in particolare l'associazione certa – attestata dal certificato - tra una data chiave pubblica ed il soggetto identificato, dipende anche dalle procedure operative della CA, dagli obblighi e responsabilità che si assumono CA e titolare, e dalle misure di sicurezza fisiche e logiche della CA. Tali aspetti sono descritti in un documento pubblico chiamato **Certification Practice Statement** (CPS).

Questo documento è il CPS di Actalis relativo all'emissione e gestione di due tipi di certificati:

- certificati per SSL Server
- certificati per Code Signing

La struttura di questo CPS si basa sulla specifica pubblica [RFC 3647].

Nell'ambito del servizio di CA disciplinato da questo CPS, Actalis rispetta la versione corrente dei **Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates** del CA/Browser Forum pubblicata su http://www.cabforum.org. In caso di conflitto tra il presente documento e tali Requisiti, questi ultimi hanno la precedenza.

Inoltre, per quanto riguarda i certificati di classe EV (Extended Validation), Actalis rispetta la versione corrente delle **Guidelines for Issuance and Management of Extended Validation Certificates** del CA/Browser Forum, pubblicata su http://www.cabforum.org. In caso di conflitto tra il presente documento e tali Linee Guida, queste ultime hanno la precedenza.

1.2 Identificazione del documento

Questo documento è il **Certification Practice Statement (CPS)** relativo ai **Certificati SSL Server e Code Signing** emessi da **Actalis S.p.A.** La *versione* e la *data di ultima revisione* del documento sono indicate nella sua prima pagina. Questo documento è pubblicato sul sito web di Actalis in due lingue: Italiano e Inglese. Nel caso di difformità tra le due versioni, fa fede la versione in Italiano.

Actalis emette anche certificati di altro tipo (es. SSL Client, S/MIME) nel rispetto di policy descritte in documenti separati. Tali policy possono fare riferimento a questo CPS per quanto riguarda gli aspetti comuni (per es. infrastruttura, organizzazione, sicurezza fisica e operativa, Root CA, ecc.).

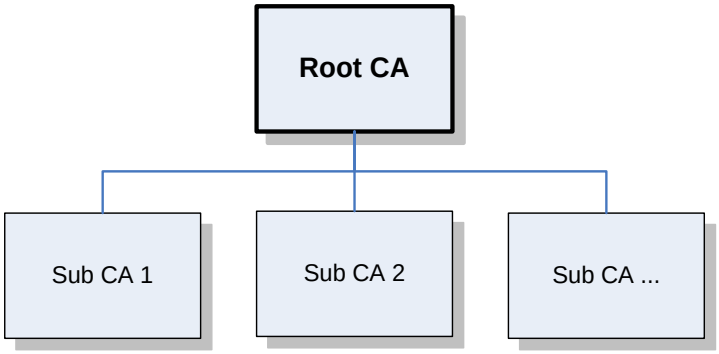
Questo CPS è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

1.3 Partecipanti alla PKI

1.3.1 Certification Authorities

La Certification Authority (CA) è il soggetto terzo e fidato che emette i certificati, firmandoli con la propria chiave privata (chiave di CA). La CA, inoltre, gestisce lo stato dei certificati.

La PKI (Public Key Infrastructure) di Actalis su cui si basa il servizio di emissione e gestione dei certificati SSL Server e Code Signing è organizzata su due livelli, come mostrato nello schema seguente:



La **Root CA** è usata esclusivamente per emettere i certificati di SubCA e le relative CRL, ed è mantenuta off-line quando non in uso. Le **Sub CA** sono le CA che emettono i certificati degli utenti finali.

Nell'ambito del servizio qui descritto, il ruolo di Root CA è ricoperto dalla società Actalis S.p.A. (in seguito solo "Actalis"), identificata come segue:

Denominazione sociale:	**Actalis S.p.A.**
Indirizzo della sede legale:	**Via S. Clemente 53 – 24036 Ponte San Pietro (BG)**
Legale rappresentante:	**Massimiliano Carollo** (Amministratore Delegato)
P.IVA e Codice Fiscale:	**03358520967**
N° di telefono (centralino):	**+39 0575.050.350**
DUNS number:	**440-489-735**
ISO Object Identifier (OID):	**1.3.159**
Sito web generale (informativo):	http://www.actalis.it
Sito web del servizio di certificazione:	https://portal.actalis.it
Indirizzo di posta elettronica (informativo):	info@actalis.it

1.3.1.1 Root Certification Authority

Come già detto, il ruolo di Root CA è gestito da Actalis S.p.A. Alla data di revisione del presente CPS, le chiavi di Root CA di Actalis sono quelle identificate di seguito; per ulteriori dettagli vedere anche il capitolo 7.

Subject DN	Subject Key ID	notBefore	notAfter
CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT	52 d8 88 3a c8 9f 78 66 ed 89 f3 7b 38 70 94 c9 02 02 36 d0	22 settembre 2011	22 settembre 2030

1.3.1.2 Subordinate Certification Authority

Alla data di revisione del presente CPS, le **Subordinate CA gestite da Actalis** sono quelle identificate di seguito; per ulteriori dettagli vedere anche il capitolo 7.

Subject DN	Subject Key ID	notBefore	notAfter
CN = Actalis Authentication CA G3 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	AA AA FD CA 8C 1D 4D F1 2E 83 E1 06 FC FA 8E EA 0E 23 AE 3D	13 feb 2014	13 feb 2024
CN = Actalis Organization Validated Server CA G1 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	23 B4 CC 8E BE 20 F9 24 D5 A9 90 A5 0A 26 39 8E D5 95 05 96	17 gen 2018	22 set 2030
CN = Actalis Organization Validated Server CA G2 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	62 FE BB 27 8A 64 44 ED 68 96 5A 58 79 A1 DB 5A 26 AD FF BB	21 mar 2019	22 set 2030
CN = Actalis Extended Validation Server CA G1 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	61 C1 E4 86 1E 4D 6D 74 74 BC D9 97 3B 31 71 78 CB 3F 9F DC	14 mag 2015	14 mag 2030
CN = Actalis Extended Validation Server CA G2 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	A1 06 8C F7 35 D0 BA 63 AF 19 08 51 98 87 01 B6 6D F6 CC DE	19 mar 2019	22 set 2030
CN = Actalis Domain Validation Server CA G1 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	1B 42 7F 5C 45 7E FF 7E 1E 1E 41 9C F3 AD AE 35 C6 65 EB C5	6 ott 2016	22 set 2030
CN = Actalis Domain Validation Server CA G2 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	D5 40 08 F7 96 22 4E 19 B3 DA E5 61 93 BA BA B7 3E EB B9 CD	19 mar 2019	22 set 2030
CN = Actalis Code Signing CA G1 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	81 39 07 34 26 00 49 44 45 CF 49 74 97 C8 9C 2B 8C A5 49 9D	21 mar 2019	22 set 2030
CN = Actalis Client Authentication CA G1 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	7E 60 FC F8 6C A7 3D 3D D7 AE 93 A1 79 02 8F B3 74 29 3B F5	14 mag 2015	14 mag 2030

CN = Actalis Client Authentication CA G2 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	6B F2 8D 9E 68 C1 25 04 1F 51 34 57 F6 16 5C 94 EA 4D 69 1A	20 set 2019	22 set 2030

Possono essere rilasciati certificati di SubCA, sotto la Root CA di Actalis, per **CA esterne** (ossia non gestite da Actalis) previa stipula di un **contratto** col quale i gestori di tali CA si impegnano, tra l'altro, a rispettare i Baseline Requirements del CAB Forum [BR][1].

A meno che non siano "technically constrained" come descritto nel par. 7.1.5 dei [BR], tali SubCA devono sottoporsi **annualmente** ad un **audit di conformità** ai [BR] da parte di un **auditor indipendente e qualificato**, nel rispetto dei requisiti di cui al cap. 8 dei [BR], e fornire tempestivamente ad Actalis l'attestazione di conformità emessa annualmente dall'auditor. In mancanza di tale attestazione, il certificato di SubCA sarà revocato. Actalis si riserva il diritto di revocare il certificato di SubCA anche nel caso in cui l'attestazione di conformità evidenzi gravi problemi, a giudizio esclusivo di Actalis.

1.3.2 Registration Authorities

La Registration Authority (RA) è la persona od organizzazione che svolge le attività di:

- accoglimento e validazione delle richieste di emissione e gestione dei certificati;
- registrazione del soggetto richiedente e dell'organizzazione di appartenenza;
- autorizzazione all'emissione, da parte della CA, del certificato richiesto.

Per i certificati EV (Extended Validation), l'attività di RA è svolta esclusivamente da Actalis.

Solo per i certificati DV ed OV, la CA può delegare alcuni compiti di RA a terze parti (Delegated Third Parties), ad eccezione dell'attività di validazione della proprietà o controllo dei domini e indirizzi IP che rimane di responsabilità esclusiva della CA.

Le organizzazioni che soddisfano i requisiti per le "Enterprise RA", come stabiliti nei [BR], possono essere abilitate ad operare come RA limitatamente ai domini e indirizzi IP di loro proprietà o sotto il loro controllo.

1.3.3 Titolari (subscribers)

I titolari sono quelle organizzazioni o individui a cui sono emessi certificati secondo questo CPS e che detengono le corrispondenti chiavi private. In particolare:

- per i certificati SSL Server OV ed EV, il Titolare può essere solamente un'organizzazione;
- per i certificati SSL Server DV e Code Signing, il Titolare può essere un'organizzazione oppure un individuo.

Ad eccezione dei certificati DV, che per definizione non contengono informazioni identificative del Titolare, il Titolare è il soggetto identificato nel campo Subject del certificato.

Prima della verifica dell'identità e dell'emissione del certificato, il soggetto che richiede il certificato è definito "Richiedente" (**Applicant**). Dopo che il certificato è stato emesso, il soggetto è definito "Titolare" (**Subscriber**).

[1] Non è prevista l'emissione di certificati di classe EV da parte di SubCA esterne, sotto la Root CA di Actalis.

Il Cliente, ovvero l'individuo o l'organizzazione che acquista il certificato, è normalmente il Richiedente stesso, ma questo non è un requisito (un'altra entità può acquistare il certificato per conto del Richiedente).

1.3.4 Relying parties

Le "Relying Parties" sono tutti i soggetti che fanno affidamento sulle informazioni contenute nel certificato. Nel caso dei certificati per SSL Server, si tratta per esempio degli utenti del sito web interessato. Nel caso dei certificati per Code Signing, si tratta tipicamente degli utilizzatori del software firmato.

1.3.5 Rivenditori

I certificati possono essere forniti anche attraverso Rivenditori (business partner), i quali possono svolgere anche l'attività di Registration Authority, secondo gli accordi con la CA.

1.4 Uso dei certificati

1.4.1 Usi appropriati dei certificati

I certificati emessi secondo questo CPS possono essere usati per i seguenti scopi, secondo il tipo di certificato:

- i certificati **SSL Server** sono usati per abilitare il protocollo TLS/SSL su uno o più server;
- i certificati di **Code Signing** sono usati per validare la firma digitale di codice eseguibile.

Un elenco delle piattaforme e browser dove i certificati emessi secondo questo CPS sono riconosciuti ("trusted") è pubblicato sul sito web di Actalis all'indirizzo https://www.actalis.it/prodotti/certificati-ssl.aspx. I Richiedenti sono tenuti a consultare tale elenco prima di richiedere i certificati.

La CA può anche emettere altri tipi di certificati (ad es. Client SSL, S / MIME) che non sono interamente regolati da questo CPS, ma da documenti di policy separati che fanno riferimento a questo CPS per gli aspetti condivisi (ad esempio infrastruttura, gestione e controlli operativi, controlli tecnici di sicurezza, Root CA, ecc.).

Si assume inoltre che il Richiedente possegga le competenze e gli strumenti necessari per richiedere, installare e utilizzare il certificato. Actalis può fornire consulenza su richiesta, come servizio separato.

La seguente tabella indica le **classi** e **policy** dei certificati emessi in conformità al presente CPS, e i requisiti del CAB Forum applicabili a ciascuna tipologia. Ogni policy è identificata da un distinto **OID** (Object IDentifier) sotto l'arco di Actalis (**1.3.159)**:

Classe	Policy di certificato	OID	Requisiti CABF
EV	SSL Server EV (Extended Validation)	1.3.159.1.17.1	[BR], [EVGL]
OV	SSL Server WildCard OV (Organization Validated)	1.3.159.1.19.1	[BR]
OV	SSL Server OV (Organization Validated)	1.3.159.1.20.1	[BR]
OV	Code Signing (Organization Validated)	1.3.159.1.21.1	[BR]
DV	SSL Server DV (Domain Validated)	1.3.159.1.22.1	[BR]
DV	SSL Server WildCard DV (Domain Validated)	1.3.159.1.23.1	[BR]

Lo OID che identifica la policy del certificato è contenuto nell'estensione *CertificatePolicies* del certificato, come dettagliato nel capitolo 7. L'estensione contiene anche i policy OID definiti dallo stesso CAB Forum, secondo la classe del certificato.

Nel caso dei certificati *qualificati* secondo il regolamento eIDAS (vedere il paragrafo 7.1), l'estensione CertificatePolicies contiene anche il pertinente policy OID definito nella norma ETSI EN 319 411-2.

1.4.2 Usi non consentiti dei certificati

Qualsiasi uso del certificato diverso da quello previsto nel paragrafo 1.4.1 è vietato e può comportare, non appena Actalis ne venga a conoscenza, la revoca del certificato (vedere anche il paragrafo 4.9.1).

1.5 Amministrazione del CPS

1.5.1 Organizzazione responsabile

Questo CPS è redatto, aggiornato e pubblicato da Actalis S.p.A.

1.5.2 Informazioni di contatto

Per qualsiasi domanda su questo CPS, si prega di inviare e-mail a cps-admin@actalis.it.

Actalis mette a disposizione di tutte le parti interessate (Titolari, Relying Party, Fornitori di Software Applicativo quale ad es. web browser, l'autorità giudiziaria, ecc.) due diversi canali di comunicazione che consentono di segnalare alla CA, in qualsiasi momento (24x7), eventuali problemi relativi ai certificati già emessi:

- la casella di posta elettronica **cert-problem@actalis.it**, della quale si garantisce la lettura tempestiva solamente in orario lavorativo (dalle 9 alle 17 dei giorni lavorativi Italiani);
- il numero di telefono (+39) **0575-050.376**, del quale si garantisce il presidio 24x7x365.

Questi canali *non sono utilizzabili per richiedere assistenza tecnica* di alcun tipo, ma solo per segnalare problemi che possono richiedere la revoca dei certificati oggetto della segnalazione.

Indipendentemente dal canale di comunicazione utilizzato, il segnalatore deve fornire almeno le seguenti informazioni, o la segnalazione non sarà presa in considerazione:

- nome e cognome;
- numero di telefono personale;
- descrizione del presunto problema;
- informazioni sufficienti per identificare il certificato oggetto della segnalazione, per esempio:
  - per un certificato SSL Server: indirizzo del sito web sul quale è installato tale certificato, oppure hostname, data di inizio validità e numero di serie;
  - per un certificato Code Signing: commonName (CN), data di inizio validità e numero di serie.

Queste segnalazioni possono essere fatte in Italiano oppure in Inglese; altre lingue non sono gestite.

La CA si impegna a prendere in carico entro 24 ore le segnalazioni correttamente formulate, avviare le indagini sul problema segnalato e prendere i necessari provvedimenti, secondo la severità del problema. La priorità assegnata alla segnalazione dipenderà da:

- la natura del presunto problema;
- l'identità del segnalatore (per es. le segnalazioni ricevute dall'autorità giudiziaria saranno trattate con maggiore priorità rispetto ad altre segnalazioni);

- la normativa applicabile al problema (es. le segnalazioni relative ad atti illeciti saranno considerate con maggiore priorità rispetto ad altre segnalazioni).

Qualora il problema sussista, la CA deciderà caso per caso le misure da adottare (per es. la revoca del certificato) e ne darà comunicazione al segnalatore mediante e-mail.

Nota: coloro che inviano messaggi indesiderati ("spam") saranno perseguiti secondo le norme vigenti.

1.5.3 Soggetto che stabilisce l'idoneità del CPS

Questo CPS è approvato dalla Direzione dei servizi di CA di Actalis, previa verifica da parte delle funzioni aziendali interessate e tenendo conto dei Requisiti [BR] e Linee guida [EVGL] del CAB Forum, delle norme ETSI applicabili, e delle raccomandazioni ricevute dagli auditor qualificati (vedere anche il capitolo 8).

1.5.4 Procedura di approvazione del CPS

L'approvazione del CPS segue le procedure previste dal Sistema di Gestione Qualità aziendale. Questo CPS viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale.

1.6 Definizioni e acronimi

AgID	Agenzia per l'Italia Digitale (ex DigitPA)
ARL	Authority Revocation List
CA	Certification Authority
CAA	CA Authorization (tipo di record DNS)
CAB	Conformity Assessment Body
CCIAA	Camera di Commercio, Industria, Agricoltura e Artigianato
CNAME	Canonical Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DN	Distinguished Name
DV	Domain (Control) Validated
eIDAS	Electronic Identification and Trust Services (Regolamento EU n.910/2014)
EV	Extended Validation
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
gTLD	Generic TLD (Top-Level Domain)
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identificazione e Autenticazione
IDN	Internationalized Domain Name
ISO	International Standards Organization
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PDF	Portable Document Format
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Subject Alternative Names
SSL	Secure Sockets Layer (di seguito, SSL si riferisce a TLS salvo dove specificato diversamente)
TLS	Transport layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
TVCC	TV a Circuito Chiuso
UPS	Uninterruptable Power Supply
VMD	Video Motion Detection

Nel presente documento, alcuni termini in lingua Inglese (per alcuni dei quali si fornisce la traduzione in Italiano) devono essere interpretati in base alle definizioni fornite in [BR] e [EVGL]. In particolare (ma non solo) i seguenti termini: Subscriber, Subject, Applicant, Applicant Representative, Affiliate, Certificate Requester, Certificate Approver, Contract Signer, Authorization Domain Name, Base Domain Name, Domain Contact, Domain Registrant, Enterprise RA, Internal Name, Reserved IP Address.

1.7 Riferimenti normativi

[DLGS196] Decreto Legislativo 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.

[RFC2251] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997. (http://www.ietf.org/rfc/rfc2251.txt)

[RFC2314] Kaliski, B., "PKCS #10: Certification Request Syntax Version 1.5", RFC 2314, March 1998. (http://www.ietf.org/rfc/rfc2314.txt)

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013. (http://www.ietf.org/rfc/rfc6960.txt)

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol, HTTP/1.1", RFC 2616, June 1999. (http://www.ietf.org/rfc/rfc2616.txt)

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003. (http://www.ietf.org/rfc/rfc3647.txt)

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008. (http://www.ietf.org/rfc/rfc5280.txt)

[CT] Laurie, B., Kasper, E., “Certificate Transparency”, RFC 6962, June 2013. (http://www.ietf.org/rfc/rfc6962.txt)

[ETSI411-1] ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, v1.1.1 (2016-02)

[ETSI411-2] ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v2.1.1 (2016-02)

[BR] CA/Browser Forum, “Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates”. (https://cabforum.org/baseline-requirements-documents/)

[EVGL] CA/Browser Forum, “Guidelines For The Issuance And Management Of Extended Validation Certificates”. (https://cabforum.org/extended-validation/)

[GDPR] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

2 Pubblicazioni e repository

Con “repository” si intende un insieme di archivi o registri on-line contenenti informazioni di interesse pubblico relative ai certificati e al servizio di emissione e gestione degli stessi descritto in questo CPS.

2.1 Repository

Il repository di Actalis è costituito da:

- sito web di Actalis (www.actalis.it e altri siti di Actalis in esso richiamati)
- directory server LDAP della CA (ldap://ldap.actalis.it)

Nota: per ragioni di bilanciamento di carico, il servizio di directory LDAP è distribuito su più server con indirizzi differenti, per cui l’hostname inserito nei certificati può essere diverso da “ldap”.

Actalis gestisce in proprio il repository e ne è direttamente responsabile.

Il repository è normalmente accessibile in modo continuo (7x24).

2.2 Informazioni pubblicate

La CA pubblica almeno la seguente documentazione sul proprio sito web:

- Certification Practice Statement (CPS)
- certificati di CA (Root CA e Sub CA)
- Condizioni Generali del servizio
- Audit Statement
- tariffe massime del servizio
- modulistica

Actalis. inoltre, pubblica le CRL sul proprio directory server LDAP.

2.3 Tempi e frequenza delle pubblicazioni

Questo CPS e la documentazione annessa sono pubblicati sul sito web della CA ad ogni aggiornamento.

Questo CPS viene riesaminato ed aggiornato almeno annualmente, anche al fine di assicurare la sua conformità con le più recenti versioni dei requisiti [BR] e linee guida [EVGL] del CAB Forum ed altri standard applicabili.

Vedere anche il paragrafo 4.10.

2.4 Controllo degli accessi

L’accesso al repository in modalità di sola lettura (read-only) è libero per chiunque.

L’accesso al repository in modalità di scrittura (per es. per la pubblicazione di informazioni nuove o aggiornate) è possibile solo da PC o server attestati sulla stessa rete locale del repository, previa autenticazione.

3 Identificazione ed autenticazione (I&A)

Le procedure di I&A seguite da Actalis sono conformi ai requisiti del CAB Forum. In particolare, per tutti i tipi di certificato emessi sotto questo CPS, la CA svolge perlomeno le verifiche obbligatorie previste nei *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* [BR]. Inoltre, per i certificati di classe EV, la CA svolge anche le ulteriori verifiche previste dalle *Guidelines For The Issuance And Management Of Extended Validation Certificates* [EVGL].

3.1 Regole di denominazione (naming)

3.1.1 Tipi di nomi

I certificati emessi in base a questo CPS contengono un Distinguished Name (DN) non nullo conforme allo standard ITU-T X.500 (ISO / IEC 9594) nei campi Subject ed Issuer.

Inoltre, per i certificati SSL Server, devono essere soddisfatti tutti i requisiti stabiliti in [BR] ed [EVGL]. In particolare, tutti i certificati SSL Server devono contenere uno o più elementi nell'estensione Subject Alternative Name (SAN), nella quale ciascun elemento dev'essere un nome di dominio completo (FQDN) oppure un indirizzo IP. Nei certificati SSL Server di classe DV (Domain Validated) ed EV (Extended Validation), tuttavia, non sono ammessi gli indirizzi IP.

3.1.1.1 Nomi interni e indirizzi IP riservati

I nomi interni (Internal Names) e gli indirizzi IP riservati (Reserved IP Address) - vedere le rispettive definizioni nei [BR] - non sono consentiti.

3.1.1.2 Nomi di Dominio Internationalizzati (IDN)

Nessuna stipula.

3.1.2 Significatività dei nomi

I nomi sottoposti ad Actalis nella fase di richiesta del certificato devono essere significativi e non ambigui.

3.1.3 Anonimato e pseudonimia dei Titolari

Ad eccezione dei certificati SSL Server di classe DV (Domain Validated), che per definizione non contengono informazioni di identificazione del Titolare, in tutti gli altri casi il certificato deve contenere il nome ufficiale (ossia registrato) del Titolare oppure un DBA ("Doing Business As") verificato.

3.1.4 Regole per l'interpretazione dei nomi

Tutti i tipi di nomi inseriti nei certificati devono essere interpretati in base agli standard ITU-T X.500 (ovvero ISO/IEC 9594) ed RFC 5820, tenendo conto anche dei Requisiti [BR] e delle Linee guida [EVGL] del CAB Forum per quanto riguarda i certificati SSL Server.

3.1.5 Univocità dei nomi

Nessuna stipula.

3.1.6 Riconoscimento, verifica e ruolo dei marchi registrati

I nomi che violano i diritti di proprietà intellettuale di altri non sono ammessi nei certificati. Actalis non sarà coinvolta in alcuna controversia riguardante la proprietà dei nomi di dominio, dei nomi o marchi commerciali o

simili. Actalis si riserva il diritto di rifiutare la richiesta di certificato (o revocare un certificato già emesso) nel caso di una tale controversia.

3.2 Validazione iniziale dell'identità

3.2.1 Dimostrazione del possesso della chiave privata

La prova del possesso, da parte del Richiedente, della chiave privata corrispondente al certificato richiesto si basa sulla verifica crittografica della CSR (Certificate Signing Request) inviata alla CA. Il Richiedente, infatti, deve inviare la propria chiave pubblica alla CA sotto forma di CSR in formato PKCS#10 [RFC2314]. La CA verifica che la firma digitale contenuta nella CSR sia valida.

3.2.2 Autenticazione dell'organizzazione e dei domini

3.2.2.1 Identità

Quando il certificato deve includere il nome o l'indirizzo di un'organizzazione, la CA verifica l'identità e l'indirizzo dell'organizzazione e che l'indirizzo corrisponda alla sede legale od operativa del Richiedente. Questa verifica viene eseguita in accordo col paragrafo 3.2.2.1 dei [BR] oppure, per i certificati EV, col par. 11.2 delle [EVGL].

Actalis normalmente consulta le seguenti fonti:

- per le organizzazioni private, la Camera di Commercio pertinente (ove applicabile) o un'altra fonte attendibile di informazioni, privata o governativa, che soddisfi i requisiti del paragrafo 3.2.2.7;
- per gli pubblici, il pertinente indice o registro ufficiale delle pubbliche amministrazioni.

A discrezione esclusiva di Actalis, secondo le circostanze, possono essere utilizzate anche altre fonti di informazione che soddisfano i requisiti del paragrafo 3.2.2.7.

Il nome del Richiedente deve corrispondere al nome dell'organizzazione risultante da tali ricerche. Nel caso di discrepanze (a meno di differenze trascurabili come ad es. le maiuscole/minuscole, i segni diacritici non significativi o la punteggiatura), a meno che il Richiedente non possa fornire una prova esplicativa, la domanda di certificato sarà respinta. Qualsiasi ambiguità deve essere risolta dal Richiedente.

La CA può utilizzare le stesse fonti di informazioni per verificare anche l'indirizzo del Richiedente. Quando l'indirizzo del Richiedente richiesto non può essere verificato in questo modo, il Richiedente dovrà fornire alla CA una fattura/bolletta (per es. del telefono, energia elettrica o altra utility) oppure un estratto conto bancario o di una carta di credito che riporti l'indirizzo completo del Richiedente. La CA potrebbe accettare anche altre forme di evidenza, previa valutazione caso per caso.

Le informazioni raccolte dalla CA comprendono almeno:

- esistenza e stato effettivi dell'organizzazione richiedente
- nome legale (cioè registrato) dell'organizzazione richiedente
- indirizzo completo della sede legale e dei siti operativi dell'organizzazione richiedente
- il numero di registrazione dell'organizzazione richiedente emesso dalla giurisdizione competente
- Partita IVA e/o Codice Fiscale dell'organizzazione equivalente o equivalente (ove applicabile)
- il numero generale di telefono e/o di fax dell'organizzazione richiedente, se disponibile
- l'indirizzo di posta elettronica generale dell'organizzazione richiedente, se disponibile

In generale, se la CA non è in grado di reperire in autonomia le informazioni di cui sopra, il Richiedente sarà tenuto a fornirle alla CA, fatta salva la successiva valutazione da parte della CA dell'affidabilità delle informazioni fornite alla luce dei requisiti minimi stabiliti nei [BR].

3.2.2.2 DBA/Tradename

Se il Subject del certificato deve includere un DBA (Doing Business As) o un nome depositato (non applicabile ai certificati SSL Server DV), la CA verifica il diritto del Richiedente di utilizzare tale DBA o nome depositato con almeno uno dei metodi nel paragrafo 3.2.2.2 dei [BR] o, per i certificati EV, nel paragrafo 11.3 delle [EVGL].

3.2.2.3 Verifica del paese (country)

Quando il campo Subject del certificato deve includere un codice paese (non applicabile ai certificati SSL Server di classe DV), la CA verifica il paese utilizzando uno dei metodi previsti nel paragrafo 3.2.2.2 dei [BR].

3.2.2.4 Verifica della proprietà o del controllo del dominio

Prima di emettere un certificato **SSL Server**, la CA verifica che **tutti gli FQDN** da includere nel certificato siano **di proprietà o sotto il controllo di fatto del Richiedente o di una sua affiliata** (ad esempio la holding o una controllata). Questa verifica (anche detta Domain Control Validation: DCV) viene svolta con uno dei seguenti metodi:

- La CA conferma, interrogando direttamente il Domain Name Registrar (ad esempio tramite WHOIS), che il Richiedente sia il Registrant del dominio. Questo metodo può essere utilizzato solo se il “Base Domain Name” è stato registrato da Aruba S.p.A. (società holding di Actalis).
- La CA invia un valore casuale via e-mail ad un Contatto del Dominio (presente nel record WHOIS dello Authorization Domain Name) e riceve una risposta di conferma basata sullo stesso valore casuale.
- La CA invia un valore casuale via e-mail a un indirizzo ottenuto concatenando "admin@" o "administrator@" o "webmaster@" o "hostmaster@" o "postmaster@" allo Authorization Domain Name e riceve una risposta di conferma basata sullo stesso valore casuale.
- La CA ottiene dal Registrar del dominio un'attestazione circa l'autorità del Richiedente ad ottenere un Certificato per il FQDN in esame. Tale attestazione deve essere fornita alla CA in modo tale da comprovarne l'origine e l'autenticità, a esclusivo giudizio della CA.
- La CA chiede al Richiedente di pubblicare un file sul server HTTP al FQDN in esame, sotto la directory "/.well-known/pki-validation", contenente un valore casuale fornito dalla CA, quindi verifica la presenza di tale file, con il contenuto previsto.
- La CA chiede al Richiedente di inserire un record TXT, contenente un valore casuale fornito dalla CA, nelle informazioni DNS dello Authorization Domain Name, quindi verifica la presenza di tale record con il contenuto previsto.
- La CA verifica, secondo il paragrafo 3.2.2.5, che il Richiedente abbia il controllo di fatto dell’indirizzo IP restituito da una query DNS per il record A oppure AAAA del FQDN in esame. Questo metodo non può essere utilizzato per gli FQDN di tipo wildcard.

Nota: nell'elenco dei metodi DCV sopra riportato, lo “Authorization Domain Name” è ottenuto eliminando zero o più componenti dal FQDN richiesto, fino ad un suffisso pubblico o un'etichetta controllata dal registro.

In tutti i casi, la DCV viene eseguita in piena conformità con il paragrafo 3.2.2.4 dei [BR]. La CA non utilizza metodi DCV diversi da quelli previsti nei [BR].

Il particolare metodo di DCV utilizzato per verificare un determinato FQDN può dipendere dalle circostanze e dalle preferenze del richiedente. La gamma dei metodi DCV supportati può variare secondo lo specifico canale utilizzato per richiedere il certificato.

3.2.2.5 Autenticazione degli indirizzi IP

Prima di emettere un certificato **SSL Server**, la CA verifica che **tutti gli indirizzi IP** da includere nel certificato (non ammessi nei certificati di classe DV ed EV) siano **controllati dal Richiedente o da una sua affiliata** (ad esempio la holding o una controllata). Questa verifica viene svolta con uno dei seguenti metodi:

- il Richiedente dimostra di avere il controllo materiale dell'indirizzo IP pubblicando un file sul server HTTP all'indirizzo IP in esame, sotto la directory "/.well-known/pki-validation", contenente un valore casuale fornito dalla CA, quindi la CA verifica la presenza di tale file con il contenuto previsto;
- La CA invia un valore casuale via e-mail ad un Contatto dell'Indirizzo IP – contatto ottenuto mediante consultazione della IANA (Internet Assigned Numbers Authority (IANA) o di un registro Internet regionale (RIPE, APNIC, ARIN, AfriNIC, LACNIC) – e riceve una risposta di conferma basata sullo stesso valore casuale;
- mediante "Reverse IP Lookup" e successiva verifica del nome di dominio così ottenuto svolta con uno dei metodi descritti nel paragrafo 3.2.2.4.

3.2.2.6 Validazione dei domini wildcard

Prima di emettere un certificato **SSL Server**, se il certificato deve includere un **FQDN di tipo wildcard** ("jolly") nel commonName (CN) del Subject oppure nell'estensione Subject Alternative Name, la CA determina se il carattere "jolly" (ossia l'asterisco) ricade nell'etichetta immediatamente a sinistra di un suffisso controllato da un Registry o un suffisso pubblico; in tal caso, la CA respingerà la richiesta di certificato a meno che il Richiedente non dimostri il suo legittimo controllo dell'intero dominio. Ai fini di questa verifica, Actalis consulta l'elenco dei suffissi pubblici disponibile all'indirizzo https://publicsuffix.org/.

3.2.2.7 Accuratezza delle fonti di informazione

Prima di utilizzare qualsiasi fonte di informazioni ai fini della validazione delle richieste, la CA valuta l'affidabilità, accuratezza e resistenza alle alterazioni o falsificazioni della fonte, in accordo col par. 3.2.2.7 dei [BR].

3.2.2.8 Record CAA del dominio

Come parte del processo di emissione, la CA verifica la presenza di eventuali record CAA per ciascun dNSName nell'estensione Subject Alternative Name del certificato da rilasciare, secondo la procedura descritta nella RFC 6844 e nel par. 3.2.2.8 dei [BR]. Le CA non rilascerà il certificato a meno che (1) la richiesta di certificato sia coerente con l'insieme dei record CAA applicabili oppure (2) si applichi un'eccezione. Le uniche eccezioni ammesse sono quelle elencate nel par. 3.2.2.8 dei [BR]. Il dominio identificativo di Actalis nei record CAA è "**actalis.it**".

3.2.2.9 Ulteriori verifiche

Per i certificati di classe EV, la CA verifica inoltre:

- l'**esistenza fisica** del Richiedente (o di una sua affiliata) ai sensi del paragrafo 11.4 di [EVGL];
- l'**esistenza operativa** del Richiedente (o di una sua affiliata) ai sensi del paragrafo 11.6 delle [EVGL].

Per il secondo punto, Actalis controlla normalmente che l'organizzazione Richiedente esista da almeno 3 anni, interrogando fonti di informazioni attendibili (vedere 3.2.2.1), o chiedendo al Richiedente di dimostrare il possesso di un conto corrente bancario. A tal fine, il Richiedente può fornire alla CA una lettera di referenze bancarie, redatta su carta intestata della banca, datata e firmata dalla banca.

Actalis si riserva di respingere la richiesta di certificato nel caso in cui riscontri situazioni problematiche (per es. procedure concorsuali, controversie, insolvenza, ecc.) a carico del Richiedente o del suo Rappresentante.

3.2.3 Autenticazione delle identità individuali

Per i certificati contenenti Informazioni sull'identità del Titolare, se il Richiedente è una persona fisica la CA verifica il nome del Richiedente, l'indirizzo del Richiedente e l'autenticità della richiesta di certificato in conformità con il paragrafo 3.2.2 dei [BR]. A tal fine, Actalis normalmente:

- verifica il nome del Richiedente attraverso l'esame di una copia leggibile, che mostra chiaramente il volto del Richiedente, di almeno un documento d'identità valido rilasciato dal governo (es. passaporto, patente di guida, carta d'identità o equivalente) e accertandosi che la copia non mostri segni evidenti di alterazione o falsificazione;
- verifica l'indirizzo del Richiedente utilizzando un metodo ritenuto affidabile, come per es. un documento di identità, una bolletta o un estratto conto bancario o della carta di credito. Actalis può fare affidamento, a questo fine, sullo stesso documento utilizzato per verificare il nome del Richiedente;
- verifica l'autenticità della richiesta di certificato contattando il Richiedente con un metodo di comunicazione affidabile.

3.2.4 Informazioni del Titolare non verificate

La CA non verifica le seguenti informazioni sul Titolare:

- nome dell'unità organizzativa da inserire nel certificato (purché non sia fuorviante);
- informazioni non necessarie ai fini dell'identificazione del Titolare;
- indirizzi di e-mail specificati nei moduli di richiesta del certificato.

In generale, la CA non verifica la correttezza delle informazioni ricevute dal Richiedente che non devono essere incluse nei campi sensibili del certificato e che non sono necessarie per l'emissione e la successiva gestione (per es. la revoca) del certificato.

3.2.5 Verifica dell'autorizzazione

Per i certificati contenenti Informazioni sull'identità del Titolare, se il Richiedente è un'organizzazione la CA utilizza un metodo di comunicazione affidabile per verificare l'autenticità della richiesta di certificato sottoposta dal Rappresentante del Richiedente, in accordo con il paragrafo 3.2.5 dei [BR] o con il paragrafo 11.8.3 delle [EVGL], secondo la classe di certificato.

La CA può utilizzare le fonti elencate nel §3.2.2.1 per individuare un metodo affidabile di comunicazione.

Actalis utilizza normalmente uno dei seguenti metodi per verificare l'autenticità della richiesta:

- Telefonicamente: un Validation Specialist della CA contatta telefonicamente il Richiedente, attraverso il numero di telefono generale dell'organizzazione Richiedente (ottenuto da una fonte affidabile di informazioni) e chiede conferma che la richiesta di certificato ricevuta dal Rappresentante del Richiedente sia autentica.
- Autenticazione on-line: il Rappresentante del Richiedente invia la richiesta di certificato alla CA tramite un sito web o un web service che richiede l'autenticazione on-line con le credenziali personali fornite al Rappresentante del Richiedente previa identificazione dello stesso da parte della CA.

- Posta elettronica certificata: il richiedente specifica il nome e i dettagli di contatto dei propri Rappresentanti in un messaggio di e-mail inviato alla CA tramite un servizio di Posta Elettronica Certificata[2] (o un servizio equivalente) dalla casella di posta certificata del Richiedente (il cui indirizzo sia confermato da una fonte di informazioni attendibile);
- Firma digitale: il Richiedente invia alla CA un modulo di richiesta di certificato comprensivo del nome e dei dettagli di contatto dei propri Rappresentanti, come documento firmato digitalmente; la firma dev'essere una *firma elettronica qualificata* (conforme alle norme Europee) e il certificato del firmatario dev'essere valido (non scaduto né revocato) e chiaramente attribuibile al Richiedente.
- Ordine di acquisto formale: il nome e i dettagli di contatto dei Rappresentanti del Richiedente sono forniti alla CA come parte di, o in allegato a, un ordine di acquisto formale emesso direttamente dal Richiedente, redatto su carta intestata del Richiedente, inclusivo dei dati identificativi completi del Richiedente, e inviato alla CA dall'Ufficio Acquisti (o analogo dipartimento) del Richiedente.

Per i certificati EV, la CA verifica il nome, il titolo e l'autorità (rappresentanza) del Firmatario del Contratto (Contract Signer) e dell'Approvatore del Certificato (Certificate Approver) in accordo col paragrafo 11.8 delle [EVGL]. Ai fini di tale verifica, Actalis richiede normalmente una specifica dichiarazione da parte del Firmatario del Contratto, basata su un modello fornito da Actalis, che deve essere firmata con le modalità indicate nel par. 4.1.2.

3.2.6 Criteri di interoperabilità

La CA divulga tutti i cross-certificati nei quali essa compare come Subject, purché abbia definito o accettato le condizioni della cross-certificazione.

3.3 Identificazione e autenticazione per le richieste di riemissione

3.3.1 Identificazione e autenticazione per le riemissioni di routine

La riemissione di un certificato può verificarsi di routine in due casi:

- quando il Titolare desidera sostituire un certificato esistente con uno nuovo (con i medesimi o diversi dettagli) contenente una chiave diversa;
- quando un Titolare desidera rinnovare un certificato che sta per scadere, ovvero ottenere un nuovo certificato con gli stessi dettagli di quello che sta per scadere; in questo caso, la CA richiede che il nuovo certificato contenga una nuova chiave.

In entrambi i casi, la CA può richiedere al Titolare di seguire le stesse procedure di identificazione e autenticazione utilizzate per l'emissione iniziale del certificato, secondo l'età dei dati di validazione utilizzati per l'emissione iniziale (in considerazione dei requisiti stabiliti nei [BR] e nelle [EVGL]) e secondo il canale di richiesta.

3.3.2 Identificazione e autenticazione per la riemissione a seguito di revoca

Dopo che un certificato è stato revocato, il Titolare che desidera un nuovo certificato deve generare una nuova coppia di chiavi e seguire tutte le normali procedure di identificazione e autenticazione come per l'emissione del certificato iniziale.

3.4 Identificazione e autenticazione per le richieste di revoca

Vedere il paragrafo 4.9.3.

[2] Vedere https://it.wikipedia.org/wiki/Posta_elettronica_certificata.

4 Requisiti operativi di gestione dei certificati

4.1 Richiesta del certificato

4.1.1 Chi può richiedere i certificati

Le richieste di certificato possono essere sottomesse alla CA dal Richiedente (ossia il futuro Titolare) oppure da una persona fisica che sia autorizzata dal Richiedente a sottomettere richieste di certificato alla CA a nome del Richiedente, nel rispetto dei requisiti descritti nel paragrafo 3.2.5.

La CA mantiene un database interno di tutti i certificati che sono stati revocati, e delle richieste di certificato che sono state rifiutate, perché vi era il sospetto di un uso illecito del certificato (es. phishing) o per altre gravi ragioni. La CA utilizza queste informazioni per identificare le successive richieste sospette.

4.1.2 Processo di richiesta e responsabilità

La procedura di richiesta del certificato include i seguenti passaggi obbligatori:

- generazione di una idonea coppia di chiavi;
- invio ad Actalis di un modulo di richiesta certificato;
- consegna ad Actalis della chiave pubblica del Richiedente;
- accettazione e/o firma dell'Accordo di Servizio (Subscriber Agreement) del caso;
- pagamento del prezzo del certificato (secondo la classe del certificato, del tipo, ecc.).

Tutti i passaggi sopra indicati, tranne l'ultimo, sono a carico del Richiedente. Il pagamento può eventualmente essere effettuato da un diverso soggetto, per conto del Richiedente.

L'ordine in cui vengono eseguiti questi passaggi può variare secondo le circostanze, ma tutti quanti devono essere completati (con l'eventuale eccezione del pagamento che può essere differito, a seconda del cliente e dell'importo dovuto, previa approvazione dal reparto vendite di Actalis) prima che la richiesta di certificato sia presa in carico dalla CA.

Per i certificati SSL server DV e OV e per i certificati di Code Signing, i seguenti ruoli del Richiedente sono richiesti, come definito nei [BR], e applicati nell'ambito del processo di richiesta:

- Richiedente (il futuro Titolare del certificato)
- Rappresentante del Richiedente (la persona fisica che sottopone la richiesta alla CA)

Per i certificati SSL Server EV, sono necessari i seguenti ruoli aggiuntivi del Richiedente, come definito in [EVGL], e applicati nell'ambito del processo di richiesta:

- Certificate Requester (la persona fisica che sottopone la richiesta alla CA)
- Certificate Approver (la persona fisica che approva la richiesta per conto del Richiedente)
- Contract Signer (la persona fisica che sottoscrive l'Accordo di Servizio – Subscriber Agreement)

Il Richiedente può autorizzare una persona a ricoprire due o più dei ruoli di cui sopra e/o può autorizzare più di una persona a ricoprire lo stesso ruolo.

A seconda della classe del certificato e del canale di richiesta, la richiesta del certificato può essere fatta compilando e inviando alla CA (ad esempio via e-mail) un opportuno modulo di richiesta, reperibile sul portale della CA, oppure compilando un modulo web. La richiesta di certificato può essere inviata/sottoposta alla CA direttamente dal Richiedente (o dal Rappresentante del Richiedente) oppure da un Rivenditore o da una Registration Authority per conto del Richiedente.

Le Enterprise RA possono richiedere certificati tramite una specifica applicazione web gestita da Actalis.

La richiesta del certificato include sempre le seguenti informazioni:

- tipo, classe e durata (validità) del certificato richiesto
- per i certificati SSL Server, gli FQDN e/o indirizzi IP da includere nel certificato
- (eccetto per i certificati SSL Server DV) il valore proposto per il Subject DN
- nome e dettagli di contatto di uno o più contatti tecnici

Solo per i certificati di classe OV ed EV, devono essere fornite anche le seguenti informazioni:

- dettagli dell'organizzazione richiedente (nome ufficiale, numero di registrazione, indirizzo, ecc.)
- nome e dettagli di contatto di un opportuno contatto organizzativo

La richiesta di certificato include, come passaggio obbligatorio, l'esplicita accettazione da parte del Richiedente di un Accordo di Servizio (che può essere denominato anche "Condizioni Generali") che incorpora questo CPS mediante riferimento. A seconda della classe del certificato e della particolare procedura o canale di richiesta, il Richiedente può accettare l'Accordo di Servizio in diversi modi, quali ad esempio:

- mediante "point & click” su un modulo web (ai sensi delle norme Europee sui contratti a distanza);
- confermando espressamente l'accettazione ad Actalis per iscritto (possibilmente via email);
- mediante firma autografa;
- mediante firma digitale.

Quando è richiesta una firma vera e propria, deve essere apposta da una persona opportunamente autorizzata.

Le richieste di certificati EV devono essere presentate da un Certificate Requester autorizzato e devono essere approvate da un idoneo Certificate Approver, in conformità con le [EVGL]. La richiesta di certificato dev’essere accompagnata da un Accordo di Servizio firmato da un idoneo Contract Signer, ai sensi delle [EVGL]. L’Accordo di Servizio EV dev’essere firmato in uno dei seguenti modi:

- mediante firma autografa apposta in presenza di un rappresentante Actalis (che controfirma come testimone);
- mediante firma autografa autenticata da un notaio o da un'altra persona che, ai sensi della legge applicabile, abbia l'autorità per autenticare l'esecuzione di una firma su un documento (per es. un pubblico ufficiale in Italia); (*)
- mediante una firma elettronica qualificata valida, conforme alle normative Europee.

(*) In questo caso, la copia autenticata dell’Accordo di Servizio dev’essere inviata alla CA in originale. La richiesta di certificato non verrà presa in carico finché Actalis non abbia ricevuto e verificato tale originale.

Prima di accettare e/o firmare l'Accordo di Servizio, il Richiedente o il suo Rappresentante deve esaminare tutti gli aspetti del servizio CA di Actalis, leggendo la documentazione pubblicata sul sito web della CA.

Il modulo di richiesta del certificato e l'Accordo di Servizio (e Condizioni Generali) sono disponibili in lingua Italiana e Inglese. Actalis non si impegna a supportare altre lingue.

Il modulo di richiesta del certificato dev'essere accompagnato o seguito da una appropriata Certificate Signing Request (CSR) conforme al paragrafo 3.2.1.

4.2 Elaborazione delle richieste

4.2.1 Svolgimento delle funzioni di identificazione e autenticazione

Al ricevimento di una richiesta di certificato, tutte le verifiche precedentemente descritte (vedere capitolo 3 e i paragrafi precedenti di questo capitolo) vengono eseguite automaticamente, ove possibile e consentito, oppure manualmente da un Validation Specialist quando necessario od obbligatorio, secondo la classe del certificato, in conformità con [BR] e [EVGL].

A seconda dell'età e dell'applicabilità dei dati di validazione già disponibili, la CA può riutilizzare le convalide precedenti (documenti, dati, ecc.), per i certificati aggiuntivi da rilasciare allo stesso Richiedente, nei limiti consentiti dai [BR] e delle [EVGL] (secondo la classe del certificato).

La CA verifica inoltre che le informazioni contenute nella CSR (ad esempio il Subject DN, gli FDQN e/o indirizzi IP) siano coerenti con quelle fornite nel modulo di richiesta del certificato e con il tipo di certificato richiesto, e respinge la richiesta in caso di conflitti o anomalie.

Per i certificati EV SSL Server, Actalis applica il principio della "Separation of Duties" per garantire che nessuna persona possa validare e autorizzare *da sola* l'emissione di un certificato EV, in conformità con il paragrafo 14.1.3 delle [EVGL]. In particolare, la "Final Cross-Correlation and Due Diligence" (vedere il paragrafo 11.13 di EVGL) viene svolta da un diverso Validation Specialist rispetto a quello che ha eseguito i precedenti passaggi.

Una volta superati con successo le principali fasi di validazione, la CA normalmente invia al Rappresentante del Richiedente, via e-mail, le credenziali di autenticazione necessarie per accedere al portale CA, per l'eventuale sottomissione di richieste di revoca.

4.2.2 Approvazione o rifiuto delle richieste

L'approvazione delle richieste di certificazione richiede il completamento con successo di tutti i passaggi di validazione descritti sin qui, nel pieno rispetto delle politiche della CA. A questo punto, l'accettazione delle richieste è subordinata ai seguenti criteri:

- Non saranno emessi certificati contenenti "internal names".
- Non saranno emessi certificati contenenti un nuovo gTLD *in esame* da parte di ICANN.
- Non saranno emessi certificati per domini che contengono ".onion" nella label più a destra.
- Saranno rigettate le richieste di certificati per domini che, al momento dell'emissione, sono segnalati come rischiosi (per es. a causa di phishing o malware) dai principali servizi di "domain reputation".
- Actalis mantiene un elenco di domini di alto profilo e bloccherà l'emissione di certificati contenenti uno di tali domini, al fine di mitigare i rischi associati. Prima che tali richieste possano essere approvate, al

Richiedente sarà richiesto di fornire informazioni aggiuntive per confermare il suo effettivo diritto di utilizzare tali domini.

4.2.3 Tempi di elaborazione delle richieste

Nessuna stipula.

4.3 Emissione del certificato

4.3.1 Azioni della CA durante l'emissione del certificato

Se i passaggi precedenti (vedere il paragrafo 4.2) sono superati con successo, il sistema CA:

- verifica che il CSR sia ben formato e non contenga dati inattesi;
- verifica che la CSR sia crittograficamente valida secondo il paragrafo 3.2.1;
- verifica che la chiave nella CSR non sia una nota "chiave debole" (vedere CVE-2008-0166);
- controlla i record CAA pertinenti (se presenti) secondo il paragrafo 3.2.2.8.

Se tutti i controlli sopra riportati hanno esito positivo, la CA genera il certificato, lo memorizza nel suo database e infine invia al Richiedente una e-mail contenente almeno:

- il certificato del Titolare (oppure un link ad esso);
- il certificato della CA emittente (oppure un link ad esso).

Per i certificati dei Titolari, le operazioni di cui sopra sono normalmente eseguite in modo automatico.

Tutti i certificati SSL Server rilasciati dopo il 30 aprile 2018 devono essere conformi ai requisiti di Certificate Transparency secondo la specifica [CT]. Quando un certificato sta per essere emesso, un pre-certificato viene anzitutto generato e sottoposto ad un numero adeguato di CT log qualificati, in base alla Chromium CT Policy (https://github.com/chromium/ct-policy). Ogni CT log restituisce un timestamp del certificato (SCT) come prova di inclusione nel log. Solo a questo punto viene generato il certificato finale, nel quale gli SCT vengono incorporati come estensione (con OID 1.3.6.1.4.1.11129.2.4.2).

Nel caso di un certificato di CA subordinata, tuttavia, l'emissione del certificato richiede l'intervento di una persona debitamente autorizzata (per es. un operatore privilegiato della CA, il security officer o il responsabile della PKI) che deve dare manualmente un comando esplicito affinché la Root CA esegua la firma del certificato.

4.3.2 Notifica di emissione certificato al Titolare

Il Titolare viene normalmente informato via e-mail dell'emissione del certificato, direttamente dalla CA oppure dalla RA e/o Rivenditore ove applicabile, a condizione che l'indirizzo e-mail fornito alla CA a tale scopo dal Rappresentante del Richiedente (o Certificate Requester nel caso EV) sia valido.

4.4 Accettazione del certificato

4.4.1 Comportamenti che costituiscono accettazione del certificato

Il Certificato si intende accettato trascorsi 30 giorni dalla data di consegna, come attestata dalla data del messaggio di posta elettronica tramite il quale esso viene inviato al Titolare, in assenza di comunicazioni in senso contrario da parte del Titolare stesso.

L'uso pubblico del certificato (per es. installazione su un sito web ad accesso pubblico, firma di codice eseguibile scaricabile da siti web ad accesso pubblico), anche se temporaneo, implica in ogni caso l'accettazione del certificato da parte del Titolare.

Qualora il certificato contenga informazioni errate a causa della errata compilazione del modulo di richiesta da parte del cliente, esso dovrà in ogni caso essere pagato.

4.4.2 Pubblicazione del certificato da parte della CA

Per quanto riguarda i certificati di Root e di Sub CA, si rimanda al paragrafo 2.2.

Nessuna stipula per quanto riguarda i certificati end-entity.

4.4.3 Notifica di emissione certificato ad altri soggetti

Per tutti i nuovi certificati SSL Server, la CA sottomette il pre-certificato ad almeno due diversi Certificate Transparency (CT) log secondo la specifica RFC 6962.

4.5 Uso della coppia di chiavi e del certificato

Il Titolare usa la chiave privata per:

- (certificati per Code Signing) firmare digitalmente codice eseguibile (per es. applet Java, librerie dinamiche, ecc.) di propria produzione e/o della cui pubblicazione si assume la responsabilità;
- (certificati per SSL Server) attivare il protocollo TLS/SSL sui propri server, consentendo la TLS server authentication e la cifratura delle transazioni tra server e client.

Le Relying Parties usano il certificato per:

- (certificati per Code Signing) verificare l'integrità e l'origine di codice eseguibile;
- (certificati per SSL Server) verificare l'identità di un server e (secondo la classe di certificato) dell'organizzazione che lo gestisce, nonché scambiare in modo sicuro la chiave di sessione SSL/TLS con il server.

Vedere anche il paragrafo 1.4.

4.6 Rinnovo del certificato

4.6.1 Circostanze per il rinnovo del certificato

Con rinnovo del certificato si intende l'emissione di un nuovo certificato contenente le stesse informazioni identificative del Titolare (secondo la classe del certificato) e gli stessi domini e indirizzi IP (secondo il tipo di certificato) che si trovano in un certificato già emesso e non ancora scaduto né revocato.

La CA compie un ragionevole sforzo per segnalare ai Titolari l'avvicinarsi della data scadenza dei loro certificati, mediante l'invio periodico di email al Contatto Tecnico. Le email di avvertimento vengono inviate, normalmente, a partire da 30 giorni prima della scadenza del certificato.

4.6.2 Chi può richiedere il rinnovo

Si applica quanto descritto nel §4.1.1.

4.6.3 Elaborazione delle richieste di rinnovo

Si applica quanto descritto nel §4.2.

4.6.4 Notifica al titolare di nuova emissione del certificato

Si applica quanto descritto nel §4.3.2.

4.6.5 Comportamenti che costituiscono accettazione del certificato rinnovato

Si applica quanto descritto nel §4.4.1.

4.6.6 Pubblicazione del certificato rinnovato da parte della CA

Si applica quanto descritto nel §4.4.2.

4.6.7 Notifica ad altri soggetti della nuova emissione del certificato

Si applica quanto descritto nel §4.4.3.

4.7 Rigenerazione della chiave

La rigenerazione della chiave di un certificato consiste nella creazione di un nuovo certificato, con una nuova chiave pubblica ed un nuovo numero di serie, mantenendo le stesse informazioni sul Titolare (Subject) presenti nel certificato corrente, purché quest'ultimo non sia scaduto né revocato (diversamente si ricade nel caso della prima emissione).

La rigenerazione della chiave è un passo obbligatorio nel caso in cui venga richiesto il rinnovo di un certificato, ma può essere richiesta anche a seguito della compromissione della chiave corrente oppure per altre ragioni a discrezione della CA.

La rigenerazione della chiave può essere richiesta dal Titolare oppure dalla CA o da una RA, secondo i casi.

Generalmente, la procedura per elaborare una richiesta rigenerazione della chiave è uguale all'emissione di un nuovo certificato. Se le evidenze raccolte in fase di I&A (vedere il par. 3.2) sono ancora valide, la CA può elaborare la richiesta senza necessariamente rifare la I&A, in tal caso essendo sufficiente una richiesta autenticata da parte del Titolare.

4.8 Modifica del certificato

Modificare un certificato significa creare un nuovo certificato per lo stesso Titolare, e con la stessa o una diversa chiave pubblica, ma con informazioni identificative (es. parti del Subject o del SubjectAlternativeNames) che differiscono dal vecchio certificato.

La modifica del certificato può essere richiesta dal Titolare oppure dalla CA o da una RA, secondo i casi.

Nel caso in cui il vecchio certificato contenga informazioni errate a causa di errori commessi dalla CA o dalla RA, quel certificato errato sarà revocato e ne verrà emesso uno corretto senza oneri aggiuntivi per il cliente.

Nel caso in cui il vecchio certificato contenga informazioni errate a causa di errori commessi dal Richiedente (per es. errata compilazione di uno o più campi del modulo di richiesta), quel certificato errato sarà revocato ed il Titolare può richiedere un nuovo certificato.

Generalmente, la procedura per modificare un certificato è uguale all'emissione di un nuovo certificato. Secondo i casi, può essere necessaria una nuova I&A (vedere il par. 3.2), completa o parziale.

4.9 Sospensione e revoca del certificato

La sospensione determina un blocco temporaneo della validità di un certificato, a partire da un dato momento (data/ora). Dopo essere stato sospeso, un certificato può essere riattivato in qualsiasi momento. Per i certificati emessi secondo il presente CPS, *la sospensione non è prevista*.

La revoca determina la cessazione anticipata della validità di un certificato, a partire da un dato momento (data/ora). La revoca di un certificato è irreversibile.

L'attuazione della revoca consiste nella generazione e pubblicazione di una nuova CRL (Certificate Revocation List) che include il numero di serie del certificato revocato, ed un corrispondente aggiornamento della base dati del servizio OCSP. Per altri dettagli sui servizi informativi sullo stato dei certificati, si rimanda al paragrafo 4.10.

4.9.1 Circostanze per la revoca

4.9.1.1 Circostanze per la revoca del certificato del Titolare

La CA revocherà un certificato **entro 24 ore** se si verifica uno o più delle seguenti circostanze:

- richiesta esplicita di revoca da parte del Titolare;
- il Titolare informa la CA che la richiesta del certificato non era stata autorizzata, e non intende autorizzarla retroattivamente;
- la CA scopre che la chiave privata del Titolare corrispondente al certificato è compromessa;
- la CA scopre che la verifica di controllo del dominio (domain control validation) per uno qualsiasi dei FQDN e/o degli indirizzi IP contenuti nel certificato non è stata eseguita in modo affidabile.

La CA revocherà un certificato **entro 5 giorni** se si verifica uno o più delle seguenti circostanze:

- il certificato non rispetta più i requisiti previsti dai paragrafi 6.1.5 e 6.1.6 dei [BR];
- la CA scopre che il certificato viene usato in modo improprio e/o illecito;
- la CA scopre che il Titolare ha violato una o più delle disposizioni delle Condizioni Generali del servizio;
- la CA scopre che l'uso di un FQDN o di un indirizzo IP contenuto nel certificato non è più consentito (per es. quando il Titolare del dominio non ha rinnovato la registrazione, oppure a seguito di un provvedimento dell'autorità giudiziaria, ecc.);
- la CA scopre che un certificato di tipo wildcard viene usato per autenticare un FQDN subordinato in modo fraudolento;
- la CA scopre che una o più delle informazioni contenute nel certificato ha subito variazioni (per es. è cambiata la denominazione dell'organizzazione Titolare);
- la CA scopre che il certificato presenta qualsiasi non conformità al presente CPS o ai requisiti [BR] o alle linee guida [EVGL] (se applicabili), indipendentemente dagli impatti di tale non conformità sulla sicurezza o sul corretto funzionamento del certificato;
- la CA scopre che il certificato contiene informazioni errate e/o fuorvianti (per es. l'organizzazione Titolare ha cessato la propria attività oppure è indicata nel certificato in modo ambiguo);
- la CA ha perso il diritto ad emettere certificati in accordo coi Baseline Requirements [BR] e non ha preso accordi con una CA sostitutiva che si faccia carico dei servizi CRL ed OCSP;
- la CA viene a sapere di una procedura che espone la chiave privata del Titolare alla compromissione (per es. viene scoperto un metodo che consente di ottenere la chiave privata partendo dalla chiave

pubblica, oppure la CA scopre che la procedura di generazione chiavi usata dal Titolare è gravemente difettosa e insicura);

- accertata compromissione della chiave privata della CA emittente (Subordinate CA);
- inadempienze contrattuali da parte del cliente (es. mancato pagamento del certificato).
- provvedimento dell'autorità giudiziaria.

Prima di revocare un certificato, la CA compirà uno sforzo ragionevole per avvisare il Titolare dell'imminente revoca, compatibilmente con i tempi massimi di revoca sopra indicati . Tuttavia, la CA revocherà *immediatamente* il certificato e *senza preavviso* nei seguenti casi:

- il certificato viene utilizzato per qualsiasi tipo di attività illecita (ad esempio attacchi di "phishing", attacchi "man-in-the-middle", distribuzione di malware, ecc.);
- il certificato è stato erroneamente emesso con CA = TRUE nella sua estensione KeyUsage.

4.9.1.2 Circostanze per la revoca del certificato della CA emittente

Actalis si atterrà a quanto stabilito nel paragrafo 4.9.1.2 dei [BR].

4.9.2 Chi può richiedere la revoca

La revoca può essere richiesta da (secondo i casi):

- Il Titolare del certificato;
- la CA emittente;
- la RA (se applicabile);
- l'autorità giudiziaria.

Inoltre, i Titolari, le Relying Party, i Fornitori di Software Applicativo e altri soggetti possono segnalare alla CA gli eventuali problemi che possono ragionevolmente giustificare la revoca del certificato (vedere il paragrafo 4.13).

In determinate circostanze il Titolare *ha l'obbligo* di richiedere prontamente la revoca del proprio certificato (vedere il paragrafo 9.6.3).

4.9.3 Procedura per la revoca

Le richieste di revoca possono essere inviate direttamente alla CA, attraverso il portale della CA. Nel caso in cui il certificato sia stato fornito tramite un Rivenditore o tramite una RA, la revoca del certificato può anche essere richiesta tramite il Rivenditore o la RA. In ogni caso, prima di poter richiedere la revoca di un certificato, è necessario autenticarsi sul sito/servizio web del caso con le credenziali fornite al Titolare, a tale scopo, al momento dell'emissione del certificato.

In alternativa, è possibile compilare un modulo di richiesta di revoca (scaricabile dal sito web di Actalis), firmato dal Titolare. Il modulo firmato deve quindi essere inviato direttamente alla CA (per es. mediante posta ordinaria o preferibilmente e-mail). Prima di eseguire la revoca, la CA verificherà che la richiesta sia autentica. Le richieste di revoca inoltrate alla CA in questo modo vengono gestite solo nei giorni lavorativi.

Per le richieste di revoca inviate on-line, i certificati saranno revocati entro 24 ore.

Indipendentemente da chi ha richiesto la revoca del certificato, la CA normalmente informerà il Titolare della avvenuta revoca tramite un messaggio di posta elettronica inviato al "Contatto Tecnico" specificato nel modulo di richiesta del certificato.

4.9.4 Periodo di grazia per le richieste di revoca

Non è previsto un periodo di grazia per le richieste di revoca dei certificati. Il Titolare deve richiedere la revoca del proprio certificato non appena siano confermate le circostanze che la impongono (vedere il par. 4.9.1).

4.9.5 Tempi massimi di attuazione della revoca

Le richieste di revoca correttamente autenticate ricevute dai Titolari vengono elaborate entro 24 ore, a condizione che la richiesta sia effettuata con la procedura on-line prevista (vedere il paragrafo 4.9.3).

Nel caso di segnalazioni di problemi che potrebbero richiedere la revoca relativi di un certificato (vedere il paragrafo 4.13), l'indagine sul presunto problema inizierà entro 24 ore dalla ricezione della segnalazione. Una volta stabilito che la revoca del certificato è giustificata, essa sarà effettuata entro 24 ore.

4.9.6 Requisiti di verifica della revoca

Vedere il paragrafo 9.6.4.

4.9.7 Frequenza di emissione delle CRL

Vedere il paragrafo 4.10.1.

4.9.8 Massima latenza delle CRL

Le CRL vengono pubblicate subito dopo essere state generate. La latenza tra il tempo di generazione e il tempo di pubblicazione può dipendere dal carico dei sistemi di elaborazione della CA; in genere è di pochi minuti e non supera i 60 minuti.

4.9.9 Disponibilità di servizi on-line di verifica revoca

Si rimanda ai paragrafi 4.10 e 7.3.

4.9.10 Requisiti dei servizi on-line di verifica revoca

La CA supporta le richieste OCSP effettuate col metodo GET, per tutti i certificati emessi.

Ad eccezione delle CA tecnicamente vincolate in linea con il paragrafo 7.1.5 dei [BR], i risponditori OCSP della CA non rispondono con uno status "good" quando sono interrogati su un certificato che non è stato rilasciato.

La CA aggiorna le informazioni fornite tramite OCSP in conformità con il paragrafo 4.9.10 dei [BR].

4.9.11 Altre modalità di pubblicizzazione della revoca

Actalis consente l’uso dello “OCSP Stapling”.

4.9.12 Requisiti particolari nel caso di compromissione della chiave

Nessuna stipula.

4.9.13 Circostanze per la sospensione

Non applicabile.

4.9.14 Chi può richiedere la sospensione

Non applicabile.

4.9.15 Procedura per la sospensione

Non applicabile.

4.9.16 Limiti sul periodo di sospensione

Non applicabile.

4.10 Servizi informativi sullo stato del certificato

In generale, lo stato dei certificati (attivo o revocato) è reso disponibile a tutti gli interessati mediante:

- pubblicazione delle Certificate Revocation List (CRL);
- erogazione di un servizio OCSP (On-line Certificate Status Protocol).

4.10.1 Caratteristiche operative

La CRL è accessibile con due modalità:

- con protocollo LDAP secondo la specifica [RFC2251]
- con protocollo HTTP secondo la specifica [RFC2616]

Gli indirizzi (URL) della CRL sono inseriti nell'estensione *CRLDistributionPoints* del certificato.

La CRL viene rigenerata e ripubblicata:

- almeno ogni 6 ore, anche in assenza di nuove revoche;
- a seguito di ogni nuova revoca.

L'indirizzo (URL) del risponditore OCSP è inserito nell'estensione *AuthorityInformationAccess* del certificato.

I servizi CRL ed OCSP sono liberamente accessibili a chiunque.

La ARL, ovvero la lista dei certificati di Sub CA revocati dalla Root CA, viene aggiornata e pubblicata:

- almeno ogni 3 mesi, anche in assenza di nuove revoche;
- a seguito di ogni nuova revoca.

4.10.2 Disponibilità del servizio

L'accesso alla CRL e al servizio OCSP è disponibile in modo continuo (24 x 7), tranne che nel caso di guasti o altri imprevisti. Vedere anche il paragrafo 9.17.1.

4.10.3 Caratteristiche opzionali

Nessuna stipula.

4.11 Cessazione del contratto

Il contratto tra la CA e il Titolare termina quando il certificato del Titolare scade o viene revocato, a seconda dell'evento che si verifica per primo.

4.12 Key escrow e key recovery

4.12.1 Politiche e pratiche di key escrow e recovery

Non applicabile.

4.12.2 Politiche e pratiche di session key encapsulation e recovery

Non applicabile.

5 Misure di sicurezza fisica e operativa

Per la gestione della proprie infrastruttura di CA, Actalis si avvale dei servizi di data center forniti dalla holding, Aruba S.p.A., che si assume la responsabilità per l'housing, la connettività Internet, la sicurezza fisica e di rete di tutti i sistemi Actalis. Il servizio di data center fornito da Aruba è certificato ISO/IEC 27001.

5.1 Sicurezza fisica

5.1.1 Ubicazione e caratteristiche costruttive dei siti produttivi

Tutti i sistemi informatici utilizzati per la fornitura dei servizi CA di Actalis sono ospitati in data center altamente sicuri di proprietà della holding Aruba S.p.A. e da essa gestiti. In particolare, Actalis dispone di almeno due infrastrutture PKI complete in luoghi separati, per ridondanza, più una terza in una località distante (> 300 km), a scopo di disaster recovery. Tutti questi data center si trovano sul territorio italiano:

- data center primario ("IT1") sito in Arezzo (AR);
- data center secondario ("IT2") sito in Arezzo (AR);
- data center di disaster recovery ("IT3") sito in Ponte S. Pietro (BG).

Le principali caratteristiche costruttive, di connettività Internet, di alimentazione elettrica, condizionamento, sicurezza ecc. dei data center sopra citati sono reperibili sul sito https://datacenter.aruba.it.

Nella seguente figura si mostra la collocazione geografica dei tre siti. Il sito "IT3" (disaster recovery) di Ponte S. Pietro (BG), nei pressi di Milano, dista circa 300 km dai siti primario e secondario in Arezzo:

Figura 1: Ubicazione dei siti produttivi della CA

5.1.2 Accessi fisici

Presso tutti i data center sono in opera:

- un sistema di **controllo accessi fisici**, in modo che l'accesso all'edificio sia possibile solo a chi ne ha effettiva necessità, previa registrazione alla reception, e che l'accesso alle sale tecniche sia consentito solo agli addetti autorizzati, previa identificazione mediante badge e relativo PIN;
- **sistemi antintrusione passivi** quali grate, vetrate antiproiettile, porte blindate, cancelli motorizzati e **sistemi antintrusione attivi** quali TVCC e VMD.

Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

5.1.3 Alimentazione elettrica e condizionamento

Tutti i data center che ospitano i servizi CA di Actalis sono dotati di:

- sistemi di alimentazione completamente ridondati per garantire la continuità dell'alimentazione elettrica in ogni condizione prevedibile;
- sistemi di ventilazione e condizionamento dell'aria (HVAC) a garanzia di condizioni climatiche ottimali per il normale funzionamento dei server ospitati nel data center.

5.1.4 Prevenzione e protezione dagli allagamenti

Tutti i data center che ospitano i servizi CA di Actalis sono dotati di sistemi di rilevamento e protezione dagli allagamenti.

5.1.5 Prevenzione e protezione dagli incendi

Presso tutti i data center è in opera un sistema antincendio realizzato nel rispetto delle norme di legge e de-gli standard tecnici di riferimento; sensori per la rilevazione incendio sono inoltre presenti in tutti i piani dell'edificio. Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

5.1.6 Conservazione dei supporti di memoria

Riguardo all'archiviazione dei supporti, si applicano le procedure stabilite dal SGSI di Actalis.

5.1.7 Smaltimento dei rifiuti

In tema di smaltimento dei rifiuti, la CA applica le disposizioni della normativa vigente.

5.1.8 Off-site backup

I backup sono archiviati in un sito diverso da quello di origine dei dati, garantendo così la possibilità di ripristino in qualsiasi condizione prevedibile.

5.2 Sicurezza operativa

Actalis mantiene un piano di sicurezza, incluso un Risk Assessment, che analizza le attività della CA, le minacce a cui sono esposte e descrive le varie misure di sicurezza tecnica, fisica e procedurale implementate al fine di mitigare adeguatamente i rischi. La valutazione del rischio viene riesaminata almeno una volta all'anno.

5.2.1 Ruoli di fiducia

Actalis ha definito e assegnato formalmente i seguenti ruoli di fiducia (trusted roles) all'interno del servizio di CA regolato da questo CPS:

- Responsabile della Sicurezza (Security Officer): responsabile dell'attuazione e della gestione delle procedure di sicurezza;
- Amministratore di Sistema (System Administrator): responsabile dell'installazione, configurazione e manutenzione dei sistemi informatici della CA;
- Operatore di Sistema (System Operator): responsabile del funzionamento quotidiano dei sistemi CA;
- System Auditor: responsabile della verifica del Giornale di Controllo (Audit Log) e degli archivi;
- Internal Auditor: responsabile dello svolgimento dei self-assessment (vedi par. 8.7) e altre verifiche;
- Specialista di Validazione (Validation Specialist): responsabile delle attività di verifica delle richieste di certificazione, come specificate in questo CPS (in particolare, con riferimento al capitolo 3);
- Registration & Revocation Officer: responsabile della verifica delle informazioni necessarie per l'emissione dei certificati e dell'approvazione delle richieste di certificato; responsabile inoltre per la modifica dello stato dei certificati (es. revoca).

Alcune persone possono ricoprire ruoli multipli purché ciò non pregiudichi la sicurezza e affidabilità della PKI e non sia vietato dalle normative e dagli standard applicabili.

I ruoli di fiducia sono assegnati dal senior management. Un elenco del personale che ricopre ruoli di fiducia è mantenuto e riesaminato annualmente e messo a disposizione degli auditor.

5.2.2 Numero di persone richieste per lo svolgimento delle attività

Per la gestione delle chiavi private della CA (generazione chiavi, backup, ripristino, cancellazione, ecc.) sono necessari almeno due soggetti designati in ruoli di fiducia ("dual control") che operano in un ambiente fisicamente protetto.

L'emissione di certificati EV richiede la partecipazione di almeno due Specialisti di Validazione.

5.2.3 Identificazione e autenticazione per ciascun ruolo

Tutti i ruoli di fiducia indicati nella sezione 5.2.1 e, in generale, il personale di Actalis utilizzano appropriati sistemi di identificazione e autenticazione prima dell'accesso ai sistemi informatici di Actalis.

In particolare, per quanto riguarda l'accesso fisico alle sale dati e agli armadi che contengono i sistemi di CA, l'identificazione ed autenticazione avviene tramite badge personale con PIN.

Per quanto riguarda gli accessi logici ai sistemi di CA, l'identificazione avviene attraverso l'utilizzo dell'account personale e relativa password oppure tramite autenticazione a due fattori (es. smartcard con PIN) nei casi che lo richiedono. In particolare, l'accesso a qualsiasi account che consenta l'emissione diretta di certificati richiede un'autenticazione forte (a più fattori).

5.2.4 Ruoli che richiedono la separazione dei compiti

Il personale che ricopre uno dei ruoli di fiducia di cui al par. 5.2.1 non può ricoprire ulteriori ruoli nell'ambito del servizio di CA, fatta eccezione per i ruoli di Validation Specialist e Registration & Revocation Officer. Vedere anche il paragrafo 5.2.2.

5.3 Sicurezza del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

Actalis, si assicura che il personale adibito ai servizi di CA sia adeguatamente competente per le mansioni assegnategli, sulla base di istruzione, formazione, addestramento, abilità ed esperienza appropriati, e che sia libero da conflitti di interesse che possono compromettere la necessaria imparzialità e il rispetto delle procedure. In particolare, in riferimento ai ruoli di fiducia, le caratteristiche e le competenze richieste sono descritte nel documento aziendale "job description".

Nel caso di nuove assunzioni, Actalis si riserva sempre di valutare quale tipo di formazione sia necessaria in relazione alle mansioni da assegnare, alle qualifiche esistenti e all'esperienza, e provvede ove necessario all'inserimento della risorsa in un piano di formazione.

5.3.2 Verifica dei precedenti

Per la definizione della rosa dei candidati, Actalis si avvale, sia in ambito tecnico che amministrativo, tanto dei curricula inviati direttamente alla società tramite gli appositi canali (es. sito web) quanto della collaborazione di società specializzate nel recruitment. Per ogni candidato viene verificata la veridicità delle informazioni contenute nei C.V. (titoli di studio, master, diplomi, corsi di qualifica specifica, ecc.). Le società di professionisti incaricate da Actalis hanno inoltre l'obbligo di richiedere referenze possibilmente per ogni potenziale candidato prima di presentarlo ad Actalis. Inoltre tutti i candidati, una volta superata la fase di selezione, devono far pervenire all'ufficio Risorse Umane copia del certificato del casellario giudiziale (o dichiarazione sostitutiva).

5.3.3 Requisiti di formazione

Il personale addetto ai servizi di CA viene adeguatamente formato, secondo le mansioni che svolge. Actalis fornisce al personale una prima formazione al momento dell'assunzione, anche attraverso corsi svolti da docenti esterni quando lo si reputa necessario, e un addestramento sul posto di lavoro ("training on the job").

Il personale addetto alle attività di verifica delle informazioni (Specialisti di Validazione) viene formato almeno sui seguenti argomenti: Infrastrutture a chiave pubblica (PKI), politiche e procedure di identificazione e autenticazione, minacce comuni alle procedure di verifica delle informazioni, requisiti [BR] e linee guida [EVGL] del CAB Forum. Le registrazioni di tale formazione, che viene erogata almeno una volta all'anno, sono conservate e messe a disposizione degli auditor su richiesta.

5.3.4 Frequenza di aggiornamento della formazione

Per tutto il personale che opera nell'ambito del servizio di CA viene valutata la necessità di nuova formazione almeno una volta all'anno (oppure anticipatamente a fronte di nuovi sviluppi / servizi), in modo da garantire che tutto il personale sia sempre in grado di eseguire le proprie mansioni in modo soddisfacente e con competenza. Inoltre, con cadenza annuale viene svolta formazione a tutto il personale su tematiche di sicurezza delle informazioni.

5.3.5 Rotazione delle mansioni

Nessuna stipula.

5.3.6 Sanzioni per le azioni non autorizzate

Nel caso di azioni non autorizzate e/o violazione delle politiche e/o procedure aziendali o di Gruppo, Actalis si riserva il diritto di attivare il procedimento disciplinare previsto dal contratto collettivo di lavoro, previa valutazione della natura e della gravità della violazione e del suo impatto sulle attività aziendali, se si è trattato del primo caso, se l'addetto era adeguatamente formato, ecc.

5.3.7 Controlli sul personale non dipendente

Qualsiasi consulente indipendente o dipendente di una Terza Parte Delegata (DTP) che partecipi all'emissione dei Certificati è pienamente soggetto al presente CPS, inclusi i requisiti di formazione e di competenza (vedere il paragrafo 5.3.3), le sanzioni (vedere il paragrafo 5.3.6), la conservazione dei documenti e la registrazione degli eventi (vedere il paragrafo 5.4.1).

Il personale non dipendente (es. consulenti) deve sottoscrivere un accordo di riservatezza (NDA) prima di iniziare a collaborare con Actalis ed eventualmente accedere a dati confidenziali.

5.3.8 Documentazione fornita al personale

Il personale in ruoli fidati viene provvisto della documentazione necessaria per svolgere i propri compiti, in base al proprio ruolo (vedere il paragrafo 5.2.1). In particolare, agli Specialisti di Validazione vengono forniti questo CPS, i Baseline Requirements [BR] e le EV Guidelines [EVGL] del CAB Forum, le istruzioni dettagliate su come svolgere correttamente le attività di identificazione e autenticazione e di rilascio dei certificati, oltre ai manuali delle applicazioni CA/RA che essi utilizzano.

5.4 Gestione del giornale di controllo

5.4.1 Tipi di eventi registrati

La CA e le eventuali Terze Parti Delegate (DTP) registrano tutti i dettagli relativi alle richieste dei certificati, alle emissioni e alla successiva gestione (ad esempio revoca) e rendono tali registrazioni disponibili agli auditor della CA. Per ciascun evento, viene registrato il tipo di evento, la data e ora di occorrenza, i dati associati (secondo il tipo di evento), il personale coinvolto (se applicabile) ed eventuali altre informazioni secondo il tipo di evento.

Sono registrati almeno i seguenti eventi, in linea con il paragrafo 5.4.1 dei [BR]:

- gli eventi relativi alla gestione del ciclo di vita delle chiavi di CA;
- gli eventi relativi alla gestione del ciclo di vita dei certificati di CA e dei Titolari;
- gli eventi rilevanti per la sicurezza (ad esempio gli accessi a sistemi PKI, azioni svolte sui sistemi della PKI e sui sistemi di sicurezza, modifiche ai profili di sicurezza, entrate e uscite dai locali della CA, ecc.).

5.4.2 Frequenza di elaborazione del giornale di controllo

Gli eventi rilevanti vengono raccolti dai sistemi che li generano e vengono trasmessi al sistema di gestione centralizzato. Presso il sistema di gestione del Giornale di Controllo, gli eventi vengono automaticamente classificati e memorizzati localmente in modo tale da consentirne la consultazione. Con frequenza giornaliera, i dati locali vengono copiati sul sistema di memorizzazione a lungo termine (vedere il par. 5.4.4).

5.4.3 Periodo di conservazione del giornale di controllo

La CA conserva il giornale di controllo per almeno 10 anni.

5.4.4 Protezione del giornale di controllo

Il giornale di controllo (audit log) viene trasferito periodicamente su un sistema remoto di archiviazione a lungo termine basato su tecnologia WORM (Write-Once, Read Many) o equivalente. La copia "live" dall'audit log è protetta da manomissioni mediante misure di sicurezza multiple.

5.4.5 Procedure di backup del giornale di controllo

I sistemi di memorizzazione in cui è archiviato il giornale di controllo (vedere il paragrafo 5.4.4) sono replicati su due data center ospitati in strutture separate.

5.4.6 Sistema di raccolta del giornale di controllo

Nessuna stipula.

5.4.7 Notifiche nel caso di rilevazione di eventi sospetti

Nessuna stipula.

5.4.8 Verifiche di vulnerabilità

Il giornale di controllo viene periodicamente esaminato, per rilevare anomalie, da parte di personale in ruoli di fiducia. Le anomalie indicanti possibili violazioni della sicurezza vengono segnalate e investigate. Gli incidenti di sicurezza sono gestiti come descritto nel paragrafo 5.7.1.

Le valutazioni delle vulnerabilità (vulnerability assessment) delle reti e dei sistemi CA vengono svolte almeno una volta all'anno da terze parti qualificate. Vedere anche il paragrafo 6.7.

Una valutazione completa del rischio viene svolta almeno una volta all'anno (vedere anche il paragrafo 5.2).

5.5 Archiviazione delle registrazioni

5.5.1 Tipi di informazioni archiviate

La CA conserva almeno le seguenti informazioni relative alla richiesta, all'emissione e alla revoca dei certificati:

- le richieste di certificati, comprese le CSR;
- i dettagli dei Richiedenti e dei loro Rappresentanti;
- ogni altra documentazione fornita dai Richiedenti;
- le verifiche effettuate dalla CA e i relativi risultati;
- le richieste di revoca di certificati;
- tutti i certificati emessi.

5.5.2 Periodo di conservazione degli archivi

Gli archivi sono conservati per almeno 7 anni oltre la data di scadenza o di revoca dei certificati.

5.5.3 Protezione degli archivi

Gli archivi sono protetti dalle modifiche o distruzioni non autorizzate da robuste misure di sicurezza. A tal fine si utilizza un servizio di conservazione documentale conforme alle norme Italiane (D.lgs. n. 82/2005: “Codice dell’Amministrazione Digitale” e successive modifiche e integrazioni) e accreditato dall’AgID.

5.5.4 Procedure di backup degli archivi

Il backup degli archivi è garantito dal sistema di conservazione di cui al paragrafo 5.5.3.

5.5.5 Marcatura temporale degli archivi

A tutte le registrazioni archiviate è associato un riferimento temporale (“timestamp”) relativo alla data e ora di creazione od occorrenza del dato, ottenute da una fonte attendibile (vedere il paragrafo 6.8).

5.5.6 Sistema di archiviazione (interno o esterno)

Vedere il paragrafo 5.5.3.

5.5.7 Procedura di recupero e verifica delle informazioni archiviate

Il sistema di conservazione di cui al paragrafo 5.5.3 consente la ricerca delle informazioni archiviate sulla base dei metadati associati, nonché il recupero e la verifica di integrità.

5.6 Passaggio a nuove chiavi

5.6.1 Root CA

Nessuna stipula.

5.6.2 CA subordinata

Almeno 2 anni prima della scadenza della chiave di certificazione corrente (CA subordinata), una nuova coppia di chiavi verrà generata e il corrispondente certificato sarà reso disponibile ai Titolari e alle Relying Party come

descritto nel paragrafo 6.1.4. Da quel momento in poi, i certificati dei Titolari e le relative CRL saranno firmati con la nuova chiave di CA.

5.7 Compromissione e disaster recovery

5.7.1 Procedure di gestione degli incidenti e delle compromissioni

Il Sistema aziendale per la Gestione della Sicurezza delle Informazioni (SGSI) di Actalis, conforme alla norma ISO/IEC 27001, prevede anche procedure di gestione degli incidenti e delle compromissioni. La gestione di un incidente di sicurezza delle informazioni è gestita tramite una procedura in più fasi coordinate da un comitato interno (Comitato per la Sicurezza e la Gestione delle Crisi, in seguito "Comitato") composto da figure di varia responsabilità e da membri della Direzione. Le fasi in cui si articola il processo sono descritte di seguito:

- Rilevazione: fase in cui qualsiasi persona (dipendente, collaboratore o comunque parte interessata) che rilevi un possibile incidente lo comunica al Comitato. Il Comitato si assicura che la segnalazione sia il più dettagliata possibile e che chi ha riscontrato il problema non compia alcuna azione in autonomia.
- Identificazione e analisi: il Comitato prende in carico la segnalazione e valuta se effettivamente sia un incidente di sicurezza. In caso positivo valuta la gravità e procede con le fasi successive. In caso negativo si limita alla chiusura dell'incidente.
- Contenimento: in questa fase si provvede per quanto possibile a contenere gli effetti dannosi provocati dall'incidente al fine di evitare che questi si propaghino ad altri ambiti dell'organizzazione.
- Raccolta evidenze: fase in cui si provvede a cercare e raccogliere le evidenze al fine di allegarle alla documentazione dell'incidente in caso di possibili conseguenze legali o per necessità di procedere con indagini più approfondite. Tutte le evidenze vengono raccolte seguendo delle linee guida il cui scopo è di garantire una raccolta corretta e attendibile.
- Rimozione e Ripristino: fase in cui si provvede a rimuovere la causa del danno e a riattivare, mediante le procedure di ripristino, i sistemi coinvolti dall'incidente, permettendo ai sistemi ed agli utenti di tornare ad operare.
- Chiusura Incidente e Notifica: terminata la fase di ripristino l'incidente si ritiene chiuso. In questa fa-se si notifica la chiusura ai vari responsabili coinvolti.

La gestione dei disastri è regolata dal Business Continuity Plan (BCP) di Actalis che copre tutti gli aspetti elencati nelil paragrafo 5.7.1 del [BR]. Vedere anche il paragrafo 5.1.

5.7.2 Corruzione o perdita degli elaboratori, del software e/o dei dati

Actalis implementa un piano di Business Continuity per il servizio di CA al fine di garantire che anche un caso di corruzione o perdita di uno o più elaboratori non possa arrecare alcun disservizio alla piattaforma di CA. In particolare, tutti i componenti critici del sistema sono ridondati sia localmente nel singolo data center che tra i due data center IT1 e IT2. Actalis inoltre implementa degli appositi piani di backup a garanzia che non ci sia perdita di software e/o dati.

5.7.3 Procedure nel caso di compromissione della chiave della CA

La chiave privata della CA è la singola più critica risorsa della CA; in quanto tale, è protetta da una serie di misure di sicurezza a più livelli, come altre risorse critiche della CA. In caso di compromissione (perdita di riservatezza) della chiave della CA, dopo la valutazione dell'incidente, Actalis eseguirà il seguente piano (non necessariamente in questo ordine):

- notifica all'organismo nazionale di supervisione (AgID);
- notifica all'organismo di valutazione della conformità (CAB);
- pubblicazione di una nota informativa ben visibile sul sito web della CA;
- notifica ai fornitori di software applicativo con i quali Actalis ha stipulato un accordo per la distribuzione di certificati di Root CA;
- notifica alle Terze Parti Delegate (DTP), per quanto possibile, e altre parti interessate;
- revoca di tutti i certificati emessi con la chiave compromessa.

Infine, salvo nel caso di cessazione della CA, verrà generata una nuova coppia di chiavi di CA e la nuova chiave pubblica di CA verrà disseminata come descritto nel paragrafo 6.1.4.

5.7.4 Continuità operativa a fronte di un disastro

La PKI di Actalis è replicata su due strutture geograficamente distanti (vedere il paragrafo 5.1), ognuna delle quali consente l'erogazione dei servizi di CA in modo indipendente dall'altra. Nel caso di disastro che renda inutilizzabile una delle strutture, i servizi CA di Actalis saranno trasferiti all'altra. Vedere anche il paragrafo 5.7.1.

5.8 Cessazione della CA o delle RA

Di seguito si descrivono le attività che saranno svolte qualora Actalis decida, per qualsiasi ragione, di cessare il proprio servizio di certificazione.

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 CA (e di altri servizi che includono i servizi di CA), nonché all'organismo di supervisione (AgID), all'organismo di verifica della conformità (CAB) e ad altri soggetti con i quali la CA ha stipulato accordi in merito;
- con preavviso minimo di 60 giorni, sarà pubblicata in modo evidente una nota informativa sul sito web della CA, al fine di rendere disponibile l'informazione anche alle Relying Parties;
- con preavviso minimo di 60 giorni, la CA invierà una comunicazione a tutti gli eventuali subappaltatori e Terze Parti Delegate (RA), informandoli che alla scadenza del termine non saranno più autorizzati ad eseguire attività collegate al servizio di emissione dei certificati;
- la responsabilità della conservazione delle evidenze (richieste di certificati, giornale di controllo, ecc.) sarà trasferita ad un altro soggetto affidabile che ne possa garantire la conservazione per un tempo adeguato. Sarà inoltre trasferita a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della CA cessata;
- sarà pianificata la distruzione delle chiavi private di certificazione nonché del materiale crittografico annesso che ne consente il ripristino.

Alla data di cessazione:

- saranno distrutte (mediante cancellazione logica) le chiavi private di certificazione nonché il materiale annesso (se presente) che ne consente il ripristino, verbalizzando l'operazione.

6 Misure di sicurezza tecnica

6.1 Generazione e installazione delle chiavi

6.1.1 Generazione della coppia di chiavi

6.1.1.1 Generazione chiavi della CA

La generazione di tutte le coppie di chiavi CA (Root CA e CA subordinate) avviene in un ambiente fisicamente protetto, seguendo una procedura documentata che richiede l'intervento congiunto di due persone diverse ("dual control") che ricoprono ruoli di fiducia. Tutte le coppie di chiavi CA sono generate all'interno di HSM (Hardware Security Modules) che soddisfano i requisiti del paragrafo 6.2.1. L'esecuzione della procedura avviene in presenza del Responsabile delle Ispezioni Interne (Internal Auditor) ed è tracciata in un verbale conservato dal Responsabile della Sicurezza della CA (Security Officer).

6.1.1.2 Generazione chiavi della RA

Nessuna stipula.

6.1.1.3 Generazione chiavi del Titolare

La CA non genera le coppie di chiavi dei Titolari.

La CA rigetterà la richiesta di certificato per una chiave pubblica che non soddisfa i requisiti indicati nei paragrafi 6.1.5 e 6.1.6 o se si tratta di una chiave notoriamente debole (come ad esempio una "Debian Weak Key", vedere http://wiki.debian.org/SSLkeys).

6.1.2 Consegna della chiave privata al titolare

Non applicabile.

6.1.3 Consegna della chiave pubblica alla CA

Il Richiedente deve fornire la propria chiave pubblica alla CA sotto forma di Certificate Signing Request (CSR) conforme allo standard PKCS#10 [RFC2314].

6.1.4 Distribuzione della chiave pubblica della CA

Le chiavi pubbliche della Root CA sono distribuite almeno con due modalità:

- mediante pubblicazione nel repository (sotto forma di certificati auto-firmati);
- mediante inclusione negli elenchi delle Root CA affidabili ("root stores") gestiti dai principali produttori di sistemi operativi e browser (secondo gli accordi in essere tra Actalis e tali soggetti);
- attraverso la Trust-service Status List (TSL) pubblicata sul sito dell'AgID.

La chiave pubblica della CA subordinata (ossia CA emittente) viene fornita ai Titolari, sotto forma di certificato emesso dalla Root CA, insieme al certificato del Titolare, ed è inoltre pubblicata nel repository.

6.1.5 Lunghezza delle chiavi

Le Root CA devono utilizzare una coppia di chiavi RSA con una dimensione del modulo di 4096 bit.

Le CA subordinate (ossia le CA emittenti) devono utilizzare una coppia di chiavi RSA con una dimensione del modulo di almeno 2048 bit.

Le chiavi dei Titolari devono essere normalmente chiavi RSA con una dimensione del modulo di 2048 bit.

Alla data di revisione di questo documento, Actalis non si impegna a certificare chiavi di tipo ECC (Elliptic Curves Cryptography), ma potrebbe farlo su richiesta. In tal caso, la dimensione minima della chiave è (NIST) P-256.

6.1.6 Generazione dei parametri e qualità delle chiavi

La CA verifica che le chiavi pubbliche soddisfino i requisiti indicati nel paragrafo 6.1.6 dei [BR].

6.1.7 Key Usage (estensione X.509 v3)

Le chiavi private della Root CA principale non possono essere utilizzate per firmare certificati eccetto nei casi elencati al paragrafo 6.1.7 della [BR].

Vedi anche il capitolo 7.

6.2 Protezione della chiave privata e sicurezza dei moduli crittografici

6.2.1 Requisiti di sicurezza dei moduli crittografici

Gli HSM (Hardware Security Module) usati dalla Root CA e dalle CA subordinate (CA emittenti) sono dotati di certificazione di sicurezza secondo la norma FIPS PUB 140-2 a livello 3 e/o di certificazione Common Criteria (ISO 15408) a livello EAL 4 o superiore.

6.2.2 Controllo multi-persona (N di M) della chiave privata

Vedere il paragrafo 5.2.2.

6.2.3 Deposito in garanzia della chiave privata

Actalis non deposita le proprie chiavi private di CA in custodia presso terzi (key escrow), né fornisce un tale servizio per le chiavi dei titolari.

6.2.4 Backup della chiave privata

Allo scopo di garantire la continuità del servizio, Actalis esegue e conserva copie di backup delle proprie chiavi di CA su supporti rimovibili, in forma cifrata. La copia di backup viene conservata in luogo sicuro e distinto da quello ove si trova la copia operativa. Le operazioni di backup e ripristino delle chiavi di CA richiedono l'intervento congiunto di almeno due persone diverse ("dual control").

6.2.5 Archiviazione della chiave privata

Nessuna stipula oltre a quanto stabilito nei [BR].

6.2.6 Trasferimento della chiave privata dal/al modulo crittografico

Quando le chiavi private CA vengono trasferite tra HSM (ad esempio a scopo di ridondanza o di backup), sono cifrate prima di lasciare il HSM di provenienza e decifrate solo all'interno del HSM di destinazione. Le chiavi private CA non esistono mai "in chiaro" all'esterno del HSM. Actalis non genera chiavi per CA subordinate esterne.

6.2.7 Memorizzazione della chiave privata sul modulo crittografico

Le chiavi private di CA sono memorizzate su HSM che soddisfano i requisiti indicati nel paragrafo 6.2.1.

6.2.8 Modalità di attivazione della chiave privata

Le chiavi private CA sono attivate solo da persone autorizzate, utilizzando i meccanismi forniti dal produttore di HSM. I dati e dispositivi di attivazione sono protetti dalla perdita e dalla divulgazione a persone non autorizzate.

I Titolari sono responsabili della protezione delle proprie chiavi private. I Titolari sono tenuti ad utilizzare una password sicura o un metodo di autenticazione equivalente per impedire l'accesso o l'uso non autorizzato delle proprie chiavi private.

6.2.9 Modalità di disattivazione della chiave privata

Le chiavi private di CA sono disattivate solo da persone autorizzate, usando i meccanismi forniti dal produttore di HSM.

6.2.10 Modalità per la distruzione della chiave privata

Le chiavi private CA sono distrutte quando non sono più necessarie. Le chiavi CA sono distrutte solo da persone autorizzate in ruoli di fiducia, utilizzando i meccanismi forniti dal produttore di HSM.

I Titolari devono distruggere in modo sicuro le proprie chiavi private quando non sono più necessarie (ad es. quando i corrispondenti certificati scadono o vengono revocati) con metodi appropriati a seconda del tipo di supporto in cui sono memorizzate le chiavi private (ad esempio supporti di memorizzazione o HSM).

6.2.11 Classificazione dei moduli crittografici

Vedere il paragrafo 6.2.1.

6.3 Altri aspetti della gestione delle chiavi

6.3.1 Archiviazione della chiave pubblica

Vedere il paragrafo 5.5.

6.3.2 Durata operativa dei certificati e delle chiavi

I certificati e le chiavi private hanno una durata operativa *massima* in accordo con la seguente tabella:

Tipo	**Uso chiave privata**	**Validità del certificato**
Root CA	15 anni	20 anni
Subordinate CA	12 anni	15 anni
Subscriber – OV SSL Server	Nessuna stipula	Certificati emessi prima del 1 Marzo 2018: 39 mesi Certificati emessi dal 1 Marzo 2018: 825 giorni
Subscriber - EV SSL Server	Nessuna stipula	27 mesi
Subscriber – Code Signing	Nessuna stipula	3 anni

Vedere anche il paragrafo 7.1.

6.4 Dati di attivazione

Con dati di attivazione si intendono i dati necessari per attivare le chiavi private all'interno degli HSM. Si tratta ad esempio di PIN, passphrase e frammenti di chiavi private utilizzati in uno schema split-knowledge, ecc.

6.4.1 Generazione dei dati di attivazione

La generazione dei dati di attivazione delle chiavi avviene nel rispetto delle best practice di sicurezza nonché (ove applicabile) delle procedure raccomandate dai produttori degli HSM.

6.4.2 Protezione dei dati di attivazione

6.4.2.1 Chiavi della CA

I dati di attivazione sono protetti da misure di sicurezza fisica (ad es. archiviazione su supporti rimovibili), logica (ad esempio cifratura) e/o procedurale (ad esempio l'assegnazione a persone in ruoli di fiducia), nel rispetto della policy di sicurezza aziendale e del requisito del “dual control” di cui al paragrafo 6.1.1.1

6.4.2.2 Chiavi dei Titolari

I dati di attivazione della chiave privata del Titolare sono protetti, a cura del titolare stesso, in modo tale da prevenire la loro rivelazione a terzi non autorizzati. Per ulteriori importanti precisazioni a questo riguardo si rimanda al paragrafo 9.6.3.

6.4.3 Altri aspetti relativi ai dati di attivazione

Le chiavi di Root CA sono normalmente mantenute in uno stato non operativo, tranne quando necessario per l'emissione o la revoca di certificati CA subordinata o per la generazione di CRL.

6.5 Sicurezza degli elaboratori

6.5.1 Requisiti di sicurezza degli elaboratori

Gli elaboratori utilizzati nell’ambito dei servizi di CA utilizzano sistemi operativi di comprovata qualità e affidabilità, configurati in modo tale da impedire l’uso non autorizzato e/o con modalità non previste delle risorse (dati, applicazioni, canali di comunicazione, ecc.).

Ove possibile e laddove tale funzionalità non sia già insita nel sistema operativo, vengono installati sistemi anti-malware al fine di mitigare il rischio di “infezioni” ed attacchi di sicurezza. Inoltre, per la stessa ragione vengono installate le “patch” di sicurezza raccomandate di volta in volta dai fornitori.

Gli elaboratori sono sottoposti ad una procedura di “hardening” finalizzata alla rimozione o disabilitazione delle funzionalità non richieste, in modo specifico su ciascun elaboratore secondo il ruolo che esso ricopre nell’ambito dell’infrastruttura.

L'accesso privilegiato agli elaboratori (ossia come “Amministratore” del sistema) è limitato al personale che ne ha effettivamente necessità e che sia stato nominato “Amministratore di Sistema” nel rispetto della normativa vigente.

6.5.2 Rating di sicurezza degli elaboratori

Nessuna stipula.

6.6 Sicurezza del ciclo di vita

6.6.1 Sicurezza nello sviluppo dei sistemi

Lo sviluppo dei sistemi software a supporto dei servizi fiduciari erogati da Actalis, incluso il servizio di CA, svolto da Actalis o per conto di Actalis, avviene nel rispetto del Sistema di Gestione Qualità (SGQ) aziendale, conforme alla norma UNI EN ISO 9001:2015.

6.6.2 Sistema di gestione della sicurezza

Actalis dispone di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conforme allo standard ISO/-IEC 27001, che copre tutte le aree aziendali, comprese quelle coinvolte nello sviluppo e fornitura del servizio CA. Tra le altre disposizioni del SGSI, tutte i sistemi e i software utilizzati per i servizi fiduciari di Actalis (inclusi i servizi CA) sono installati e aggiornati secondo un processo documentato di gestione delle modifiche (change management).

6.6.3 Gestione del ciclo di vita

Nessuna stipula.

6.7 Sicurezza di rete

L'accesso agli host on-line della CA è protetto da firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni. Prima dei firewall, una batteria di router che implementano opportune ACL (Access Control List) costituisce un'ulteriore barriera di protezione. Sui server del servizio di certificazione, tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quegli agenti che supportano i protocolli e le funzioni necessarie per il funzionamento del servizio.

Per irrobustire il filtraggio delle comunicazioni tutto il sistema di certificazione è suddiviso in un'area esterna, una interna ed una DMZ. I sistemi più critici sono installati nella zona interna e non possono essere direttamente accessibili dalla zona esterna.

Actalis svolge almeno annualmente un assessment di sicurezza per verificare l'eventuale presenza di vulnerabilità di rete, avvalendosi di specialisti indipendenti.

6.8 Riferimento temporale

Il riferimento temporale usato da Actalis, col quale vengono mantenuti sincronizzati i sistemi di elaborazione della CA, è ottenuto da un dispositivo di alta precisione che garantisce una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC.

7 Profilo dei certificati, CRL e OCSP

7.1 Profilo del certificato

I certificati emessi secondo questo CPS sono conformi alla specifica pubblica [RFC 5280], basata sullo standard ITU-T X.509 v3 (ovvero ISO/IEC 9594-8:2005), nonché alle norme europee ETSI EN 319 411 ed ETSI EN 319 412 (nelle parti applicabili).

Salvo diversa richiesta degli interessati, i certificati qualificati secondo il regolamento eIDAS sono inoltre emessi secondo l'applicazione delle raccomandazioni emanate dall'Agenzia e volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete nel contesto italiano (Determinazione AgID n.121/2019, e successive modificazioni ed integrazioni). La piena applicazione delle raccomandazioni oggetto del provvedimento è normalmente dichiarata attraverso la codifica, nella estensione CertificatePolicies (OID 2.5.29.32), di un elemento aggiuntivo PolicyIdentifier con valore **agIDcert** (OID 1.3.76.16.6), salvo dove tale indicazione fosse ridondante o inapplicabile in considerazione dei requisiti del particolare contesto applicativo.

7.1.1 Numeri di versione

Tutti i certificati sono di tipo X.509 v3.

7.1.2 Contenuto ed estensioni dei certificati

Tutti i certificati sono conformi alla specifica pubblica [RFC 5280] nonché ai Baseline Requirements [BR] o alle EV Guidelines [EVGL] del CAB Forum, secondo la classe del certificato.

7.1.2.1 Certificati della Root CA

Il certificato della Root CA ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	1
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	dal 22 settembre 2011 al 22 settembre 2030
Subject	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 4096 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<assente>
SubjectKeyIdentifier (SKI)	52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<assente>
CertificatePolicies	<assente>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<assente>
CRLDistributionPoints (CDP)	<assente>

7.1.2.2 Certificati di CA subordinata

7.1.2.2.1 Sub CA per certificati di classe DV

I certificati delle CA subordinate hanno il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Domain Validation Server CA G***N*** O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<può essere omesso nelle SubCAs create fino al 31 dic. 2018> <include serverAuth + clientAuth a partire dal 1 gennaio 2019>
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.1.2.2.2 Sub CA per certificati di classe OV

I certificati delle CA subordinate hanno il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Authentication CA G***N*** O = Actalis S.p.A./03358520967 L = Milano C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<può essere omesso nelle SubCAs create fino al 31 dic. 2018> <include serverAuth + clientAuth a partire dal 1 gennaio 2019>
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

Campo	Valore
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Organization Validated Server CA G***N*** O = Actalis S.p.A./03358520967 L = Ponte San Pietro ST= Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<può essere omesso nelle SubCAs create fino al 31 dic. 2018> <include serverAuth + clientAuth a partire dal 1 gennaio 2019>
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.1.2.2.3 Sub CA per certificati di classe EV

I certificati delle CA subordinate hanno il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Extended Validation Server CA G***N*** O = Actalis S.p.A./03358520967 L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<può essere omesso nelle SubCAs create fino al 31 dic. 2018> <include serverAuth + clientAuth a partire dal 1 gennaio 2019>
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.1.2.2.4 Sub CA per certificati di Code Signing

I certificati delle CA subordinate hanno il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Code Signing CA G***N*** O = Actalis S.p.A./03358520967 L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	codeSigning (1.3.6.1.5.5.7.3.3) OCSPSigning (1.3.6.1.5.5.7.3.9)
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.1.2.3 Certificati dei Titolari

7.1.2.3.1 SSL Server DV

Il certificato per SSL Server DV viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = <uno dei FQDN contenuti nella estensione SAN>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**22**.1 PolicyOID = 2.23.140.1.2.1 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<contiene uno o più FQDN, in conformità a [BR]>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

Nota: nel caso di certificato richiesto per un FQDN del tipo www.<dominio>, l'estensione SAN contiene anche <dominio> (senza la label "www") a condizione che la Domain Control Validation venga svolta sul <dominio> e non sul www.<dominio>. Esempio: nel caso di un certificato emesso per *www.example.com* l'estensione SAN può contenere due voci:, *www.example.com* ed *example.com*.

7.1.2.3.2 SSL Server DV Wildcard

Il certificato per SSL Server Wildcard DV viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = < FQDN wildcard, contenuto anche nella estensione SAN >
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**23**.1 PolicyOID = 2.23.140.1.2.1 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<Lo stesso FQDN wildcard contenuto nel campo Subject.CN più eventuali altri FQDN>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

Nota: l'estensione SAN contiene anche il nome di dominio ottenuto rimuovendo l'asterisco ("*") dal FQDN wildcard. Esempio: nel caso di un certificato emesso per *.example.com l'estensione SAN contiene, oltre a **.example.com*, anche *example.com*.

7.1.2.3.3 SSL Server OV

Il certificato per SSL Server OV viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	C = <codice a due lettere del paese dove ha sede il Titolare> ST = <provincia o stato dove ha sede il Titolare> L = <località dove ha sede il Titolare> O = <nome ufficiale o DBA del Titolare> OU = <opzionale> CN = <uno dei FQDN contenuti nella estensione SAN>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**20**.1 PolicyOID = 2.23.140.1.2.2 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<contiene uno o più FQDN, in conformità a [BR]>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

Nota: nel caso di certificato richiesto per un FQDN del tipo www.<dominio>, l'estensione SAN contiene anche <dominio> (senza la label "www") a condizione che la Domain Control Validation venga svolta sul <dominio> e non sul www.<dominio>. Esempio: nel caso di un certificato emesso per *www.example.com* l'estensione SAN può contenere due voci:, *www.example.com* ed *example.com*.

7.1.2.3.4 SSL Server OV Wildcard

Il certificato per SSL Server OV Wildcard viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	C = <codice a due lettere del paese dove ha sede il Titolare> ST = <provincia o stato dove ha sede il Titolare> L = <località dove ha sede il Titolare> O = <nome ufficiale o DBA del Titolare > OU = <opzionale> CN = <FQDN wildcard, contenuto anche nella estensione SAN>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**19**.1 PolicyOID = 2.23.140.1.2.2 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<Lo stesso FQDN wildcard contenuto nel campo Subject.CN più eventuali altri FQDN>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

Nota: l'estensione SAN contiene anche il nome di dominio ottenuto rimuovendo l'asterisco ("*") dal FQDN wildcard. Esempio: nel caso di un certificato emesso per *.example.com l'estensione SAN contiene, oltre a **.example.com*, anche *example.com*.

7.1.2.3.5 SSL Server EV

Il certificato per SSL Server EV viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	C = <codice a due lettere del paese dove ha sede il Titolare> ST = <provincia o stato dove ha sede il Titolare > L = <località dove ha sede il Titolare> O = <nome ufficiale o DBA del Titolare> OU = <opzionale> CN = <uno dei FQDN contenuti nella estensione SAN > serialNumber = <numero di registrazione del Titolare presso la camera di commercio o un codice equivalente> businessCategory = <tipo di organizzazione>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**17**.1 PolicyOID = 2.23.140.1.1 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<contiene uno o più FQDN, in conformità a [EVGL]>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

Nota: nel caso di certificato richiesto per un FQDN del tipo www.<dominio>, l'estensione SAN contiene anche <dominio> (senza la label "www") a condizione che la Domain Control Validation venga svolta sul <dominio> e non sul www.<dominio>. Esempio: nel caso di un certificato emesso per *www.example.com* l'estensione SAN può contenere due voci:, *www.example.com* ed *example.com*.

7.1.2.3.6 Qualified Website Authentication Certificate

Il certificato SSL Server *qualificato* ("Qualified Website Authentication Certificate"), variante del certificato SSL Server EV, viene emesso col seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	C = <codice a due lettere del paese dove ha sede il Titolare> ST = <provincia o stato dove ha sede il Titolare > L = <località dove ha sede il Titolare> O = <nome ufficiale o DBA del Titolare> OU = <opzionale> CN = <uno dei FQDN contenuti nella estensione SAN > serialNumber = <numero di registrazione del Titolare presso la camera di commercio o un codice equivalente> businessCategory = <tipo di organizzazione>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: digitalSignature, keyEncipherment (solo per chiavi RSA)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.**17**.1 PolicyOID = 2.23.140.1.1 PolicyOID = 0.4.0. 194112.1.4 (QCP-w) CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<contiene uno o più FQDN, in conformità a [EVGL]>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>
QCStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

7.1.2.3.7 Code Signing

Il certificato per Code Signing viene emesso col seguente profilo:

Campo	Valore
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN della CA che ha emesso il certificato>
Validity	<In accordo col paragrafo 6.3.2>
Subject	C = <codice a due lettere del paese dove ha sede il Titolare> ST = <provincia o stato dove ha sede il Titolare> L = <località dove ha sede il Titolare > O = <nome ufficiale o DBA del Titolare> OU = <opzionale> CN = <valore proposto dal Titolare >
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit oppure ECC P256/P384>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<assente>
AuthorityKeyIdentifier (AKI)	<valore della estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	digitalSignature
ExtendedKeyUsage (EKU)	codeSigning (1.3.6.1.5.5.7.3.3)
CertificatePolicies	PolicyOID = 1.3.159.1.**21**.1 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)	<indirizzo di e-mail del titolare>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP> <indirizzo HTTP del certificato della CA emittente>
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> <indirizzo LDAP per accedere alla CRL>

7.1.2.4 Tutti i certificati

La CA può includere nel certificato ulteriori informazioni (ad esempio estensioni aggiuntive e/o valori aggiuntivi nelle estensioni) a condizione che tali informazioni aggiuntive:

- rispettano pienamente sia la specifica [RFC 5280] che i Requisiti e le Linee Guida del CAB Forum; e
- non inducano in errore le Relying Party in merito alle informazioni nel certificato verificate dalla CA.

7.1.3 Identificatori degli algoritmi

I certificati sono normalmente firmati usando uno dei seguenti algoritmi:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11

Le risposte OSCP sono firmate usando uno dei seguenti algoritmi:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.4 Forme dei nomi

7.1.4.1 Informazioni sull'Emittente

Il contenuto del campo Issuer DN del certificato deve corrispondere al DN della CA emittente per consentire il concatenamento dei nomi come specificato in [RFC 5280], paragrafo 4.1.2.4.

7.1.4.2 Informazioni sul Titolare

Con il rilascio del certificato, la CA dichiara di aver seguito le procedure descritte in questo CPS per verificare che, alla data di rilascio del certificato, tutte le informazioni relative al Titolare fossero accurate. La CA non può includere nel certificato un nome di dominio o un indirizzo IP se non nel rispetto di quanto specificato rispettivamente nei paragrafi 3.2.2.4 e 3.2.2.5.

7.1.4.2.1 Estensione Subject Alternative Names

Per tutti i certificati **SSL Server**, si applica la seguente regola:

- l'estensione **SubjectAlternativeNames** (**SAN**) deve contenere almeno un elemento. Ciascuno degli elementi di questa estensione deve essere un indirizzo IP o un nome di dominio completo (FQDN) di proprietà di, o sotto il controllo del Titolare. Non sono consentiti nomi di server interni o indirizzi IP riservati. Vedere anche il paragrafo 3.1.1.

NB: il carattere *underscore* ("_") non è ammesso negli FQDN.

7.1.4.2.2 Campi del Subject Distinguished Name

Per i certificati **DV SSL server**, si applicano le seguenti regole:

- L'attributo **commonName** (OID 2.5.4.3) del Subject DN deve contenere un singolo indirizzo IP o FQDN (Fully Qualified Domain Name) tra quelli inclusi nell'estensione SAN (vedere il paragrafo precedente).
- Nessun altro attributo del Subject DN è presente.

Per i certificati **OV SSL Server e Code Signing**, si applicano le seguenti regole:

- L'attributo **commonName** (OID 2.5.4.3) del Subject DN:
  - in un certificato Server SSL, deve contenere un singolo indirizzo IP o FQDN (Fully Qualified Domain Name) tra quelli contenuti nell'estensione SAN (vedere il paragrafo precedente);
  - in un certificato di Code Signing, può contenere qualsiasi stringa scelta dal Richiedente a condizione che non sia fuorviante rispetto all'identità del Titolare o allo scopo del certificato. In ogni caso, non può essere un nome di dominio o un indirizzo IP.
- L'attributo **organizationName** (OID 2.5.4.10) del Subject DN deve contenere il nome o DBA (Doing Business As) del Titolare. Per un certificato Server SSL, deve essere l'entità che possiede o controlla tutti i nomi di dominio completi (FQDN) e/o gli indirizzi IP inclusi nel certificato.
- L'attributo facoltativo **organizationalUnitName** (OID 2.5.4.11) del Subject DN, se presente, può contenere qualsiasi stringa a discrezione del Titolare, a condizione che non sia fuorviante rispetto all'identità del Titolare.

- L'attributo **localityName** (OID 2.5.4.7) del Subject DN deve contenere il nome della località (ad es. Città) ove si trova la sede principale del Titolare.
- L'attributo **stateOrProvinceName** (OID 2.5.4.8) del Subject DN deve contenere il nome della provincia (per organizzazioni italiane) o la regione/stato (per organizzazioni estere) in cui si trova la sede principale del Titolare.
- L'attributo **countryName** (OID 2.5.4.6) del Subject DN deve contenere il codice a due lettere ISO 3166 (ad esempio "IT") del paese in cui si trova la sede principale del Titolare.

Per i certificati **EV SSL Server**, si applicano le seguenti regole aggiuntive:

- L'attributo **businessCategory** (OID 2.5.4.15) del Subject DN deve contenere il tipo di organizzazione Titolare ("Organizzazione privata" o "Entità governativa").
- L'attributo **serialNumber** (OID 2.5.4.5) del Subject DN deve contenere il numero di partita IVA o altro numero di registrazione ufficiale del Titolare.
- L'attributo **jurisdictionOfIncorporationCountryName** (OID 1.3.6.1.4.1.311.60.2.1.3) del Subject DN deve contenere il codice ISO 3166 a due lettere (es. “IT”) del paese in cui l'organizzazione Titolare è stata registrata o costituita.
- L'attributo **streetAddress** (OID 2.5.4.9) del Subject DN deve contenere l'indirizzo completo (ad esempio il nome della via e il numero civico) della sede principale del Titolare.

7.1.5 Vincoli sui nomi

Actalis può emettere, previo accordo contrattuale, certificati di CA subordinata per soggetti esterni, firmati da una Root CA di Actalis. In tal caso, il certificato di CA subordinata sarà tecnicamente vincolato in conformità al paragrafo 7.1.5 dei [BR].

7.1.6 Identificatori delle policy

Vedere il paragrafo 1.4.

7.1.7 Uso dell’estensione PolicyConstraints

Non applicabile.

7.1.8 Sintassi e semantica dei qualificatori delle policy

Vedere il paragrafo 7.1.

7.1.9 Regole di elaborazione dell’estensione CertificatePolicies

Non applicabile.

7.2 Profilo della CRL

Le CRL sono conformi alla specifica pubblica [RFC 5280].

La versione delle CRL è v2 (1).

Oltre ai dati obbligatori, le CRL contengono:

- il campo *nextUpdate* (data della prossima emissione della CRL)
- l’estensione *cRLNumber* (numero progressivo della CRL)

La CRL è firmata con algoritmo sha256WithRSAEncryption (1.2.840.113549.1.1.11).

Inoltre, in corrispondenza di ogni voce della CRL è presente l'estensione *reasonCode* a indicare la motivazione della sospensione o revoca.

7.3 Profilo OCSP

Il servizio OCSP erogato da Actalis è conforme alla specifica pubblica [RFC6960].

Le risposte OCSP non sono firmate direttamente con la chiave privata della CA emittente, bensì con una chiave specifica del risponditore OCSP. Pertanto, il certificato del risponditore OCSP contiene il key purpose **ocspSigning** (OID 1.3.6.1.5.5.7.3.9) nell'estensione ExtendedKeyUsage. Inoltre, il certificato del risponditore OCSP contiene l'estensione **id-pkix-ocsp-nocheck** (OID 1.3.6.1.5.5.7.48.1.5).

La risposta OCSP è conforme al profilo "pkix-ocsp-basic" (OID 1.3.6.1.5.5.7.48.1.1).

7.3.1 Numeri di versione

La versione della risposta OCSP è v1 (0).

7.3.2 Estensioni OCSP

La risposta OCSP contiene l'estensione Nonce (OID 1.3.6.1.5.5.7.48.1.2).

8 Verifiche di conformità

Actalis deve rilasciare i certificati e gestire la propria PKI in conformità con i requisiti [BR] e linee guida [EVGL] del CAB Forum e con la normativa vigente applicabile.

8.1 Frequenza e circostanze dalle verifiche

La conformità dei servizi CA di Actalis al presente CPS, al Regolamento (UE) n.910/2014 ("eIDAS"), agli standard ETSI ed ai requisiti [BR] ed [EVGL] applicabili viene verificata su base annuale da un Organismo di Valutazione accreditato (Conformity Assessment Body, CAB).

Inoltre, sempre su base almeno annuale, viene svolta un'attività di auditing interno sui servizi di CA che tiene conto anche di aspetti inerenti la sicurezza delle informazioni, le norme applicabili sulla protezione dei dati e le politiche e procedure interne.

8.2 Identità e qualificazione degli ispettori

Le verifiche di conformità (audit) sulla CA sono svolte da un Organismo di Valutazione (CAB) accreditato in conformità al Regolamento (CE) n. 765/2008, attraverso personale qualificato e competente sul tema delle valutazioni di conformità, secondo la norma ETSI EN 319 403, dei Prestatori di Servizi Fiduciari (Trust Service Provider) e dei relativi servizi fiduciari forniti ai sensi del Regolamento eIDAS. Eventuali audit di seconda parte vengono eseguiti sempre da organismi accreditati in conformità al Regolamento (CE) n. 765/2008.

8.3 Relazioni tra la CA e gli auditor

Gli Organismi di Valutazione (CAB) che svolgono audit sul servizio di CA, ed eventualmente sulle RA esterne che collaborano con la CA, non hanno alcuna relazione con Actalis.

L'auditor interno non appartiene alla struttura che si occupa delle attività di CA.

8.4 Argomenti coperti dalle verifiche

Gli audit esterni devono valutare, sulla base delle norme ETSI EN 319 411-1 ed ETSI EN 319 411-2, la conformità con i [BR] e le [EVGL] e la corretta operatività della CA come descritta in questo CPS, incluse le eventuali Terze Parti Delegate (DTP) che non sono "Enterprise RA", ad eccezione delle eventuali CA subordinate "technically constrained" (cfr. §1.3.1).

Le DTP non conformi non possono continuare a svolgere le funzioni a loro delegate fino a quando le non conformità non siano completamente sanate.

8.5 Azioni conseguenti alle non-conformità

Le azioni conseguenti alle eventuali non-conformità riscontrate durante gli audit (mancato soddisfacimento dei requisiti definiti nei regolamenti, standard, procedure applicabili) dipendono dalla natura e dalla severità della non-conformità rilevata, dalle regole di gestione delle non-conformità definite dall'Organismo di Valutazione (CAB) e/o dalle procedure interne di gestione delle non-conformità.

In linea generale, se da una verifica (audit) risultasse una non conformità sostanziale, Actalis svilupperà un piano per rimediare a tale non conformità il più rapidamente possibile. Tale piano potrebbe comportare la modifica delle politiche e/o pratiche di certificazione e/o del software di CA. Il piano sarà presentato alla Direzione di Actalis per l'approvazione, quindi alle eventuali terze parti con cui Actalis sia impegnata a tal riguardo.

8.6 Comunicazione dei risultati delle verifiche

Il risultato dell'audit svolto dal CAB viene comunicato alla Direzione aziendale e ai responsabili della struttura organizzativa preposta all'erogazione del servizio di CA. Il risultato dell'audit viene inoltre comunicato all'Organismo nazionale di Supervisione (AgID) attraverso l'invio del report prodotto dal CAB.

La CA rende pubblico il risultato dell'audit entro tre mesi dalla fine del periodo di audit.

Il risultato dell'audit interno o dell'audit di seconda parte viene comunicato alla Direzione aziendale, ai responsabili della struttura organizzativa preposta all'erogazione del servizio di CA e, ove applicabile, all'entità/organizzazione esterna coinvolta.

8.7 Autovalutazioni (self-audit)

Durante il periodo in cui la CA emette certificati, la CA monitora l'aderenza a questo CPS (e ai documenti collegati, se presenti) e alle specifiche [BR] e [EVGL] e controlla rigorosamente la qualità del servizio, eseguendo autovalutazioni (self-audit) almeno su base trimestrale. Le autovalutazioni sono svolte su un campione casuale di almeno il 3% dei certificati rilasciati nel periodo che inizia immediatamente dopo l'ultima autovalutazione.

9 Condizioni generali del servizio

Le "Condizioni Generali" del servizio sono fornite all'utente come documento separato, da accettare in fase di richiesta, disponibile sul sito web della CA (vedere il paragrafo 2.2).

9.1 Tariffe del servizio

9.1.1 Tariffe per l'emissione o rinnovo del certificato

Le tariffe massime del servizio sono pubblicate sul sito web della CA.

Condizioni diverse possono essere negoziate caso per caso, in base ai volumi richiesti.

Le tariffe del servizio sono soggette a modifiche senza preavviso.

9.1.2 Tariffe per l'accesso ai certificati

Non applicabile.

9.1.3 Tariffe per l'accesso alle informazioni di stato dei certificati

L'accesso ai servizi informativi (CRL, OCSP) sullo stato dei certificati è libero e gratuito.

9.1.4 Tariffe per altri servizi

Nessuna stipula.

9.1.5 Politica per il rimborso

Si rimanda alle Condizioni Generali di fornitura pubblicate sul sito web della CA.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Actalis ha stipulato un'apposita assicurazione, con una società assicuratrice di primaria importanza, a copertura dei rischi derivanti dall'erogazione del servizio di certificazione e altri servizi fiduciari. In particolare, l'assicurazione prevede un massimale unico per sinistro e per periodo di assicurazione di EUR 15.000.000 (quindici milioni di Euro). La società assicuratrice ha un rating almeno "A" nella Best's Insurance Guide.

9.2.2 Altri asset

Nessuna stipula.

9.2.3 Garanzia o copertura assicurativa per gli utenti finali

Si rimanda al par. 9.2.1.

9.3 Confidenzialità delle informazioni trattate

9.3.1 Ambito di applicazione delle informazioni confidenziali

Le seguenti informazioni sono considerate e trattate come confidenziali:

- tutte le informazioni fornite alla CA dai Richiedenti, ad eccezione di quelle destinate a essere incluse nei Certificati;
- tutte le comunicazioni tra la CA e i Richiedenti o Titolari;
- i codici riservati forniti al Titolare dalla CA o dalla RA (per es. le credenziali necessarie per accedere al sito web della CA o della RA);
- tutte le informazioni raccolte dalla CA nell'ambito del processo di verifica delle richieste (identificazione e autenticazione);
- i contratti tra la CA e le altre parti, compresi i Titolari, i fornitori di software applicativo, le Terze Parti Delegate (ad esempio i rivenditori e le Autorità di Registrazione), i subappaltatori, ecc.;

- tutte le informazioni private della CA (quali le chiavi private di CA, gli account dei sistemi CA, le password e altri strumenti di autenticazione, i piani di continuità aziendale e disaster recovery, le procedure interne, la documentazione interna dell'infrastruttura, le analisi del rischio, le transazioni finanziarie, ecc.);
- gli audit log (giornali di controllo) dei sistemi CA.

9.3.2 Informazioni considerate non confidenziali

Tutte le informazioni che devono essere pubbliche ai sensi delle norme vigenti (cfr. il paragrafo 9.15) e dei regolamenti applicabili (inclusi i Requisiti e le Linee Guida del CAB Forum), o su richiesta esplicita del Titolare, sono considerate non riservate. In particolare, le seguenti informazioni sono considerate non riservate:

- tutti i certificati emessi nell'ambito del presente CPS;
- tutte le CRL (elenchi dei certificati revocati: vedere il paragrafo 4.10);
- questo CPS e gli altri documenti pubblici di Actalis ivi citati;
- lo stato dei certificati fornito attraverso il servizio OCSP (vedere il paragrafo 4.10);
- tutte le informazioni che il Richiedente ha richiesto alla CA di rendere pubbliche;
- tutte le informazioni ottenibili da fonti di informazione pubbliche;
- qualsiasi informazione che è già di dominio pubblico.

9.3.3 Responsabilità di protezione delle informazioni confidenziali

Actalis garantisce che tutte le informazioni riservate siano adeguatamente protette dall'accesso non autorizzato e dal rischio di perdita a causa di disastri (vedere il paragrafo 5.7).

Tutte le informazioni confidenziali sono trattate dalla CA nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 [DLGS196] e del Regolamento (UE) 2016/679 [GDPR].

9.4 Trattamento e protezione dei dati personali

9.4.1 Programma sulla privacy

Per quanto riguarda la privacy, la CA rispetta le norme vigenti, in particolare il D.lgs. 196/03 [DLGS196] ed il Regolamento (UE) 2016/679 [GDPR]. La protezione dei dati personali rientra nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Actalis, certificato ISO/IEC 27001.

9.4.2 Dati che sono considerati personali

Si rimanda alla definizione di dati personali di cui alle norme vigenti, in particolare il D.lgs. 196/03 [DLGS196].

9.4.3 Dati che non sono considerati personali

Sono considerati dati non personali quelli che non rientrano nella definizione al par. 9.4.2. Si rimanda inoltre al paragrafo 9.3.2.

9.4.4 Responsabilità di protezione dei dati personali

Actalis è il “titolare del trattamento” dei dati personali ai sensi del D.lgs. 196/03 [DLGS196].

9.4.5 Informativa e consenso al trattamento dei dati personali

L'informativa sul trattamento dei dati personali, ai sensi del D.lgs. 196/03 [DLGS196], è pubblicata sul sito web della CA. La richiesta del certificato richiede il consenso, da parte del Richiedente, al trattamento dei propri dati personali da parte della CA, in coerenza con tale informativa.

9.4.6 Divulgazione dei dati a seguito di richiesta dell'autorità giudiziaria

I dati personali del Titolare potranno essere comunicati alle forze di polizia, all'autorità giudiziaria, agli organismi di informazione e sicurezza o ad altri soggetti pubblici, ai sensi del D.lgs. 196/2003 [DLGS196], nel caso in cui ciò sia richiesto per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

9.4.7 Altre circostanze di possibile divulgazione dei dati personali

Non applicabile.

9.5 Diritti di proprietà intellettuale

Il presente CPS è di proprietà di Actalis che si riserva tutti i diritti ad esso relativi.

Il Titolare mantiene tutti gli eventuali diritti sui propri marchi commerciali (brand) e sui propri nomi di dominio.

Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi vigenti.

9.6 Dichiarazioni e garanzie

9.6.1 Dichiarazioni e garanzie della CA

Con l'emissione di un Certificato, la CA rilascia determinate garanzie ai seguenti beneficiari del certificato:

- il Titolare;
- i fornitori di software applicativo (ad esempio i fornitori di taluni web browser e/o sistemi operativi) che hanno stipulato un contratto di distribuzione di certificati di Root con Actalis;
- tutte le Relying Party che ragionevolmente fanno affidamento su un Certificato valido.

In generale, Actalis si impegna a operare, in tutti gli aspetti materiali, in conformità con questo CPS.

Più in particolare, Actalis dichiara e garantisce ai Beneficiari del certificato che:

- [per i certificati SSL Server] al momento dell'emissione, la CA ha seguito le procedure descritte in questo CPS per verificare che il Richiedente avesse il diritto di utilizzare oppure il controllo di fatto dei nomi di dominio e/o indirizzi IP elencati nel campo Subject del Certificato e nell'estensione SubjectAlt-Name (o, solo nel caso dei nomi di dominio, che al Richiedente fosse delegato tale diritto o controllo da parte del soggetto che aveva tale diritto o controllo);
- al momento dell'emissione, la CA ha seguito le procedure descritte in questo CPS per verificare che il Richiedente autorizzasse l'emissione del Certificato e che il Rappresentante del Richiedente fosse autorizzato a richiedere il Certificato per conto del Richiedente;
- al momento dell'emissione, la CA ha seguito le procedure descritte in questo CPS per verificare l'esattezza di tutte le informazioni contenute nel campo Subject del Certificato (ad eccezione dell'attributo organizationalUnitName);

- al momento dell'emissione, la CA ha seguito una procedura per ridurre la probabilità che le informazioni contenute nell'attributo organizationalUnitName del Subject del Certificato risultino fuorvianti;
- se il Certificato contiene informazioni sull'identità del Titolare, la CA ha verificato l'identità del Richiedente in conformità con le procedure descritte in questo CPS;
- nel caso di certificati EV, la CA ha consultato il pertinente ente di registrazione imprese della giurisdizione di costituzione o registrazione del Titolare per accertare che, al momento dalla data di emissione del Certificato, il Titolare indicato nel Certificato esistesse legalmente come organizzazione valida nella relativa giurisdizione di costituzione o registrazione;
- se la CA e il Titolare non sono affiliati, il Titolare e la CA sono controparti di un Accordo di Servizio (Subscriber Agreement) legalmente valido e applicabile che soddisfa i [BR] o le [EVGL] (secondo la classe del Certificato), o, se la CA e il Titolare sono la stessa entità o sono affiliati, il Rappresentante del Richiedente ha accettato le Condizioni di Servizio (Terms of Use);
- la CA mantiene un Repository accessibile al pubblico 24 x 7 con informazioni aggiornate sullo stato (valido o revocato) di tutti i Certificati non scaduti;
- la CA revocherà il certificato per uno dei motivi specificati in questo CPS.

9.6.2 Dichiarazioni e garanzie delle RA

Le RA sono tenute al pieno rispetto del contratto stipulato con la CA, in particolare (ma non solo) alla:

- corretta e sicura I&A (identificazione a autenticazione) dei Richiedenti;
- diligente conservazione di tutte le evidenze raccolte (salvo che non sia a cura della CA, secondo lo specifico contratto stipulato con la RA), per tutto il tempo previsto dal contratto;
- corretto utilizzo degli strumenti e canali trasmissivi che la CA mette a loro disposizione.

9.6.3 Dichiarazioni e garanzie dei Titolari

Prima dell'emissione di un Certificato, la CA deve ottenere l'accettazione di un Accordo di Servizio (Subscriber Agreement) o di Condizioni d'Uso (Terms of Use). Come parte dell'Accordo di Servizio o Condizioni d'Uso, il Richiedente deve assumere gli impegni elencati di seguito.

Il Richiedente dichiara e garantisce di:

- leggere, comprendere ed accettare integralmente questo CPS;
- richiedere il certificato con le modalità previste da questo CPS;
- fornire alla CA, in ogni momento, informazioni esatte, veritiere e complete;
- assicurare la confidenzialità dei codici riservati (es. password) ricevuti dalla CA;
- adottare tutte le misure ragionevoli per evitare la compromissione delle proprie chiavi private;
- installare e utilizzare il certificato solo previa verifica che esso contenga informazioni corrette;
- utilizzare il certificato unicamente con le modalità e per le finalità previste da questo CPS;
- non usare mai, per nessuna ragione, la propria chiave privata per emettere a sua volta certificati;
- nel caso di accertata compromissione di una delle proprie chiavi private, richiedere immediatamente la revoca del corrispondente certificato e cessarne immediatamente l'utilizzo;
- nel caso di compromissione della CA, cessare immediatamente l'utilizzo dei certificati;

- richiedere immediatamente la revoca di un certificato nel caso in cui una o più delle informazioni contenute nel certificato (es. ragione sociale, indirizzo del sito web, ecc.) perdano di validità;
- successivamente all'emissione e fino alla scadenza o revoca del certificato, avvisare prontamente la CA di ogni variazione alle informazioni fornite in fase di richiesta;
- rispondere entro 24 ore alle richieste della CA relative all'eventuale uso improprio del certificato o compromissione della chiave;
- al momento della eventuale revoca dei propri certificati, cessare immediatamente l'uso dei certificati revocati e inoltre…
  - nel caso di certificato per Code Signing: rimuovere prontamente il software firmato dai siti web sui quali esso è pubblicato,
  - nel caso di certificato SSL Server: rimuovere prontamente il certificato dai server sui quali esso è installato;
- cessare ogni utilizzo del certificato dopo la data di scadenza dello stesso.

Inoltre, i Titolari dei certificati si impegnano a:

- nel caso dei certificati per Code Signing: non firmare software maligno ("malware") e non descrivere il software firmato in modo fuorviante rispetto alle sue reali funzionalità e finalità;
- nel caso dei certificati SSL Server: installare il Certificato esclusivamente sui server che sono accessibili ai SubjectAlternativeName elencati nel Certificato e gestire tali server solo come consentito dal presente CPS e dalle norme vigenti.

Il Titolare riconosce e accetta che la CA, qualora e non appena scopra che un certificato viene usato dal Titolare per attività illecite (es. "Phishing", attacchi di tipo "man-in-the-middle", distribuzione di malware, ecc.) e/o per l'emissione di altri certificati, è autorizzata a revocare il certificato immediatamente e senza alcun preavviso.

9.6.4 Relying Party

Si definisce "Relying Party" chiunque (eccetto il Titolare) faccia affidamento su un certificato per prendere decisioni (come ad esempio: rendere disponibili informazioni o risorse al Titolare, utilizzare le informazioni o risorse ottenute dal Titolare, ecc.).

Ogni Relying Party che si affida ad un Certificato emesso da Actalis dichiara e garantisce che:

- ha compiuto uno sforzo ragionevole per acquisire un'adeguata comprensione dei certificati e delle PKI;
- ha letto, compreso e accettato questo CPS, incluso il paragrafo 9.8 (Limitazioni di responsabilità);
- ha verificato lo stato del Certificato attraverso i servizi informativi descritti nel paragrafo 4.10;
- NON farà affidamento sul Certificato se questo è scaduto o revocato.

9.7 Esclusione di garanzie

Actalis non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente indicato in questo CPS o in un eventuale accordo separato con un Titolare. Vedere anche le Condizioni Generali del servizio pubblicate sul sito web di Actalis.

9.8 Limitazioni di responsabilità

Gli obblighi e le responsabilità di Actalis sono esclusivamente quelli definiti dal presente documento e dal Contratto di fornitura del Servizio. In caso di violazione o inadempimento imputabile ad Actalis, nel caso in cui la stessa abbia dimostrato che detta violazione o inadempimento si siano verificati senza proprio dolo o negligenza, la medesima non risponderà per un importo superiore al corrispettivo versato dal Cliente per il Servizio, ordinato o rinnovato, interessato dall'evento dannoso riferito al mese in cui detto evento si è verificato, restando in tal caso espressamente escluso, ora per allora, qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie.

Fermo quanto precede, fatte salve le ipotesi inderogabilmente previste dalla legge, in nessun altro caso, per nessun titolo e/o ragione, Actalis potrà essere ritenuta responsabile nei confronti del Cliente, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati al Cliente, per danni, diretti o indiretti, perdite di dati, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare a fronte dell'erogazione del Servizio, ove connessi, direttamente o indirettamente, o derivanti da:

a) cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni, scioperi, sommosse, ecc.); e/o

b) manomissioni o interventi sul Servizio o sulle apparecchiature effettuati dal Cliente e/o da parte di terzi non autorizzati da Actalis.

Actalis non sarà considerata in nessun caso responsabile per l'uso fatto del Servizio in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici; in tali casi, Actalis si rende disponibile a valutare e negoziare con il Cliente uno specifico accordo "mission critical" con i rispettivi "SLA" (Service Level Agreements).

Actalis non presta alcuna garanzia sulla validità ed efficacia, anche probatoria, del Servizio o di qualsiasi dato, informazione, messaggio, atto o documento ad esso associato o comunque immesso, comunicato, trasmesso, conservato o in ogni modo trattato mediante il Servizio medesimo:

a) quando il Cliente intende utilizzarli o farli valere in Stati ovvero ordinamenti diversi da quello Italiano, fatta eccezione, per quanto riguarda gli Stati facenti parte dell'Unione Europea, per i Certificati emessi in base al presente documento;

b) per la loro segretezza e/o integrità (nel senso che eventuali violazioni di queste ultime sono, di norma, rilevabili dall'Utente o dal destinatario attraverso l'apposita procedura di verifica).

Actalis non assume, in nessun caso, alcuna responsabilità per le informazioni, i dati, i contenuti immessi o trasmessi e, comunque, trattati dal Cliente mediante il Servizio ed in genere per l'uso fatto dal medesimo del predetto Servizio e si riserva di adottare qualsiasi iniziativa ed azione, a tutela dei propri diritti ed interessi, ivi compresa la comunicazione ai soggetti coinvolti dei dati utili a consentire l'identificazione del Cliente.

9.9 Indennizzi

9.9.1 Indennizzi da parte della CA

La CA si atterrà al paragrafo 9.9.1 dei [BR] nei confronti dei fornitori di software applicativo che hanno stipulato un contratto di distribuzione di certificati di Root CA con Actalis.

9.9.2 Indennizzi da parte dei Titolari

I Titolari sono obbligati al risarcimento dei danni eventualmente sofferti da Actalis nei seguenti casi:

- false dichiarazioni nella richiesta di certificazione;
- omessa informazione alla CA in merito ad atti o fatti essenziali, per negligenza o con l'obiettivo di raggirare Actalis;
- utilizzo di nomi (per es. nomi di dominio, marchi commerciali) in violazione dei diritti di proprietà intellettuale;
- utilizzo del certificato per finalità illecite e/o non previste dal presente COPS.

9.10 Durata e risoluzione del contratto

9.10.1 Durata del contratto

Il Contratto ha inizio dalla data dell'adesione da parte del Contraente ed ha termine alla data di scadenza del certificato emesso da Actalis; in caso di rinnovo del certificato medesimo, la validità del Contratto è differita sino alla data di scadenza del certificato rinnovato. In ogni caso la validità del Contratto cesserà in conseguenza della revoca, per qualunque motivo effettuata, del certificato.

9.10.2 Risoluzione del contratto

Si rimanda alle Condizioni Generali pubblicate sul sito web della CA.

9.10.3 Effetti della risoluzione

Nel caso di risoluzione del contratto, il certificato del Titolare viene revocato dalla CA.

9.11 Avvisi e comunicazioni

Actalis accetta comunicazioni relative a questo CPS, da inviare con i metodi indicati nel paragrafo 1.5.2. I mittenti sono invitati a firmare digitalmente le proprie comunicazioni, se possibile, o utilizzare un altro metodo di comunicazione affidabile. Alle comunicazioni valide sarà data risposta in modo tempestivo.

Le richieste di assistenza relative al servizio qui descritto (per es. dubbi di carattere operativo, mancata ricezione del certificato, difficoltà di installazione, ecc.) possono essere fatte ad Actalis nel caso in cui il certificato sia stato acquistato direttamente da Actalis. In tal caso, si può richiedere assistenza mediante e-mail all'indirizzo sslweb-server@actalis.it avendo cura di riportare nella mail, oltre alla descrizione del presunto problema, perlomeno il nome, cognome, numero di telefono e organizzazione di appartenenza del mittente. Se invece il certificato è stato acquistato da un rivenditore di Actalis, l'assistenza deve essere richiesta a quel rivenditore.

Le segnalazioni di problemi relativi a certificati già emessi ed installati, invece, devono essere fatte con le modalità descritte nel paragrafo 4.13.

9.12 Revisioni del CPS

9.12.1 Procedura per le revisioni

La CA si riserva di apportare modifiche a questo CPS in qualsiasi momento, senza preavviso, per esigenze tecniche od organizzative proprie oppure a seguito di variazioni normative. Ogni nuova versione del CPS annulla e sostituisce le versioni precedenti.

9.12.2 Periodo e meccanismo di notifica

Questo CPS viene riesaminato dalla CA e, se necessario, aggiornato almeno una volta ogni anno anche in assenza di variazioni normative.

Le nuove versioni del CPS sono pubblicate sul sito web del CA.

9.12.3 Circostanze che richiedono la modifica dell'OID

Questo CPS si applica a varie policy di certificato (vedere il par. 1.4), ciascuna identificata da uno specifico OID. La revisione del CPS non implica, di per sé, la modifica di tali OID.

9.13 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 CPS sarà competente esclusivamente il Foro di Arezzo.

9.14 Legge applicabile, interpretazione e giurisdizione

Questo CPS è soggetto alla legge Italiana e come tale sarà interpretato ed eseguito. Per quanto non espressamente previsto nel presente CPS, valgono le norme vigenti.

Altri contratti nei quali questo CPS è incorporato mediante riferimento, possono contenere clausole distinte rispetto alla legge applicabile.

9.15 Conformità alle leggi applicabili

Si riportano di seguito i principali riferimenti normativi applicabili:

- Regolamento (UE) 2014/910 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 (anche "eIDAS").
- Decreto Legislativo 7 marzo 2005, n.82: "Codice dell'Amministrazione Digitale", G.U. n.112 del 16 maggio 2005, e s.m.i. (anche "CAD").
- Decreto Legislativo 30 giugno 2003, n. 196: "Codice in materia di protezione dei dati personali", G.U. n. 174 del 29 luglio 2003, e s.m.i.
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

9.16 Disposizioni varie

9.16.1 Intero accordo

Il presente CPS, che può essere integrato o meno da Condizioni Generali o particolari di contratto sottoscritte specificamente dal Richiedente, costituisce la disciplina che regola l'utilizzo del Certificato da parte del Titolare e regola inoltre i rapporti tra Titolare e CA. La richiesta del Certificato implica l'accettazione integrale e incondizionata del presente CPS da parte del Titolare.

9.16.2 Cessione del contratto

Si rimanda alle Condizioni Generali del servizio pubblicate sul sito web della CA.

9.16.3 Salvaguardia

La CA si atterrà al paragrafo 9.6.13 dei [BR], se applicabile, e alle Condizioni Generali pubblicate sul sito web della CA.

9.16.4 Applicazione (spese legali e rinuncia ai diritti)

Si rimanda alle Condizioni Generali del servizio pubblicate sul sito web della CA.

9.16.5 Forza maggiore

Actalis non sarà responsabile della mancata esecuzione delle obbligazioni qui assunte qualora tale mancata esecuzione sia dovuta a cause non imputabili ad Actalis, quali - a scopo esemplificativo e senza intento limitativo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgano nell'esecuzione delle attività connesse al servizio qui descritto - ed altre cause imputabili a terzi.

9.17 Altre disposizioni

9.17.1 Livelli di servizio

La CA si impegna a rispettare i seguenti livelli di servizio:

Metrica	Obiettivo	Base di misura
Disponibilità di CRL e OCSP (24 x 7)	99.8 %	annuale
Disponibilità del sito web (24 x 7)	99.8 %	annuale
Tempo di emissione del certificato	massimo 5 gg lavorativi nel 95% di casi	annuale
Tempo di revoca del certificato (se richiesta on-line)	massimo 2 minuti nel 95% dei casi	annuale
Tempo di revoca del certificato (se richiesta via fax, posta, email)	massimo 6 ore nel 95% dei casi	annuale

Andrea
Sassetti
Firmato
digitalmente
il 23/01/2020
16:07:14 CET