Certificate Policy and Certification Practice Statement

Certificati TLS Server

Versione: **6.1**

Data: **09 Novembre 2026**

Approvato da:	Andrea Sassetti
Codice documento:	MODAC_A_66
Distribuzione:	Pubblica



Sassetti
Andrea
09.11.2026
08:39:43
UTC

Sommario

1 INTRODUZIONE 7
1.1 SCOPO DEL DOCUMENTO 7
1.2 IDENTIFICAZIONE DEL DOCUMENTO 7
1.3 PARTECIPANTI ALLA PKI 8
1.3.1 Certification Authorities 8
1.3.2 Registration Authorities 11
1.3.3 Titolari (subscribers) 11
1.3.4 Relying parties 12
1.3.5 Rivenditori 12
1.4 USO DEI CERTIFICATI 12
1.4.1 Usi appropriati dei certificati 12
1.4.2 Usi non consentiti dei certificati 13
1.5 AMMINISTRAZIONE DEL CPS 13
1.5.1 Organizzazione responsabile 13
1.5.2 Informazioni di contatto 13
1.5.3 Soggetto che stabilisce l'idoneità del CPS 14
1.5.4 Procedura di approvazione del CPS 14
1.6 DEFINIZIONI E ACRONIMI 15
1.7 RIFERIMENTI NORMATIVI 16

2 PUBBLICAZIONI E REPOSITORY 17
2.1 REPOSITORY 17
2.2 INFORMAZIONI PUBBLICATE 17
2.2.1 Divulgazione delle informazioni su CCADB e Root Programs 17
2.3 TEMPI E FREQUENZA DELLE PUBBLICAZIONI 17
2.4 CONTROLLO DEGLI ACCESSI 18

3 IDENTIFICAZIONE ED AUTENTICAZIONE (I&A) 19
3.1 REGOLE DI DENOMINAZIONE (NAMING) 19
3.1.1 Tipi di nomi 19
3.1.2 Significatività dei nomi 19
3.1.3 Anonimato e pseudonimia dei Titolari 19
3.1.4 Regole per l'interpretazione dei nomi 19
3.1.5 Univocità dei nomi 19
3.1.6 Riconoscimento, verifica e ruolo dei marchi registrati 19
3.2 VALIDAZIONE INIZIALE DELL'IDENTITÀ 19
3.2.1 Dimostrazione del possesso della chiave privata 19
3.2.2 Autenticazione dell'organizzazione e dei domini 20
3.2.3 Autenticazione delle identità individuali 24
3.2.4 Informazioni del Titolare non verificate 24
3.2.5 Verifica dell'autorizzazione 24
3.2.6 Criteri di interoperabilità 25
3.3 IDENTIFICAZIONE E AUTENTICAZIONE PER LE RICHIESTE DI RIEMISSIONE 25
3.3.1 Identificazione e autenticazione per le riemissioni di routine 25
3.3.2 Identificazione e autenticazione per la riemissione a seguito di revoca 25
3.4 IDENTIFICAZIONE E AUTENTICAZIONE PER LE RICHIESTE DI REVOCA 25

4 REQUISITI OPERATIVI DI GESTIONE DEI CERTIFICATI 26
4.1 RICHIESTA DEL CERTIFICATO 26
4.1.1 Chi può richiedere i certificati 26
4.1.2 Processo di richiesta e responsabilità 26
4.2 ELABORAZIONE DELLE RICHIESTE 28
4.2.1 Svolgimento delle funzioni di identificazione e autenticazione 28
4.2.2 Approvazione o rifiuto delle richieste 29
4.2.3 Tempi di elaborazione delle richieste 29
4.3 EMISSIONE DEL CERTIFICATO 29
4.3.1 Azioni della CA durante l'emissione del certificato 29
4.3.2 Notifica di emissione certificato al Titolare 30
4.4 ACCETTAZIONE DEL CERTIFICATO 30
4.4.1 Comportamenti che costituiscono accettazione del certificato 30

4.4.2 Pubblicazione del certificato da parte della CA 30
4.4.3 Notifica di emissione certificato ad altri soggetti 30
4.5 USO DELLA COPPIA DI CHIAVI E DEL CERTIFICATO 31
4.5.1 Uso della chiave privata e del certificato da parte del titolare 31
4.5.2 Uso della chiave pubblica e del certificato da parte delle Relying Part 31
4.6 RINNOVO DEL CERTIFICATO 31
4.6.1 Circostanze per il rinnovo del certificato 31
4.6.2 Chi può richiedere il rinnovo 31
4.6.3 Elaborazione delle richieste di rinnovo 31
4.6.4 Notifica al titolare di nuova emissione del certificato 31
4.6.5 Comportamenti che costituiscono accettazione del certificato rinnovato 31
4.6.6 Pubblicazione del certificato rinnovato da parte della CA 31
4.6.7 Notifica ad altri soggetti della nuova emissione del certificato 31
4.7 RIGENERAZIONE DELLA CHIAVE 31
4.7.1 Circostanze per il re-key del certificato 32
4.7.2 Chi può richiedere il re-key della chiave pubblica 32
4.7.3 Elaborazione delle richieste di re-key 32
4.7.4 Notifica al Titolare del rilascio del nuovo certificato 32
4.7.5 Comportamenti che costituiscono l'accettazione dei un certificato re-key 32
4.7.6 Distribuzione del nuovo certificato da parte della CA 32
4.7.7 Notifica ad altri soggetti della nuova emissione del certificato 32
4.8 MODIFICA DEL CERTIFICATO 32
4.8.1 Circostanze per la modifica del certificato 32
4.8.2 Chi può richiedere la modifica del certificato 32
4.8.3 Elaborazione delle richieste di modifica del certificato 32
4.8.4 Notifica al titolare dell'emissione del rilascio del nuovo certificato 33
4.8.5 Comportamenti che costituiscono l'accettazione del nuovo certificato 33
4.8.6 Pubblicazione del certificato modificato da parte della CA 33
4.8.7 Notifica ad altri soggetti della nuova emissione del certificato 33
4.9 SOSPENSIONE E REVOCA DEL CERTIFICATO 33
4.9.1 Circostanze per la revoca 33
4.9.2 Chi può richiedere la revoca 35
4.9.3 Procedura per la revoca 35
4.9.4 Periodo di grazia per le richieste di revoca 36
4.9.5 Tempi massimi di attuazione della revoca 36
4.9.6 Requisiti di verifica della revoca 36
4.9.7 Frequenza di emissione delle CRL 36
4.9.8 Massima latenza delle CRL 36
4.9.9 Disponibilità di servizi on-line di verifica revoca 36
4.9.10 Requisiti dei servizi on-line di verifica revoca 36
4.9.11 Altre modalità di pubblicizzazione della revoca 36
4.9.12 Requisiti particolari nel caso di compromissione della chiave 36
4.9.13 Circostanze per la sospensione 37
4.9.14 Chi può richiedere la sospensione 37
4.9.15 Procedura per la sospensione 37
4.9.16 Limiti sul periodo di sospensione 37
4.10 SERVIZI INFORMATIVI SULLO STATO DEL CERTIFICATO 37
4.10.1 Caratteristiche operative 37
4.10.2 Disponibilità del servizio 38
4.10.3 Caratteristiche opzionali 38
4.11 CESSAZIONE DEL CONTRATTO 38
4.12 KEY ESCROW E KEY RECOVERY 38
4.12.1 Politiche e pratiche di key escrow e recovery 38
4.12.2 Politiche e pratiche di session key encapsulation e recovery 38
5 MISURE DI SICUREZZA FISICA E OPERATIVA 39
5.1 SICUREZZA FISICA 39
5.1.1 Ubicazione e caratteristiche costruttive dei siti produttivi 39
5.1.2 Accessi fisici 39
5.1.3 Alimentazione elettrica e condizionamento 39
5.1.4 Prevenzione e protezione dagli allagamenti 39

5.1.5 Prevenzione e protezione dagli incendi ... 39
5.1.6 Conservazione dei supporti di memoria ... 39
5.1.7 Smaltimento dei rifiuti ... 40
5.1.8 Off-site backup ... 40
5.2 SICUREZZA OPERATIVA ... 40
5.2.1 Ruoli di fiducia ... 40
5.2.2 Numero di persone richieste per lo svolgimento delle attività ... 40
5.2.3 Identificazione e autenticazione per ciascun ruolo ... 40
5.2.4 Ruoli che richiedono la separazione dei compiti ... 41
5.3 SICUREZZA DEL PERSONALE ... 41
5.3.1 Qualifiche, esperienze e autorizzazioni richieste ... 41
5.3.2 Verifica dei precedenti ... 41
5.3.3 Requisiti di formazione ... 41
5.3.4 Frequenza di aggiornamento della formazione ... 41
5.3.5 Rotazione delle mansioni ... 42
5.3.6 Sanzioni per le azioni non autorizzate ... 42
5.3.7 Controlli sul personale non dipendente ... 42
5.3.8 Documentazione fornita al personale ... 42
5.4 GESTIONE DEL GIORNALE DI CONTROLLO ... 42
5.4.1 Tipi di eventi registrati ... 42
5.4.2 Frequenza di elaborazione del giornale di controllo ... 42
5.4.3 Periodo di conservazione del giornale di controllo ... 43
5.4.4 Protezione del giornale di controllo ... 43
5.4.5 Procedure di backup del giornale di controllo ... 43
5.4.6 Sistema di raccolta del giornale di controllo ... 43
5.4.7 Notifiche nel caso di rilevazione di eventi sospetti ... 43
5.4.8 Verifiche di vulnerabilità ... 43
5.5 ARCHIVIAZIONE DELLE REGISTRAZIONI ... 44
5.5.1 Tipi di informazioni archiviate ... 44
5.5.2 Periodo di conservazione degli archivi ... 44
5.5.3 Protezione degli archivi ... 44
5.5.4 Procedure di backup degli archivi ... 44
5.5.5 Marcatura temporale degli archivi ... 44
5.5.6 Sistema di archiviazione (interno o esterno) ... 44
5.5.7 Procedura di recupero e verifica delle informazioni archiviate ... 44
5.6 PASSAGGIO A NUOVE CHIAVI ... 44
5.6.1 Root CA ... 44
5.6.2 CA subordinata ... 45
5.7 COMPROMISSIONE E DISASTER RECOVERY ... 45
5.7.1 Procedure di gestione degli incidenti e delle compromissioni ... 45
5.7.2 Corruzione o perdita degli elaboratori, del software e/o dei dati ... 46
5.7.3 Procedure nel caso di compromissione della chiave della CA ... 46
5.7.4 Continuità operativa a fronte di un disastro ... 47
5.8 CESSAZIONE DELLA CA O DELLE RA ... 47

6 MISURE DI SICUREZZA TECNICA ... 48
6.1 GENERAZIONE E INSTALLAZIONE DELLE CHIAVI ... 48
6.1.1 Generazione della coppia di chiavi ... 48
6.1.2 Consegna della chiave privata al titolare ... 48
6.1.3 Consegna della chiave pubblica alla CA ... 48
6.1.4 Distribuzione della chiave pubblica della CA ... 48
6.1.5 Lunghezza delle chiavi ... 48
6.1.6 Generazione dei parametri e qualità delle chiavi ... 49
6.1.7 Key Usage (estensione X.509 v3) ... 49
6.2 PROTEZIONE DELLA CHIAVE PRIVATA E SICUREZZA DEI MODULI CRITTOGRAFICI ... 49
6.2.1 Requisiti di sicurezza dei moduli crittografici ... 49
6.2.2 Controllo multi-persona (N di M) della chiave privata ... 49
6.2.3 Deposito in garanzia della chiave privata ... 49
6.2.4 Backup della chiave privata ... 50
6.2.5 Archiviazione della chiave privata ... 50
6.2.6 Trasferimento della chiave privata dal/al modulo crittografico ... 50

6.2.7 Memorizzazione della chiave privata sul modulo crittografico 50
6.2.8 Modalità di attivazione della chiave privata 50
6.2.9 Modalità di disattivazione della chiave privata 50
6.2.10 Modalità per la distruzione della chiave privata 50
6.2.11 Classificazione dei moduli crittografici 50
6.3 ALTRI ASPETTI DELLA GESTIONE DELLE CHIAVI 50
6.3.1 Archiviazione della chiave pubblica 50
6.3.2 Durata operativa dei certificati e delle chiavi 50
6.4 DATI DI ATTIVAZIONE 51
6.4.1 Generazione dei dati di attivazione 51
6.4.2 Protezione dei dati di attivazione 51
6.4.3 Altri aspetti relativi ai dati di attivazione 51
6.5 SICUREZZA DEGLI ELABORATORI 51
6.5.1 Requisiti di sicurezza degli elaboratori 51
6.5.2 Rating di sicurezza degli elaboratori 52
6.6 SICUREZZA DEL CICLO DI VITA 52
6.6.1 Sicurezza nello sviluppo dei sistemi 52
6.6.2 Sistema di gestione della sicurezza 52
6.6.3 Gestione del ciclo di vita 52
6.7 SICUREZZA DI RETE 52
6.8 TIME-STAMPING 53

7 PROFILO DEI CERTIFICATI, CRL E OCSP 54
7.1 PROFILO DEL CERTIFICATO 54
7.1.1 Numeri di versione 54
7.1.2 Contenuto ed estensioni dei certificati 54
7.1.3 Identificatori degli algoritmi 68
7.1.4 Forme dei nomi 68
7.1.5 Vincoli sui nomi 70
7.1.6 Identificatori delle policy 70
7.1.7 Uso dell'estensione PolicyConstraints 70
7.1.8 Sintassi e semantica dei qualificatori delle policy 70
7.1.9 Regole di elaborazione dell'estensione CertificatePolicies 70
7.2 PROFILO DELLA CRL 70
7.2.1 Numeri di versione 70
7.2.2 Estensioni della CRL 70
7.3 PROFILO OCSP 70
7.3.1 Numeri di versione 71
7.3.2 Estensioni OCSP 71

8 VERIFICHE DI CONFORMITÀ 72
8.1 FREQUENZA E CIRCOSTANZE DALLE VERIFICHE 72
8.2 IDENTITÀ E QUALIFICAZIONE DEGLI ISPETTORI 72
8.3 RELAZIONI TRA LA CA E GLI AUDITOR 72
8.4 ARGOMENTI COPERTI DALLE VERIFICHE 72
8.5 AZIONI CONSEGUENTI ALLE NON-CONFORMITÀ 72
8.6 COMUNICAZIONE DEI RISULTATI DELLE VERIFICHE 73
8.7 AUTOVALUTAZIONI (SELF-AUDIT) 73

9 CONDIZIONI GENERALI DEL SERVIZIO 74
9.1 TARIFFE DEL SERVIZIO 74
9.1.1 Tariffe per l'emissione o rinnovo del certificato 74
9.1.2 Tariffe per l'accesso ai certificati 74
9.1.3 Tariffe per l'accesso alle informazioni di stato dei certificati 74
9.1.4 Tariffe per altri servizi 74
9.1.5 Politica per il rimborso 74
9.2 RESPONSABILITÀ FINANZIARIA 74
9.2.1 Copertura assicurativa 74
9.2.2 Altri asset 74
9.2.3 Garanzia o copertura assicurativa per gli utenti finali 74
9.3 CONFIDENZIALITÀ DELLE INFORMAZIONI TRATTATE 74
9.3.1 Ambito di applicazione delle informazioni confidenziali 74

9.3.2 Informazioni considerate non confidenziali *75*
9.3.3 Responsabilità di protezione delle informazioni confidenziali *75*
9.4 TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI 75
9.4.1 Programma sulla privacy *75*
9.4.2 Dati che sono considerati personali *75*
9.4.3 Dati che non sono considerati personali *75*
9.4.4 Responsabilità di protezione dei dati personali *76*
9.4.5 Informativa e consenso al trattamento dei dati personali *76*
9.4.6 Divulgazione dei dati a seguito di richiesta dell'autorità giudiziaria *76*
9.4.7 Altre circostanze di possibile divulgazione dei dati personali *76*
9.5 DIRITTI DI PROPRIETÀ INTELLETTUALE 76
9.6 DICHIARAZIONI E GARANZIE 76
9.6.1 Dichiarazioni e garanzie della CA *76*
9.6.2 Dichiarazioni e garanzie delle RA *77*
9.6.3 Dichiarazioni e garanzie dei Titolari *77*
9.6.4 Relying Party *78*
9.6.5 Dichiarazioni e garanzie degli altri partecipanti *78*
9.7 ESCLUSIONE DI GARANZIE 78
9.8 LIMITAZIONI DI RESPONSABILITÀ 78
9.9 INDENNIZZI 79
9.9.1 Indennizzi da parte della CA *79*
9.9.2 Indennizzi da parte dei Titolari *80*
9.10 DURATA E RISOLUZIONE DEL CONTRATTO 80
9.10.1 Durata del contratto *80*
9.10.2 Risoluzione del contratto *80*
9.10.3 Effetti della risoluzione *80*
9.11 AVVISI E COMUNICAZIONI 80
9.12 REVISIONI DEL CPS 81
9.12.1 Procedura per le revisioni *81*
9.12.2 Periodo e meccanismo di notifica *81*
9.12.3 Circostanze che richiedono la modifica dell'OID *81*
9.13 FORO COMPETENTE 81
9.14 LEGGE APPLICABILE, INTERPRETAZIONE E GIURISDIZIONE 81
9.15 CONFORMITÀ ALLE LEGGI APPLICABILI 81
9.16 DISPOSIZIONI VARIE 82
9.16.1 Intero accordo *82*
9.16.2 Cessione del contratto *82*
9.16.3 Salvaguardia *82*
9.16.4 Applicazione (spese legali e rinuncia ai diritti) *82*
9.16.5 Forza maggiore *82*
9.17 ALTRE DISPOSIZIONI 82
9.17.1 Livelli di servizio *82*

APPENDICE A – STORICO DELLE MODIFICHE 83

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).

l presente documento costituisce il documento combinato CP/CPS di Actalis relativo all'emissione e alla gestione dei certificati TLS Server. Il presente CPS è strutturato conformemente allo schema previsto dalla sezione 6 della [RFC 3647], come eventualmente integrato o modificato dai BRs dei certificati TLS del CA/Browser Forum.

Actalis aderisce alle ultime versioni pubblicate dei seguenti documenti:

- i "TLS Baseline Requirements" e le "EV Guidelines" del CAB Forum, disponibili all'indirizzo https://www.cabforum.org;
- la "CCADB Policy", disponibile all'indirizzo https://www.ccadb.org/policy;
- tutte le politiche relative ai Root Programs, inclusi, a titolo esemplificativo ma non esaustivo, il "*Chrome Root Program*", l'"*Apple Root Program*", la "*Mozilla Root Store Policy*" e il "*Microsoft Root Program*".

Qualora siano previsti requisiti di diverso rigore nelle policy sopra menzionate, con specifico riferimento ai Root Programs, Actalis si conforma al requisito più restrittivo. In caso di incongruenze tra il presente CPS e tali documenti, questi ultimi hanno la precedenza.

I certificati **TLS Server** disciplinati da questo CPS, Actalis rispetta la versione corrente dei **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates** e delle **Guidelines for Issuance and Management of Extended Validation Certificates** pubblicate su http://www.cabforum.org (nel prosieguo definiti congiuntamente anche come "Linee Guida"). In caso di conflitto tra il presente documento e tali Linee Guida, queste ultime hanno la precedenza.

Questo CPS è distribuito sotto la *Creative Commons Attribution-NoDerivatives 4.0 International License*.
Per visualizzare una copia di questa licenza, visitare http://creativecommons.org/licenses/by-nd/4.0/ o inviare una lettera a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA

1.2 Identificazione del documento

Il presente documento costituisce la **Certificate Policy e Certification Practice Statement** (di seguito, per brevità, "CPS") applicabile ai **certificati TLS Server** emessi da **Actalis S.p.A**. La versione del documento e la data dell'ultima revisione sono riportate nella prima pagina.

Il presente documento è pubblicato sul sito web di Actalis in lingua italiana e in lingua inglese. In caso di difformità o incoerenza tra le due versioni, prevale la versione in lingua inglese.

Il presente CPS è pubblicato in formato PDF firmato digitalmente, al fine di garantirne l'autenticità dell'origine e l'integrità.

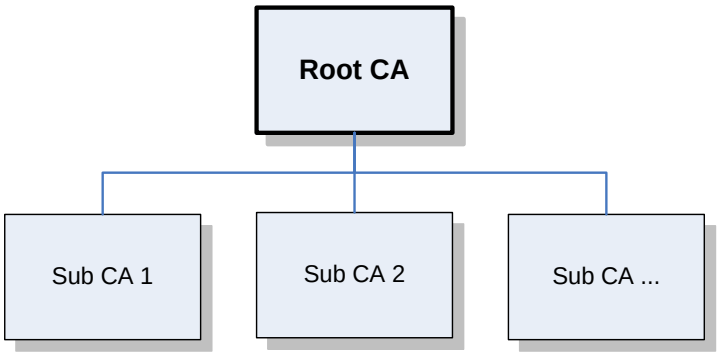
Actalis pubblica inoltre il presente CPS in formato Markdown, al fine di favorire la trasparenza, la verificabilità, il confronto tra le diverse versioni e la tracciabilità delle modifiche. Qualora il presente CPS sia pubblicato in più formati, Actalis garantisce la coerenza del contenuto ufficiale tra le diverse rappresentazioni e identifica chiaramente la versione avente valore ufficiale in caso di discrepanze. La versione avente valore ufficiale è quella pubblicata in formato PDF.

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 TLS Server è organizzata gerarchicamente su due livelli, come mostrato nello schema seguente:



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

In particolare, esistono ad oggi:

- Una gerarchia *legacy* basata sulla singola Root CA multi-purpose *"Actalis Authentication Root CA",* inclusa nei principali root certificate store, ad oggi in produzione. Sotto quest'unica Root CA operano varie SubCA che emettono certificati di diversa tipologia (TLS Server, Code Signing, S/MIME, ecc.);
- Nuove gerarchie basate su Root CA *single-purpose* dettagliate di seguito e ad oggi non incluse, nei principali root certificate store. Queste gerarchie sono destinate a sostituire la struttura legacy, costituendo la base per la migrazione strutturata dei certificati. Le nuove gerarchie sono specifiche per tipologia di certificato (TLS Server, Code Signing, S/MIME, etc.).

Actalis gestisce la propria gerarchia PKI in conformità ai requisiti applicabili dei Root Store Program relativi al ciclo di vita delle infrastrutture di certificazione, inclusi i requisiti e le aspettative concernenti le gerarchie PKI dedicate a uno specifico scopo, la pianificazione della successione delle Root CA e la progressiva dismissione delle Root CA legacy o multiuso. Le nuove gerarchie di Root CA dedicate esclusivamente all'emissione di certificati TLS Server, descritte nella presente sezione, sono finalizzate a supportare la migrazione dalla preesistente gerarchia multiuso verso gerarchie dedicate all'autenticazione TLS Server, in conformità alle policy applicabili dei Root Store Program e ai relativi piani di transizione.

Alcune delle Root CA su cui si basano le nuove gerarchie sono state cross-certificate dalla Root CA *multi-purpose*, consentendo così l'emissione di certificati anche utilizzando le CA subordinate sottostanti a tali nuove Root CA.

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
Indirizzo di posta elettronica (informativo):	info@actalis.it

1.3.1.1 Root Certification Authority

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	SHA-256 Fingerprint	notBefore	notAfter
CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT	55926084EC963A64B96E2ABE01CE0BA86A64FBFEBCC7AAB5AFC155B37FD76066	22 Settembre 2011	22 Settembre 2030
CN = Actalis TLS Server ECC Root CA 2025 O = Actalis S.p.A. C = IT	4EFAADA2543E1E02666998574B3BAD96AE264088FA5917F75D32E7A609D1869C	28 Febbraio 2025	22 Febbraio 2050
CN = Actalis TLS Server RSA Root CA 2025 O = Actalis S.p.A. C = IT	6D0E47DFDE7CF48308CD4C6C1517DD1AF033DCC72BB0501C04268B03B58A9085	28 Febbraio 2025	22 Febbraio 2050

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	SHA-256 Fingerprint	notBefore	notAfter
CN = Actalis Organization Validated Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	931AAA1EC9B2BA0FA59A82302F4F830628C86D9B2D2A50A4D1B2CE895C4CC648	06 luglio 2020	22 settembre 2030

CN = Actalis Extended Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	124EAAF26F570C4FB4D89F5D61078F15B885345FCAF0C57F3477D8C63B5AB26F	06 luglio 2020	22 settembre 2030
CN = Actalis Domain Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	3450B6D38290C3CA5D7BB38B71495BBF72C6D0C44DBA292245F9BCA9843A9FFF	06 luglio 2020	22 settembre 2030
CN = Actalis DV Server ACME CA G1 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	C0A9FB425D0EDEBC72BC6C47AD3D3A2B68245ED1D59A5883BF19CE9F8C4DED1F	06 giugno 2023	22 settembre 2030
CN = Actalis Domain Validated TLS Server ECC CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	E102A52A016B025B31C749A9A0A7F4650E1227AFA27C27E9A37C846AD42FA8B0	07 luglio 2025	05 luglio 2035
CN = Actalis Extended Validation TLS Server ECC CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	12D8FBF-FEB27481EB0EECD032336D6D1E2B1A678A9B1018E653E7FC253D929A5	07 luglio 2025	05 luglio 2035
CN = Actalis Organization Validated TLS Server ECC CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	E7929CDA1A88D2E94016A3F2D52BE95DB1C28C178C425B4303A82E3E29293544	07 luglio 2025	05 luglio 2035
CN = Actalis Domain Validated TLS Server RSA CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	C511EF2F15EF7681EEA-DFF97F1E90596270EADB71BDA8F847AB36FFF15DC6264	07 luglio 2025	05 luglio 2035
CN = Actalis Extended Validation TLS Server RSA CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	8FA40E1594EB493E5D2954F577BB50473A3512F2D203A99B402BBCB608AED73B	07 luglio 2025	05 luglio 2035
CN = Actalis Organization Validated TLS Server RSA CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	BAE1C37CEE8621A3016AE4E76E36204949DA3160BCE5AE56CF4003860EE3B2CD	07 luglio 2025	05 luglio 2035

Possono essere rilasciati certificati di SubCA, sotto una Root CA di Actalis, per **CA esterne** (ossia non gestite da Actalis) previa stipula di un **contratto** col quale i gestori di tali SubCA si impegnano, tra l'altro, a rispettare i

Baseline Requirements del CAB Forum [BR][1] nonché a sottoporsi **annualmente** ad un **audit di conformità** ai [BR] da parte di un **auditor indipendente e qualificato** 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.

Actalis notifica ai Root Store Program, con il preavviso previsto dalle rispettive policy, l'emissione di qualsiasi certificato di CA (Subordinate CA o Cross Certificate) che comporti un'estensione del *trust boundary* dei Root Store o sostituisca un certificato di CA non revocato il cui Subject CA Owner non sia incluso nei Root Store. Tali certificati non sono emessi senza la preventiva approvazione esplicita, ove prevista, del relativo Program notificato.

1.3.1.3 Cross Certificati

Alla data di revisione del presente CPS, i cross-certificati di Actalis (certificazione incrociata tra vecchie e nuove Root CA di Actalis) sono quelli identificati di seguito; per ulteriori dettagli vedere anche il capitolo 7.

Subject DN	SHA-256 Fingerprint	notBefore	notAfter
CN = Actalis TLS Server ECC Root CA 2025 O = Actalis S.p.A./03358520967 L = Milan C = IT	471F644699FD038E07D73D6E980586AA232FA7DCAD57380B0C89EDD1DCFDB61E	07 agosto 2025	22 settembre 2030
CN = Actalis TLS Server RSA Root CA 2025 O = Actalis S.p.A./03358520967 L = Milan C = IT	944D87943C5B47F4DBCE29F55CF92CDA8F27556BE6237D1C51D1B7E574F189D0	07 agosto 2025	22 settembre 2030

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.

L'abilitazione è subordinata alla sottoscrizione di specifici accordi contrattuali che disciplinano le attività autorizzate, il rispetto dei requisiti normativi nei [BR] e nel CP/CPS della Certification Authority. Tali accordi prevedono inoltre la formazione degli operatori, l'eventuale svolgimento di audit periodici e l'utilizzo degli strumenti messi a disposizione dalla CA per le richieste di emissione e gestione dei certificati.

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

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

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**).

I certificati disciplinati dal presente CPS sono rilasciati a Richiedenti stabiliti o residenti in qualsiasi giurisdizione a livello mondiale, purché Actalis possa completare con esito positivo tutte le procedure di convalida applicabili. Il rilascio è negato qualora non sia possibile ottenere o verificare le informazioni e la documentazione richieste, oppure qualora sia vietato dalla normativa applicabile, da provvedimenti dell'autorità giudiziaria o da sanzioni vincolanti.

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 TLS Server, si tratta per esempio degli utenti del sito web interessato.

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 in conformità al presente CPS sono destinati esclusivamente all'abilitazione del protocollo TLS/TLS su uno o più server.

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-TLS.aspx. I Richiedenti sono tenuti a consultare tale elenco prima di richiedere i certificati.

Actalis emette altresì ulteriori tipologie di certificati (quali, a titolo esemplificativo, certificati S/MIME e Code Signing), non disciplinate dal presente CPS. Per tali servizi si applicano specifici CPS, pubblicati e consultabili sul sito web di Actalis.

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	TLS Server EV (Extended Validation)	1.3.159.1.17.1	[BR], [EVGL]
OV	TLS Server WildCard OV (Organization Validated)	1.3.159.1.19.1	[BR]
OV	TLS Server OV (Organization Validated)	1.3.159.1.20.1	[BR]
DV	TLS Server DV (Domain Validated)	1.3.159.1.22.1	[BR]
DV	TLS 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).

Actalis sconsiglia inoltre l'utilizzo di certificati TLS pubblicamente attendibili nelle infrastrutture critiche (ad esempio nei settori sanitario, dei trasporti o della difesa) qualora i Titolari non siano in grado di richiederne la riemissione in tempi molto rapidi a seguito di una revoca.

Actalis si riserva il diritto di mettere in esercizio nuove CA subordinate ovvero CA intermedie (ICA) quando lo ritiene necessario secondo le proprie valutazioni, e di sospendere l'emissione di certificati da quelle vecchie. In alcune circostanze, Actalis può anche dover revocare alcune ICA prima della loro naturale scadenza.

Actalis pertanto raccomanda di *non incorporare i certificati delle ICA nelle applicazioni e/o piattaforme software*.

Actalis sconsiglia fortemente il "*certificate pinning*" e non lo considera un motivo sufficiente per ritardare la revoca dei certificati.

I Titolari non dovrebbero utilizzare certificati "trusted" (ossia attendibili sul Web) in contesti in cui non vi è tale necessità (ad esempio su reti private), soprattutto dove una rapida sostituzione dei certificati non è fattibile.

I Titolari e tutte le terze parti interessate devono tenere presente che tutti i certificati "*trusted*" devono essere conformi a tutti i requisiti previsti dalle "*Root Policy*" dei browser applicabili, inclusi i periodi di revoca richiamati nella sezione 4.9.1 di questo CPS.

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;
- descrizione del presunto problema;
- informazioni sufficienti a identificare il certificato interessato, quali, a titolo esemplificativo, l'indirizzo del sito web presso il quale il certificato è utilizzato, ovvero l'hostname del certificato, la data di decorrenza della validità e il relativo 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[2]. 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, delle indicazioni di AgID 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.
La redazione, la verifica e l'approvazione del documento sono affidate a soggetti o funzioni distinti e indipendenti tra loro, garantendo la separazione delle responsabilità e un controllo sul contenuto prima della pubblicazione. Il personale incaricato della redazione e della revisione del presente documento possiede competenze specialistiche in materia di servizi di certificazione e sui requisiti normativi, tecnici e di settore applicabili. Il processo di aggiornamento prevede il controllo delle versioni del documento (*versioning*), la tracciabilità delle modifiche, delle verifiche e delle approvazioni, nonché la conservazione del-lo storico delle versioni precedenti. Ogni versione riporta la data di emissione e una sintesi del-le modifiche introdotte ed è pubblicata solo dopo il completamento dell'iter di approvazione. Ogni versione riporta la data di emissione e una sintesi delle modifiche introdotte ed è pubblicata solo dopo il completamento dell'iter di approvazione.

Questo CP/CPS viene riesaminato e aggiornato con frequenza almeno annuale, ovvero entro 365 giorni dall'ultimo aggiornamento, e ogniqualvolta intervengano modifiche dei requisiti applicabili o dei processi descritti che ne rendano necessario l'adeguamento.

[2] L'invio di messaggi indesiderati (spam) comporta l'applicazione delle azioni previste dalla normativa vigente nei confronti dei responsabili

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
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
ECC	Elliptic Curve Cryptography
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
ISMS	Information Security Management System
ISO	International Standards Organization
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
TLS	Secure Sockets Layer (di seguito, TLS 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.

[RFC2314] Kaliski, B., "PKCS #10: Certification Request Syntax Version 1.5", RFC 2314, March 1998. (http://www.ietf.org/rfc/rfc2251.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)

[RFC8659] P. Hallam-Baker, R. Stradling, J. Hoffman-Andrews, “DNS Certification Authority Authorization (CAA) Resource Record”, RFC 8659, November 2019. (https://www.rfc-editor.org/rfc/rfc8659)

[RFC 8657] Request for Comments: 8657, Certification Authority Authorization (CAA) Record Extensions for Account URI and Automatic Certificate Management Environment (ACME) Method Binding. H. Landau, et al. November 2019.

[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/working-groups/server/baseline-requirements/documents/)

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

[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.

[ACME] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, March 2019. (https://www.rfc-editor.org/info/rfc8555)

[CCADB] CCADB Policy - (https://www.ccadb.org/policy)

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 pubblicato sul sito web di Actalis (www.actalis.it e altri siti di Actalis in esso richiamati).

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;
- Modulistica.

2.2.1 Divulgazione delle informazioni su CCADB e Root Programs

Actalis mantiene nel CCADB informazioni accurate e aggiornate relative ai propri certificati di Root CA inclusi nei Root Store e ai relativi certificati di CA subordinate (ivi compresi i certificati cross). Salvo che una policy applicabile di un Root Store Program preveda un termine più breve, Actalis aggiorna le informazioni presenti nel CCADB entro quattordici (14) giorni di calendario dal verificarsi di ogni modifica rilevante.

Actalis registra nel CCADB tutti i certificati di CA subordinate, inclusi i certificati cross, entro sette (7) giorni di calendario dalla loro emissione e, in ogni caso, prima che tali certificati siano utilizzati per emettere certificati pubblicamente trusted. Actalis provvede inoltre a registrare nel CCADB i certificati di CA subordinate revocati entro sette (7) giorni di calendario dalla revoca, comprensivi delle informazioni richieste relative alla revoca. Per ciascun certificato di CA subordinata incluso nel Mozilla Root Store, Actalis valorizza la sezione "Pertaining to Certificates Issued by This CA" del corrispondente record CCADB con il CRL Distribution Point della "Full CRL Issued By This CA" oppure con un JSON Array of Partitioned CRLs, entro e non oltre sette (7) giorni di calendario dalla prima emissione di un certificato TLS da parte della relativa CA intermedia.

Actalis mantiene nel CCADB i punti di contatto richiesti, inclusi almeno un contatto principale (Primary Point of Contact) e un alias di posta elettronica non personale, costantemente monitorato dal personale competente.

Actalis pubblica le versioni aggiornate dei documenti CP/CPS prima che le relative modifiche acquistino efficacia e trasmette al CCADB le informazioni aggiornate relative ai CP/CPS entro quattordici (14) giorni di calendario dalla loro pubblicazione.

Actalis trasmette e mantiene nel CCADB le informazioni richieste relative alle attestazioni di audit per i certificati di Root CA e di CA subordinate rientranti nell'ambito di applicazione delle policy dei Root Store Program, incluse, ove applicabili, le impronte digitali (fingerprint) dei certificati, gli standard di audit adottati, i periodi di audit, i documenti di policy, le date degli audit e le informazioni richieste in merito a incidenti o rilievi emersi nel corso degli audit.

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] ed [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 [BR]. Inoltre, per i certificati di classe EV, la CA svolge anche le ulteriori verifiche previste dalle [EVGL].

3.1 Regole di denominazione (naming)

3.1.1 Tipi di nomi

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

Nei certificati DV (Domain Validated), il campo *Subject* può non contenere alcun valore, in funzione delle modalità di presentazione della richiesta di certificato. In tale circostanza, l'estensione *Subject Alternative Name (SAN)* è impostata con l'attributo *critical*.

Inoltre, devono essere soddisfatti tutti i requisiti stabiliti in [BR] ed [EVGL].

In particolare, tutti i certificati TLS Server devono contenere uno o più elementi nell'estensione Subject Alternative Name (SAN), ciascun dei quali dev'essere un nome di dominio completo (FQDN) oppure un indirizzo IP. Nei certificati TLS Server DV (Domain Validated) ed EV (Extended Validation), tuttavia, non sono ammessi indirizzi IP.

3.1.2 Significatività dei nomi

Actalis inserisce nomi significativi nei campi Issuer e Subject dei certificati, con la possibile eccezione del campo Subject nei certificati DV come indicato in precedenza.

3.1.3 Anonimato e pseudonimia dei Titolari

Ad eccezione dei certificati TLS 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] ed [EVGL] del CAB Forum secondo la classe e il tipo del certificato.

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 coi requisiti del CAB Forum [BR] ed [EVGL] secondo la classe e il tipo del certificato.

Actalis normalmente consulta le seguenti fonti:

- per le organizzazioni private, il registro delle imprese pertinente per territorio o un'altra fonte equivalente di informazioni, privata o governativa, che soddisfi i requisiti del paragrafo 3.2.2.7;
- per gli enti pubblici, il pertinente indice o registro ufficiale degli enti pubblici applicabile territorialmente.

Nel caso in cui la consultazione delle fonti di cui sopra non sia possibile, o restituisca informazioni incomplete o obsolete sul Richiedente (es. identità e marchi registrati, indirizzo, numeri di telefono, referenti, ecc.), Actalis può accettare un documento di attestazione firmato da un avvocato, funzionario governativo o altra terza parte affidabile normalmente deputata a certificare tali informazioni nella giurisdizione del Richiedente. Unitamente a questo documento sarà necessario mettere a disposizione di Actalis anche la copia della licenza o documento comprovante il ruolo della terza parte. Queste informazioni devono essere redatte in lingua italiana o, se in una lingua diversa, devono essere redatti anche in inglese.

A discrezione di Actalis, secondo le circostanze, possono essere utilizzate anche altre fonti di informazione che soddisfano i requisiti del §3.2.2.7 al fine di corroborare le informazioni ottenute dalle fonti sopra indicate.

Per i certificati TLS Server EV, le fonti di informazioni approvate che possono essere utilizzate per validare l'identità del Richiedente sono quelle pubblicate sul sito web di Actalis al seguente indirizzo:
https://www.actalis.it/documenti-it/actalis-approved-incorporation-agencies.aspx.
L'elenco delle fonti utilizzate è monitorato ed aggiornato nel tempo dalla CA così da garantire il massimo standard di accuratezza e affidabilità delle informazioni ottenute.

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 altre 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] ed [EVGL].

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

- l'**esistenza fisica** del Richiedente (o di una sua affiliata) ai sensi del paragrafo 3.2.2.4 di [EVGL] mediante consultazione di registri nazionali affidabili, quali i registri delle imprese, dai quali siano ricavabili informazioni idonee a confermarne l'esistenza fisica;
- l'**esistenza operativa** del Richiedente (o di una sua affiliata) ai sensi del paragrafo 3.2.2.6 delle [EVGL].
- l'eventuale presenza del **Richiedente, del Contract Signer e del Certificate Approver, o delle relative giurisdizioni, in liste governative di soggetti sottoposti a sanzioni, restrizioni o analoghe liste di esclusione**, per maggiori dettagli si rimanda al par. 3.2.2.10. Tale verifica viene effettuata prima dell'emissione del certificato. In caso di corrispondenza, **la CA non procede all'emissione del certificato EV**.

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 in tutti i casi nei quali siano riscontrate situazioni problematiche (per es. procedure concorsuali, controversie, insolvenza, ecc.) a carico del Richiedente o del suo Rappresentante.

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 TLS Server DV), la CA verifica il diritto del Richiedente di utilizzare tale DBA o nome depositato mediante consultazione di registri affidabili, quali quelli gestiti da WIPO, EUIPO o dalle competenti autorità nazionali, nel rispetto dei metodi previsti nei [BR] e negli [EVGL], secondo la classe e il tipo del certificato.

3.2.2.3 Verifica del paese (country)

Quando il campo Subject del certificato deve includere un codice paese (non applicabile ai certificati TLS Server di classe DV), la CA verifica il paese utilizzando uno dei metodi previsti nel paragrafo 3.2.2.3 dei [BR], ovvero tramite registri autoritativi nazionali o internazionali.

3.2.2.4 Verifica della proprietà o del controllo del dominio

Prima di emettere un certificato **TLS 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 come descritto di seguito.

Anzitutto, Actalis sceglie un appropriato Authorization Domain Name (ADN) secondo il processo previsto dal §3.2.2.4 dei [BR], partendo dal FQDN o dal nome di dominio wildcard richiesto e selezionando un metodo di validazione compatibile con il tipo di nome. Successivamente, Actalis esegue la validazione di quell'ADN con uno dei seguenti metodi:

- La CA conferma, interrogando direttamente il Domain Name Registrar, che il Richiedente è 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). Questo metodo è implementato in conformità al §3.2.2.4.12 dei [BR].

- La CA invia un valore casuale via e-mail a un indirizzo ottenuto concatenando "admin@" o "administrator@" o "webmaster@" o "hostmaster@" o "postmaster@" allo ADN e riceve una risposta di conferma basata sullo stesso valore casuale. Questo metodo è implementato in conformità al §3.2.2.4.4 dei [BR].
- La CA chiede al Richiedente di pubblicare un file sul server HTTP allo ADN 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. Questo metodo non può essere utilizzato per domini di tipo wildcard e non copre i sottodomini del dominio validato. Questo metodo è implementato in conformità al §3.2.2.4.18 dei [BR].
- La CA chiede al Richiedente di pubblicare un file sul server HTTP allo ADN in esame, sotto la directory "/.well-known/acme-challenge", nel rispetto del §8.3 della RFC8555 [ACME], contenente il valore fornito dalla CA, quindi verifica la presenza di tale file, con il contenuto previsto. Questo metodo non può essere utilizzato per domini di tipo wildcard e non copre i sottodomini del dominio validato. Questo metodo è implementato in conformità al §3.2.2.4.19 dei [BR].
- La CA chiede al Richiedente di inserire un record TXT, contenente un valore casuale fornito dalla CA, nelle informazioni DNS dello ADN, quindi verifica la presenza di tale record con il contenuto previsto. Questo metodo è implementato in conformità al §3.2.2.4.7 dei [BR].
- La CA verifica la presenza, sullo ADN, di un record TXT di DCV di tipo Persistente che identifica il Richiedente (Applicant). Il record dev'essere inserito in corrispondenza della label "validation-persist" anteposta all'ADN oggetto di convalida. Questo metodo è implementato in conformità al §3.2.2.4.22 dei [BR].

In tutti i casi, la validazione del controllo del dominio (Domain Control Validation – DCV) è effettuata nel pieno rispetto del § 3.2.2.4 dei [BR] e Actalis non utilizza metodi di DCV diversi da quelli espressamente consentiti dai [BR]. Nell'ambito del processo di DCV, Actalis esegue inoltre la validazione DNSSEC fino alla trust anchor DNSSEC della root IANA, utilizzando resolver DNS che implementano la validazione DNSSEC in conformità alla Sezione 5 della RFC 4035, supportano NSEC3 secondo quanto previsto dalla RFC 5155, supportano gli algoritmi SHA-2 conformemente alle RFC 4509 e RFC 5702 e rispettano le considerazioni di sicurezza descritte nella Sezione 4 della RFC 6840, come richiesto dal § 3.2.2.4 dei [BR].

Lo specifico metodo di Domain Control Validation (DCV) utilizzato per ciascun FQDN o dominio wildcard dipende dalle circostanze del caso concreto e dalle preferenze del richiedente il certificato. L'insieme dei metodi di DCV supportati può inoltre variare in funzione del canale utilizzato per la richiesta del certificato. Per i metodi di validazione del dominio basati sulla posta elettronica, descritti ai §§ 3.2.2.4.4, Actalis esegue la validazione DNSSEC fino alla trust anchor DNSSEC della root IANA su tutte le interrogazioni DNS di tipo CNAME, CAA e TXT utilizzate per determinare l'Authorization Domain Name e non applica policy locali che disabilitino la validazione DNSSEC. Per tutti gli altri metodi di validazione del dominio, Actalis esegue la validazione DNSSEC fino alla trust anchor DNSSEC della root IANA su tutte le interrogazioni DNS associate alla verifica dell'autorizzazione o del controllo del dominio e non applica policy locali che disabilitino la validazione DNSSEC per tali interrogazioni.

3.2.2.5 Autenticazione degli indirizzi IP

Prima di emettere un certificato TLS 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) così come descritto nella sezione 3.2.2.5.1 dei [BR]. A tal fine, il Richiedente dimostra il controllo dell'indirizzo IP pubblicando sul server HTTP raggiungibile a tale indirizzo, nella directory *"/.well-known/pki-validation",* un file contenente un valore casuale fornito dalla CA, che ne verifica la presenza e la corrispondenza del contenuto al valore previsto.

3.2.2.6 Validazione dei domini wildcard

Prima di emettere un certificato **TLS 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-8659 e nel par. 3.2.2.8 dei [BR]. Le CA non rilascerà il certificato a meno che la richiesta di certificato sia coerente con l'insieme dei record CAA applicabili. Il dominio identificativo di Actalis nei record CAA è "**actalis.it**".

3.2.2.9 Multi-Perspective Issuance Corroboration

Al fine di rafforzare la protezione contro attacchi o dirottamenti del Border Gateway Protocol (BGP), Actalis implementa il meccanismo di *Multi-Perspective Issuance Corroboration* (MPIC) per la Domain Control Validation (DCV) e per la verifica dei record CAA, in conformità al § 3.2.2.9 dei [BR].

In particolare, Actalis utilizza 5 (cinque) prospettive di rete remote dispiegate nelle seguenti regioni geografiche:

- *eu-central*
- *eu-west*
- *us-east*
- *ap-northeast*
- *ap-southeast*

Queste prospettive di rete sono indipendenti dalla prospettiva primaria operante presso il data center di Actalis.

L'emissione del certificato può procedere solo quando il risultato della validazione con MPIC soddisfa un quorum di almeno 4 (quattro) prospettive di rete. Se il quorum richiesto non viene raggiunto, Actalis non emette il certificato e ritorna al richiedente un errore interattivo o applicativo secondo il canale di richiesta.

La MPIC viene applicata ai metodi di validazione del dominio descritti nel § 3.2.2.4 del presente CP/CPS e alle verifiche dei record CAA, nei casi e secondo le modalità previsti dal § 3.2.2.9 dei [BR].

3.2.2.10 Liste di esclusione

Prima di autorizzare il rilascio di un certificato TLS Server di classe EV, Actalis verifica il Richiedente, il Firmatario del contratto (**Contract Signer**), il Responsabile dell'approvazione del certificato (**Certificate Approver**), nonché la giurisdizione di costituzione o registrazione e il luogo di attività del Richiedente, rispetto alle liste governative di soggetti sottoposti a divieti o restrizioni, alle liste di persone o entità proibite, alle altre liste di blocco previste dalla normativa e ai regimi sanzionatori applicabili[3], anche secondari.

[3] A titolo esemplificativo e non esaustivo, la Certification Authority consulta le liste sanzionatorie pubblicate dall'OFAC e dall'Unione europea, anche tramite servizi di aggregazione forniti da operatori specializzati, ad es. o*penSanctions.*

La verifica è effettuata consultando liste autoritative nelle giurisdizioni dell'Unione Europea e degli USA o altre liste ritenute affidabili da Actalis. Tali verifiche sono opportunamente registrate per garantire la piena tracciabilità ex-post delle azioni eseguite.

Qualora il Richiedente, il Contract Signer o il Certificate Approver siano presenti in una o più liste sanzionatorie, Actalis non blocca l'emissione del certificato.

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:

- 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 i [BR] o [EVGL], secondo la classe e il tipo del 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 inviata alla CA tramite un servizio di Posta Elettronica Certificata[4] (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 3.2.2.8 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] ed [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.

[4] 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 delle Condizioni Generali della CA;
- 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.

L'ordine e la modalità con cui vengono eseguiti questi passaggi possono variare secondo il canale di richiesta, ma tutti i passaggi 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 TLS server DV e OV, 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 TLS 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 EV – vedere più avanti)

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.

La richiesta del certificato avviene normalmente mediante sottomissione di un modulo on-line (web form) sul portale della CA stessa oppure sul portale di un Rivenditore. Nei casi particolari in cui questa modalità non può essere seguita, è possibile trasmettere alla CA (per es. via email) un modulo di richiesta off-line (reperibile sul portale della CA).

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 TLS Server, gli FQDN e/o indirizzi IP da includere nel certificato;
- (eccetto per i certificati TLS 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 delle Condizioni Generali della CA che richiamano questo CPS mediante riferimento. A seconda della classe del certificato e della particolare procedura o canale di richiesta, il Richiedente può accettare tali condizioni 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 apposito Accordo (EV) firmato da un idoneo Contract Signer, ai sensi delle [EVGL]. L'Accordo EV dev'essere firmato in uno dei seguenti modi:

- mediante firma autografa apposta in presenza di un rappresentante Actalis (che controfirma come testimone, dopo aver verificato l'identità del firmatario esaminando un valido documento d'identità dello stesso e conservandone scansione);
- mediante firma autografa accompagnata dalla scansione di un documento d'identità del firmatario in corso di validità; in questo caso, il documento firmato in originale e la scansione del documento d'identità devono essere anticipati ad Actalis per e-mail, da un dominio di posta sotto il controllo del Richiedente, quindi spediti ad Actalis, per posta, entro 30 giorni dall'emissione del certificato;
- mediante firma autografa autenticata da un notaio o da un'altra persona che, ai sensi delle norme vigenti nella giurisdizione del Richiedente, abbia l'autorità per autenticare una firma (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 EV 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 EV, 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 EV (e le 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.

4.1.2.1 Supporto del protocollo ACME

Actalis supporta inoltre il protocollo di automazione ACME, in conformità alla RFC 8555. Il server ACME di Actalis è accessibile al seguente indirizzo: https://acme-api.actalis.com/acme/directory.

In linea generale, tramite ACME è possibile richiedere qualsiasi tipologia di certificato TLS (DV, OV ed EV) emesso da Actalis, fermo restando che possono applicarsi limitazioni in funzione della tipologia di account del cliente (ad esempio, retail o corporate).

L'accesso al servizio ACME di Actalis richiede credenziali di External Account Binding (EAB), fornite al momento dell'onboarding del cliente ovvero rese disponibili in modalità self-service, in funzione del portale di gestione dei certificati utilizzato dal Subscriber.

Attualmente, per i certificati richiesti mediante ACME sono supportate le challenge di tipo "http-01", "dns- 01", e "dns-persist-01".

Sono inoltre supportate le seguenti funzionalità aggiuntive del protocollo ACME:

1. record CAA con gli attributi accounturi e validationmethods, conformemente alla RFC 8657;
2. ACME Renewal Information (ARI), in conformità alla RFC 9773.

Per ciascun Object Identifier (OID) di Certificate Policy previsto dai TLS Baseline Requirements del CA/Browser Forum per il quale Actalis offre un processo di emissione automatizzato, Actalis pubblica nel CCADB le informazioni relative alla soluzione di automazione adottata. Qualora il protocollo ACME sia supportato per il relativo Certificate Policy OID, Actalis pubblica nel CCADB anche il corrispondente endpoint della directory ACME.

Per i Certificate Policy OID dei TLS Baseline Requirements applicabili, Actalis mantiene Automation Test Certificates al fine di dimostrare le proprie capacità di automazione. Tali certificati sono rinnovati almeno ogni trenta (30) giorni di calendario e almeno un Automation Test Certificate valido è reso disponibile mediante un URL pubblicamente accessibile, pubblicato nel CCADB nel record della corrispondente Certification Authority intermedia.

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 e il tipo del certificato, in conformità con [BR] ed [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] ed [EVGL] secondo la classe e il tipo 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.

La CA controlla inoltre i record CAA pertinenti (se presenti) secondo il paragrafo 3.2.2.8. L'identificativo di dominio da utilizzarsi nei record CAA per autorizzare la CA di Actalis è "actalis.it".

Per i certificati EV TLS 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 3.2.2.13 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. Nel trattamento dei record CAA, Actalis elabora i parametri *accounturi* e *validationmethods* conformemente a quanto specificato nella RFC 8657.

L'accettazione delle richieste è inoltre subordinata ai seguenti criteri:

- Non saranno emessi certificati contenenti "internal names" o indirizzi IP riservati.
- 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.
- Non saranno emessi certificati che contengano "Domain Names" che terminano con "IP Reverse Zone Suffix", come definiti in [BR];
- Actalis mantiene un elenco di domini ad alto rischio di phishing. Le richieste di certificati contenenti tali domini sono sospese in attesa di verifiche aggiuntive, nell'ambito delle quali al Richiedente è richiesto di fornire ulteriori informazioni a conferma del proprio effettivo diritto di utilizzare i domini interessati. L'emissione è consentita esclusivamente a seguito dell'esito positivo di tali verifiche; in caso contrario, la richiesta è respinta.

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);
- esegue un linting del *tbsCertificate*, per mezzo di linters ampiamente adottati dall'industria del settore, al fine di minimizzare il rischio di emissione errate;
- controlla i record CAA pertinenti (se presenti) secondo il paragrafo 3.2.2.8 dei [BR].

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

- invia al Titolare un'e-mail contenente il certificato del Sottoscrittore (o un link a esso) e la relativa catena di certificazione (o un link a essa);
- e/o rende il certificato disponibile al Titolare sul portale web tramite il quale è stato richiesto il certificato;
- e/o rende il certificato disponibile al Titolare o al Rivenditore tramite le API applicabili, a seconda del canale di richiesta.

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

Tutti i certificati TLS Server rilasciati devono essere conformi ai requisiti di Certificate Transparency applicabile 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 alle CT Policies dei Browser vendor applicabili (Google, Mozilla, Microsoft e Apple)). 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).

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 TLS 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

4.5.1 Uso della chiave privata e del certificato da parte del titolare

Il Subscriber utilizza la chiave privata per abilitare il protocollo TLS/SSL sui propri server, consentendo l'autenticazione del server TLS e la cifratura delle sessioni di comunicazione con i client.

4.5.2 Uso della chiave pubblica e del certificato da parte delle Relying Part

Le Relying Party utilizzano il certificato per verificare l'identità del server e, in funzione della tipologia del certificato, anche dell'organizzazione che ne detiene il controllo, nonché per stabilire in modo sicuro la chiave di sessione (*session key*) con il server.

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).

4.7.1 Circostanze per il re-key del certificato

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.

4.7.2 Chi può richiedere il re-key della chiave pubblica

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

4.7.3 Elaborazione delle richieste di re-key

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.

4.7.4 Notifica al Titolare del rilascio del nuovo certificato

Si applica quanto descritto nel §4.3.2.

4.7.5 Comportamenti che costituiscono l'accettazione dei un certificato re-key

Si applica quanto descritto nel §4.4.1.

4.7.6 Distribuzione del nuovo certificato da parte della CA

Si applica quanto descritto nel §4.4.2.

4.7.7 Notifica ad altri soggetti della nuova emissione del certificato

Si applica quanto descritto nel §4.4.3.

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.

4.8.1 Circostanze per la modifica del certificato

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.

4.8.2 Chi può richiedere la modifica del certificato

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

4.8.3 Elaborazione delle richieste di modifica del certificato

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

4.8.4 Notifica al titolare dell'emissione del rilascio del nuovo certificato

Si applica quanto descritto nel §4.3.2.

4.8.5 Comportamenti che costituiscono l'accettazione del nuovo certificato

Si applica quanto descritto nel §4.4.1.

4.8.6 Pubblicazione del certificato modificato da parte della CA

Si applica quanto descritto nel §4.4.2.

4.8.7 Notifica ad altri soggetti della nuova emissione del certificato

Si applica quanto descritto nel §4.4.3.

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:

1. richiesta esplicita di revoca da parte del Titolare;
2. il Titolare informa la CA che la richiesta del certificato non era stata autorizzata, e non intende autorizzarla retroattivamente (CRLReason #9, *privilegeWithdrawn*);
3. la CA scopre che la chiave privata del Titolare corrispondente al certificato è compromessa (CRLReason #1, *keyCompromise*);
4. la CA ottiene evidenza di un metodo dimostrato o comprovato in grado di ricavare agevolmente la chiave privata del Titolare a partire dai dati della corrispondente chiave pubblica contenuti nel certificato (CRLReason #1, *keyCompromise*);
5. la CA ottiene evidenza che la verifica dell'autorizzazione o del controllo del dominio relativa a uno qualsiasi dei FQDN o degli indirizzi IP contenuti nel certificato non possa essere considerata affidabile, inclusi i casi in cui la CA non abbia eseguito correttamente il controllo CAA o in cui l'emissione non fosse permessa (CRLReason #4, *superseded*).;

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

6. il certificato non rispetta più i requisiti previsti dai paragrafi 6.1.5 e 6.1.6 dei [BR] o di altri obblighi previsti dalle policy e dagli standard applicabili (CRLReason #4, *superseded*);
7. la CA scopre che il certificato viene usato in modo improprio e/o illecito (CRLReason #9, *privilegeWithdrawn*);

8. la CA scopre che il Titolare ha violato una o più delle disposizioni delle Condizioni Generali del servizio (CRLReason #9, *privilegeWithdrawn*);
9. 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 o di sanzioni nazionali e/o internazionali, ecc.) (CRLReason #5, *cessationOfOperation*);
10. la CA scopre che un certificato di tipo wildcard viene usato per autenticare un FQDN subordinato in modo fraudolento (CRLReason #9, *privilegeWithdrawn*);
11. la CA scopre che una o più delle informazioni contenute nel certificato ha subito variazioni (per es. è cambiata la denominazione dell'organizzazione Titolare) (CRLReason #9, *privilegeWithdrawn*);
12. 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 (CRLReason #4, *superseded*);
13. 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) (CRLReason #9, *privilegeWithdrawn*);
14. 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 (CRLReason omessa);
15. la CA ottiene evidenza di una procedura che espone la chiave privata del Titolare alla compromissione oppure la CA scopre che la procedura di generazione chiavi usata dal Titolare è gravemente difettosa e insicura) (CRLReason omessa);
16. accertata compromissione della chiave privata della CA emittente (Subordinate CA) (CRLReason #1, *keyCompromise*);
17. inadempienze contrattuali da parte del cliente (es. mancato pagamento del certificato) (CRLReason #9, *privilegeWithdrawn*);
18. provvedimento dell'autorità giudiziaria (CRLReason #9, *privilegeWithdrawn*).

Qualora venga richiesto un certificato di tipologia EV, tramite firma autografa, la CA potrà revocare il certificato per le seguenti circostanze:

- mancato invio, entro 30 giorni dall'emissione del certificato, della documentazione in originale unita alla scansione del documento di identità del firmatario in corso di validità;
- non coerenza della documentazione in originale rispetto alla copia anticipata via e-mail.

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 revocherà un certificato di SubCA **entro 7 giorni** se si verifica uno o più delle seguenti circostanze:

1. la SubCA richiede per iscritto la revoca del certificato;
2. la SubCA comunica ad Actalis che la richiesta originaria del certificato di SubCA non era stata autorizzata e non concede tale autorizzazione con effetto retroattivo;

3. Actalis ottiene evidenza che la chiave privata della SubCA, corrispondente alla chiave pubblica contenuta nel certificato, sia stata compromessa o non soddisfi più i requisiti di sicurezza previsti dai paragrafi 6.1.5 e 6.1.6;
4. Actalis ottiene evidenza del fatto che il certificato della SubCA è stato utilizzato impropriamente;
5. Actalis viene a conoscenza del fatto che il certificato della SubCA non è stato emesso conformemente ai Baseline Requirements del CA/Browser Forum e agli altri requisiti applicabili, compreso il presente CP\CPS;
6. Actalis accerta che una qualsiasi delle informazioni contenute nel certificato di SubCA è inesatta o fuorviante;
7. Actalis o la SubCA cessa le proprie attività, per qualsiasi motivo, senza aver adottato misure per garantire la continuità del servizio di revoca del certificato;
8. il diritto di Actalis o SubCA di emettere Certificati ai sensi dei Baseline Requirements e degli altri requisiti normativi applicabili scade, viene revocato o cessa totalmente, salvo che la Actalis abbia già adottato misure idonee a garantire la continuità della gestione del repository CRL/OCSP;
9. la revoca è richiesta dalla CP o dal CPS applicabile di Actalis.

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 (secondo le circostanze descritte al cap. 4.9.1 e secondo le modalità descritte al cap. 1.5.2).

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 di un certificato (così come descritto al cap. 1.5.2), l'indagine sul presunto problema inizierà entro 24 ore dalla ricezione della segnalazione. Se la revoca è necessaria, essa sarà effettuata entro i tempi massimi previsti secondo il caso (vedere il paragrafo 4.9.1.1).

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

La CA supporta le richieste OCSP effettuate col metodo GET, per tutti i certificati e i precertificati a cui è stato assegnato un seriale. Il servizio OCSP è disponibile a partire da 15 minuti dall'assegnazione del seriale.

Le risposte OCSP relative ai certificati del risponditore presentano un intervallo di validità pari o superiore a otto ore e pari ed inferiore a dieci giorni.

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 o su un precertificato a cui non è stato assegnato un seriale.

La CA aggiorna le informazioni fornite tramite OCSP in conformità con [BR].

4.9.10 Requisiti dei servizi on-line di verifica revoca

Si rimanda ai paragrafi 4.10 e 7.3.

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

Nessun requisito particolare nel caso di compromissione della chiave rilevata dal Titolare del certificato. In tal caso, si rammenta l'obbligo del Titolare di richiedere prontamente ad Actalis la revoca del proprio certificato (vedere la sezione 9.6.3).

Soggetti *diversi* dal Titolare possono segnalare la compromissione della chiave di un certificato Actalis (non scaduto e non revocato) utilizzando uno dei seguenti metodi per dimostrare di avere il possesso o controllo della chiave privata in questione:

- Creare un file di testo contenente la frase “Questa chiave è compromessa” (o una frase analoga), quindi firmare il file con la chiave privata che si vuole segnalare come compromessa ed inviare il file firmato ad Actalis (§).
- Creare, con la chiave privata che si vuole segnalare come compromessa, una CSR che include nel commonName il testo “Questa chiave è compromessa” (o una frase analoga), quindi inviare la CSR ad Actalis (§).
- Inviare ad Actalis (§) I riferimenti a fonti di informazioni su vulnerabilità e/o incidenti di sicurezza che consentono di verificare la compromissione.

(§) Inviare a cert-problem@actalis.it specificando come oggetto “Compromissione chiave”.

Actalis può consentire, a propria discrezione, anche altri metodi per dimostrare di avere il possesso o controllo di una chiave privata.

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 protocollo HTTP secondo la specifica [RFC2616]

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

La CRL viene rigenerata integralmente e ripubblicata:

- almeno ogni 6 ore, anche in assenza di nuove revoche;
- entro 24 ore 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;

- entro 24 ore 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 propria 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 sono distribuiti sul territorio italiano.

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;
- **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 elettrica** ridondati a tutti i livelli a garanzia della continuità dell'alimentazione elettrica in ogni condizione prevedibile;
- sistemi di **ventilazione** e di **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.
I supporti sono custoditi in ambienti sicuri e protetti da accessi non autorizzati, anche durante lo stoccaggio temporaneo precedente allo smaltimento. In caso di riutilizzo o dismissione, sono previste operazioni di cancellazione sicura dei dati e/o distruzione fisica, secondo la tipologia e lo stato del supporto, per impedirne il recupero da parte di soggetti non autorizzati. Le attività sono tracciate e il relativo esito è documentato; gli eventuali trasferimenti dei supporti sono autorizzati e soggetti a specifiche misure di sicurezza

5.1.7 Smaltimento dei rifiuti

La CA gestisce lo smaltimento dei rifiuti nel rispetto della normativa vigente, con particolare attenzione ai rifiuti di apparecchiature elettriche ed elettroniche (RAEE). Per le attività svolte presso i data center Aruba, si applicano inoltre le procedure del sistema di gestione ambientale certificato secondo la norma ISO 14001.

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.
Inoltre, Actalis ha definito un inventario degli asset (Hardware e Software) come quanto previsto dalla policy e dalla procedura aziendale.

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 per mezzo di accesso controllato.

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 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, mediante strutture dedicate, 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, mediante strutture dedicate, 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, attività rilevanti su router e firewall, in particolare riguardo le configurazioni di quest'ultimo 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.

I penetration test sono eseguiti almeno annualmente e a seguito di modifiche infrastrutturali o applicative definite come significative. Sono condotti da specialisti qualificati in sicurezza informatica appartenenti a una società del Gruppo dedicata alla cybersecurity, indipendenti dal personale responsabile dei sistemi sottoposti a test e in possesso di competenze adeguate e qualifiche riconosciute a livello internazionale (ad esempio, OSCP, OSCE, eCPPT, CEH o equivalenti).

Le vulnerabilità individuate mediante valutazioni delle vulnerabilità, penetration test o altri mezzi sono esaminate, gestite e risolte in funzione della loro gravità e del rischio associato, entro i seguenti tempi massimi di risoluzione, che comprendono le fasi di identificazione, analisi, risposta e rimedio:

Gravità	Tempo massimo di risoluzione
Critica	5 giorni
Alta	30 giorni
Media	3 mesi
Bassa	1 anno

Il termine applicabile è determinato sulla base di un'analisi documentata dei rischi e della sicurezza che considera, ove pertinente: la criticità degli asset; la riservatezza, l'integrità e la disponibilità; i requisiti normativi; la probabilità e l'impatto dello sfruttamento delle vulnerabilità; le dipendenze; le risorse disponibili per la risoluzione; i dati storici; e l'attuale panorama delle minacce

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.

5.5.2 Periodo di conservazione degli archivi

Gli archivi sono conservati per almeno 10 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)

Nessuna stipula.

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

Actalis mantiene un piano di gestione del ciclo di vita e di successione delle Root CA utilizzate per l'emissione di certificati TLS Server pubblicamente trusted. Tale piano tiene conto dei requisiti applicabili dei Root Store Program in materia di età del materiale crittografico delle Root CA, gerarchie PKI dedicate a uno specifico scopo, inclusione delle Root CA sostitutive, cross-certification, transizione delle emissioni verso gerarchie sostitutive e progressiva dismissione o rimozione della fiducia (trust) dalle gerarchie di Root CA legacy.

Per l'emissione di certificati TLS Server destinati a essere pubblicamente trusted, Actalis provvede a trasferire progressivamente le emissioni dalle gerarchie di Root CA legacy o multiuso verso gerarchie dedicate all'autenticazione TLS Server, in conformità alle policy applicabili dei Root Store Program, alle informazioni pubblicate nel CCADB e agli eventuali piani di transizione o di inclusione delle Root CA approvati. Actalis non farà affidamento sulle gerarchie di Root CA legacy o multiuso oltre i limiti del relativo ciclo di vita previsti dai Root Store Program applicabili, salvo nei casi espressamente consentiti dal relativo Root Store Program

5.6.2 CA subordinata

Almeno una volta, prima della scadenza della validità della chiave di certificazione in uso (chiave della Certification Authority subordinata – Subordinate CA), viene generata una nuova coppia di chiavi e il corrispondente certificato viene reso disponibile ai Subscriber e alle Relying Party secondo le modalità descritte nella Sezione 6.1.4. A decorrere da tale momento, i certificati dei Subscriber e le relative CRL sono sottoscritti mediante la nuova chiave della Subordinate CA.

I nuovi certificati delle Subordinate CA hanno un periodo massimo di validità pari a tre (3) anni[5].

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.

Actalis rende pubblici gli incidenti e/o risponde alle relative segnalazioni mediante Bugzilla (https://bugzilla.mozilla.org/), indipendentemente dall'impatto percepito dell'incidente. Le segnalazioni sono presentate in conformità alla versione vigente del formato e delle tempistiche di incident reporting previste dal CCADB.

Actalis risponde alle richieste di informazioni integrative formulate dai Root Store Program entro i termini previsti dalle rispettive policy applicabili, incluso il termine di quattordici (14) giorni di calendario previsto dal Chrome Root Program, salvo che sia espressamente stabilito un diverso termine.

Qualora Actalis non sia in grado di completare entro i termini prescritti un'azione di follow-up conseguente a un incidente, inclusa la revoca di certificati, provvede a presentare una segnalazione di incidente secondaria (secondary incident report), contenente l'indicazione dei certificati interessati, della tempistica prevista per il completamento delle attività e delle azioni correttive adottate per garantire la conformità in futuro.

[5] A partire dal mese di Giugno 2026.

Laddove richiesto dalle policy di un Root Store Program, Actalis fornisce preventiva comunicazione in caso di acquisizioni, cessioni, modifiche della proprietà o del controllo operativo, cessazione delle attività, modifiche ai soggetti terzi delegati, variazioni delle sedi operative o altri eventi di change management suscettibili di incidere in modo significativo sull'operatività o sull'affidabilità percepita di una Root CA inclusa nei Root Store.

La gestione delle situazioni di emergenza è disciplinata dal Business Continuity Plan (BCP) di Actalis, che copre tutti gli aspetti previsti dal paragrafo 5.7.1 dei [BR]. Si rinvia altresì alla Sezione 5.1 del presente documento.

Actalis si impegna inoltre a mantenere un piano completo e concretamente attuabile per la gestione degli eventi di revoca massiva (mass revocation), effettuandone almeno una verifica annuale e recependo le lezioni apprese al fine di migliorare costantemente il proprio livello di preparazione, in conformità al paragrafo 5.7.1.2 dei [BR].

Actalis mantiene un piano operativo completo per la gestione della revoca massiva dei certificati e ne verifica l'efficacia almeno una volta all'anno. Le esperienze maturate nel corso delle esercitazioni e degli eventi reali di revoca sono integrate nelle procedure operative al fine di migliorarne continuamente l'efficacia.

Actalis informa proattivamente i Subscriber in merito ai termini applicabili per la revoca dei certificati e ai rischi derivanti dall'utilizzo di certificati TLS pubblicamente trusted in contesti nei quali non sia possibile procedere tempestivamente alla loro sostituzione. Attraverso il Subscriber Agreement o le Condizioni Generali di Servizio applicabili, Actalis richiede ai Subscriber di collaborare tempestivamente affinché possa adempiere agli obblighi di revoca previsti dai requisiti del CA/Browser Forum e dalle policy applicabili dei Root Store Program.

Qualora Actalis accerti che una revoca ritardata si renda necessaria ovvero sia effettivamente intervenuta, gestisce e comunica tale circostanza in conformità alle CCADB Incident Reporting Guidelines applicabili e alle policy dei Root Store Program interessati.

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, primario e secondario. 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:

1. 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;
2. 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;
3. 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;
4. 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 il tempo previsto dalla regolamentazione vigente, compresa quella dello Stato Italiano. Sarà inoltre trasferita a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della CA cessata;
5. sarà pianificata la distruzione delle chiavi private di certificazione nonché del materiale crittografico annesso che ne consente il ripristino.

Alla data di cessazione:

6. 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 che ricoprono ruoli di fiducia nel rispetto dei principi di "*dual control*" e "*split knowledge*". 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) e di un auditor qualificato come testimone terzo indipendente; l'attività è tracciata in un verbale conservato sotto la responsabilità del Responsabile del Servizio di Certificazione della CA.

6.1.1.2 Generazione chiavi della RA

Nessuna stipula.

6.1.1.3 Generazione chiavi del Titolare

Per i certificati TLS, le coppie di chiavi dei Titolari devono essere generate dai Titolari stessi se non diversamente concordato.

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/TLSkeys) oppure qualora la chiave risulti vulnerabile agli attacchi ROCA (https://github.com/crocs-muni/roca) o Close Primes (https://fermatattack.secvuln.info/).

6.1.2 Consegna della chiave privata al titolare

Vedere il par. 6.1.1.3.

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 o chiavi ellittiche ECSDA con modulo di 384 bit.

Le CA subordinate (ossia le CA emittenti) devono utilizzare una coppia di chiavi RSA con una dimensione del modulo di almeno 2048 bit, o in alternativa chiavi ellittiche ECSDA con modulo di almeno 256 bit .

Le chiavi dei Titolari devono essere:

- chiavi RSA con una dimensione del modulo di almeno 2048 bit (fino a 4096);
- oppure chiavi ECC di tipo NIST P-256 oppure P-384.

6.1.6 Generazione dei parametri e qualità delle chiavi

Actalis verifica che le chiavi pubbliche soddisfino i requisiti indicati nel paragrafo 6.1.6 dei [BR].
In particolare, nel caso di chiavi RSA, Actalis svolge le seguenti verifiche secondo la norma NIST SP 800-89:

- il valore dell'esponente pubblico sia un numero dispari pari o superiore a 3;
- l'esponente pubblico sia compreso tra 2^16 + 1 e 2^256 – 1;
- il modulo sia un numero dispari, non una potenza di un numero primo e che non abbia fattori inferiori a 752.

Per le chiavi ECDSA, Actalis verifica la validità delle chiavi utilizzando la procedura di convalida completa della chiave pubblica ECC o la procedura di convalida parziale della chiave pubblica ECC secondo la norma NIST SP 800-56A: Revision 2.

6.1.7 Key Usage (estensione X.509 v3)

Le chiavi private delle Root CA afferenti alla Certification Authority Actalis sono utilizzate esclusivamente per la sottoscrizione di:

1. Certificati autofirmati rappresentativi della Root CA stessa;
2. Certificati di SubCA e cross-certificati;
3. Certificati per finalità infrastrutturali, quali certificati associati a ruoli amministrativi e certificati dei dispositivi utilizzati internamente per l'operatività della CA;
4. Certificati destinati alla verifica delle risposte OCSP;
5. Certificate Revocation List (CRL).

6.2 Protezione della chiave privata e sicurezza dei moduli crittografici

6.2.1 Requisiti di sicurezza dei moduli crittografici

Tutte le chiavi di CA (sia Root CA che CA emittenti) sono generate, conservate ed usate all'interno di HSM dotati di certificazione di sicurezza secondo le norme FIPS PUB 140-2 a Livello 3 (o superiore), FIPS PUB 140-3 Livello 3 (o superiore) 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 delle CA sono memorizzate e protette all'interno di HSM dotati di certificazione di cui al paragrafo 6.2.1 del presente documento.

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
Actalis Authentication Root CA	18 anni	20 anni
Subordinate CA	13 anni	15 anni
Root CA emesse nel corso del 2025	15 anni	25 anni
Subordinate emesse nel corso del 2025	Nessuna stipula	10 anni
Cross certificates	Nessuna stipula	5 anni
Subscriber – DV TLS Server	Nessuna stipula	Massimo 200 giorni
Subscriber – OV TLS Server	Nessuna stipula	Massimo 200 giorni
Subscriber – EV TLS Server	Nessuna stipula	Massimo 200 giorni

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 antimalware al fine di mitigare il rischio di “infezioni” ed attacchi di sicurezza. . Le vulnerabilità identificate sono esaminate, gestite e risolte, anche mediante l’installazione delle patch di sicurezza raccomandate, entro i tempi massimi definiti nel paragrafo 5.4.8. Tali tempi comprendono le fasi di identificazione, analisi, risposta e rimedio e sono determinati in funzione della gravità e del rischio associato, sulla base dell’analisi documentata dei rischi e della sicurezza e dei criteri di valutazione descritti nel medesimo paragrafo.

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.
Per i sistemi software forniti da terze parti per lo svolgimento delle proprie attività di CA, Actalis prevede un monitoraggio continuo del versioning e dell’upgrade del software al fine di garantire la massima qualità dei servizi offerti.

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.

I sistemi di Root CA si trovano su reti fisicamente separate da tutte le altre infrastrutture CA.

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

Le vulnerabilità identificate sono esaminate, gestite e risolte nel rispetto dei tempi massimi di risoluzione definiti nella sezione 5.4.8, sulla base della valutazione del rischio.

Actalis rispetta inoltre quanto richiesto dai “Network and Certificate System Security Requirements” pubblicati su https://cabforum.org/working-groups/netsec/.

6.8 Time-stamping

Il riferimento temporale utilizzato da Actalis si basa su molteplici sorgenti GPS di livello *Stratum 1*, al fine di garantire un riferimento orario affidabile e ridondato. I sistemi coinvolti nei servizi di certificazione sono configurati per sincronizzarsi automaticamente e continuativamente con tali sorgenti temporali.

L’orario di sistema viene sottoposto a verifiche e a monitoraggio continuo mediante confronto con i riferimenti temporali previsti e con i riferimenti temporali esterni indipendenti al fine di verificare la correttezza del riferimento adottato e rilevare eventuali scostamenti anomali o fuori soglia.

L’infrastruttura è configurata per mantenere un’accuratezza temporale inferiore a un secondo rispetto al riferimento adottato.

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 [BR] o [EVGL] del CAB Forum, secondo la classe e il tipo del certificato.

7.1.2.1 Certificati delle Root CA

I certificati delle Root CA hanno i profili descritti di seguito.

7.1.2.1.1 Gerarchia legacy

Di seguito il profilo del certificato della Root CA *multi-purpose:*

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>

7.1.2.1.2 Nuove gerarchie

Di seguito i profili dei certificati della Root CA *single-purpose:*

Nel caso di chiavi RSA

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	sha512WithRSAEncryption (1.2.840.113549.1.1.13)
Issuer	<Stesso valore del Subject>
Validity	<25 anni>
Subject	CN = Actalis <scopo> Root CA <anno> O = Actalis S.p.A. L = Milano C = IT
SubjectPublicKeyInfo	<Chiave pubblica RSA da 4096 bit>
SignatureValue	<Firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<SHA1- della chiave pubblica>
SubjectKeyIdentifier (SKI)	<SHA1- della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<assente>
CertificatePolicies	<assente>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<assente>
CRLDistributionPoints (CDP)	<assente>

Dove <scopo> è per esempio “TLS Server ECC”, “SMIME RSA”, ecc., mentre <anno> è l’anno di creazione della Root CA. Per esempio il commonName completo può essere “Actalis TLS Server RSA Root CA 2025”.

Nel caso di chiavi ECC

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)
Issuer	<Stesso valore del Subject>

Validity	<25 anni>
Subject	CN = Actalis <scopo> Root CA <anno> O = Actalis S.p.A. L = Milano C = IT
SubjectPublicKeyInfo	<Chiave pubblica ECDSA P-384>
SignatureValue	<Firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<SHA1- della chiave pubblica>
SubjectKeyIdentifier (SKI)	<SHA1- della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<assente>
CertificatePolicies	<assente>
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<assente>
CRLDistributionPoints (CDP)	<assente>

Dove <scopo> è per esempio “TLS Server ECC”, “SMIME RSA”, ecc., mentre <anno> è l’anno di creazione della Root CA. Per esempio il commonName completo può essere “Actalis TLS Server ECC Root CA 2025”.

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.

7.1.2.2.1.1 Gerarchia legacy

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 GN O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA di almeno 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true

AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth + clientAuth
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>

7.1.2.2.1.2 Nuova gerarchia

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
Issuer	<Subject della Root CA emittente>
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Domain Validated <scopo> CA <anno> O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth
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>

Dove <scopo> è per esempio "TLS Server ECC", mentre <anno> è l'anno di creazione della SubCA. Per esempio, il commonName completo può essere "Actalis Domain Validated TLS Server RSA CA 2025".

7.1.2.2.2 Sub CA per certificati di classe DV - ACME

I certificati delle CA subordinate hanno il seguente profilo.

7.1.2.2.2.1 Gerarchia legacy

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 DV Server ACME CA GN O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA di almeno 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth + clientAuth
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>

7.1.2.2.3 Sub CA per certificati di classe OV

I certificati delle CA subordinate hanno il seguente profilo.

7.1.2.2.3.1 Gerarchia legacy

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 GN O = Actalis S.p.A. L = Ponte San Pietro ST= Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da almeno 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth + clientAuth
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>

7.1.2.2.3.2 Nuova gerarchia

Campo	**Valore**
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
Issuer	<Subject della Root CA emittente>
Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Organization Validated <scopo> CA <anno> O = Actalis S.p.A. L = Ponte San Pietro ST= Bergamo C = IT
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth
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>

Dove <scopo> è per esempio “TLS Server ECC”, mentre <anno> è l’anno di creazione della SubCA. Per esempio, il commonName completo può essere “Actalis Organization Validated TLS Server RSA CA 2025”.

7.1.2.2.4 Sub CA per certificati di classe EV

I certificati delle CA subordinate hanno il seguente profilo.

7.1.2.2.4.1 Gerarchia legacy

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 GN O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da almeno 2048 bit>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell’estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth + clientAuth
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>

7.1.2.2.4.2 Nuova gerarchia

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
Issuer	<Subject della Root CA emittente>

Validity	<In accordo col paragrafo 6.3.2>
Subject	CN = Actalis Extended Validation <scopo> CA <anno> O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth
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>

Dove <scopo> è per esempio "TLS Server ECC", mentre <anno> è l'anno di creazione della SubCA. Per esempio, il commonName completo può essere "Actalis Extended Validation TLS Server RSA CA 2025".

7.1.2.3 Certificati Cross

I cross-certificati di Actalis hanno i profili descritti di seguito.

7.1.2.3.1 Gerarchia per certificati TLS Server

Nel caso di chiavi RSA

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	<Secondo il tipo di chiave della vecchia Root CA e in accordo coi paragrafi 6.1.5 e 7.1.3>
Issuer	<Subject della vecchia Root CA>
Validity	<NotAfter: data di scadenza della vecchia Root CA>
Subject	<Subject della nuova Root CA>
SubjectPublicKeyInfo	<Chiave pubblica RSA da 4096 bit>
SignatureValue	<Firma della vecchia Root CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<SHA1- della chiave publica della vecchia Root CA>
SubjectKeyIdentifier (SKI)	<SHA1- della chiave pubblica della nuova Root CA>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	TLS Web Server Authentication

CertificatePolicies	Any Policy
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<URL di accesso al servizio OCSP>
CRLDistributionPoints (CDP)	<URL di accesso alla CRL>

Nel caso di chiavi ECC

Campo	Valore
Version	V3 (2)
SerialNumber	<include almeno 8 byte pseudo-random>
Signature	<Secondo il tipo di chiave della vecchia Root CA e in accordo coi paragrafi 6.1.5 e 7.1.3>
Issuer	<Subject della vecchia Root CA>
Validity	<NotAfter: data di scadenza della vecchia Root CA>
Subject	<Subject della nuova Root CA>
SubjectPublicKeyInfo	<Chiave pubblica ECDSA P-384>
SignatureValue	<Firma della vecchia/precedente Root CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true
AuthorityKeyIdentifier (AKI)	<SHA1- della chiave publica della vecchia Root CA>
SubjectKeyIdentifier (SKI)	<SHA1- della chiave publica della nuova Root CA>
KeyUsage	critico: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	TLS Web Server Authentication
CertificatePolicies	Any Policy
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<URL di accesso al servizio OCSP>
CRLDistributionPoints (CDP)	<URL di accesso alla CRL>

7.1.2.4 Certificati dei Titolari

7.1.2.4.1 TLS Server DV

Il certificato per TLS Server DV viene emesso col seguente profilo.

Campo	Valore
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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)
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>
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> (non sul www.<dominio>) con un metodo che copre anche i sottodomini. Esempio: nel caso di un certificato richiesto per *www.example.org*, l'estensione SAN può contenere le due voci *www.example.org* ed *example.org* qualora sia stato validato *example.org* col metodo "DNS Change" (§3.2.2.4.7 dei BR) o altro metodo che copre i sottodomini.

7.1.2.4.2 TLS Server DV Wildcard

Il certificato per TLS Server Wildcard DV viene emesso col seguente profilo.

Campo	Valore
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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)
CertificatePolicies	PolicyOID = 1.3.159.1.23.1 PolicyOID = 2.23.140.1.2.1 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)[6]	<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>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

7.1.2.4.3 TLS Server OV

Il certificato per TLS Server OV viene emesso col seguente profilo.

Campo	Valore
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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> CN = <opzionale, uno degli elementi contenuti nella estensione SAN>

[6] L'estensione SAN contiene anche il nome di dominio ottenuto rimuovendo l'asterisco ("*") dal FQDN wildcard. Esempio: nel caso di un certificato richiesto per *.example.org l'estensione SAN contiene, oltre a **.example.org*, anche *example.org*.

SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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)
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>
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> (non sul www.<dominio>) con un metodo che copre anche i sottodomini. Esempio: nel caso di un certificato richiesto per *www.example.org*, l'estensione SAN può contenere le due voci *www.example.org* ed *example.org* qualora sia stato validato *example.org* col metodo "DNS Change" (§3.2.2.4.7 dei BR) o altro metodo che copre i sottodomini.

7.1.2.4.4 TLS Server OV Wildcard

Il certificato per TLS Server OV Wildcard viene emesso col seguente profilo.

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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 > CN = <opzionale, uno degli elementi contenuti nella estensione SAN>
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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),

CertificatePolicies	PolicyOID = 1.3.159.1.**19**.1 PolicyOID = 2.23.140.1.2.2 CPS-URI = <indirizzo HTTP di questo CPS>
SubjectAlternativeName (SAN)[7]	<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>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

7.1.2.4.5 TLS Server EV

Il certificato per TLS Server EV viene emesso col seguente profilo.

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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> STREET= <opzionale, via dove il Titolare ha la sede> O = <nome ufficiale o DBA del Titolare> CN = <opzionale, uno degli elementi contenuti nella estensione SAN> serialNumber = <numero di registrazione del Titolare presso la camera di commercio o un codice equivalente> businessCategory = <tipo di organizzazione>
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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),
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>

[7] L'estensione SAN contiene anche il nome di dominio ottenuto rimuovendo l'asterisco ("*") dal FQDN wildcard. Esempio: nel caso di un certificato richiesto per *.example.org l'estensione SAN contiene, oltre a **.example.org*, anche *example.org*.

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> (non sul www.<dominio>) con un metodo che copre anche i sottodomini. Esempio: nel caso di un certificato richiesto per *www.example.org*, l'estensione SAN può contenere le due voci *www.example.org* ed *example.org* qualora sia stato validato *example.org* col metodo "DNS Change" (§3.2.2.4.7 dei BR) o altro metodo che copre i sottodomini.

7.1.2.4.6 Qualified Website Authentication Certificate

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

Campo	**Valore**
Version	V3 (2)
SerialNumber	< include almeno 8 byte pseudo-random>
Signature	<In accordo coi paragrafi 6.1.5 e 7.1.3>
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> STREET=<via dove ha sede il Titolare> O = <nome ufficiale o DBA del Titolare> CN = < CN = <opzionale, uno degli elementi contenuti nella estensione SAN> serialNumber = <numero di registrazione del Titolare nel registro delle imprese o un codice equivalente> joiCountryName=<codice del paese dove il Titolare è registrato> businessCategory = <tipo di organizzazione secondo [EVGL]> organizationIdentifier = <secondo [EVGL]>
SubjectPublicKeyInfo	<In accordo coi paragrafi 6.1.5 e 7.1.3>
SignatureValue	<firma della CA>
Estensione	**Valore**
Basic Constraints	<se incluso, critico: CA=FALSE>
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)
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>

QCStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS id-etsi-qcs-QcType
cabfOrganizationIdentifier	<secondo [EVGL]>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962 [CT]

7.1.2.5 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:

7. rispettino pienamente sia la specifica [RFC 5280] che i Requisiti e le Linee Guida del CAB Forum; e
8. 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, secondo il tipo di chiave della CA:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3

Le CRL e le risposte OSCP sono firmate usando uno dei seguenti algoritmi, secondo il tipo di chiave della CA:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3

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 **TLS 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.
- Questa estensione è contrassegnata come *critica* nel caso in cui il campo Subject DN sia vuoto.

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

7.1.4.2.2 Campi del Subject Distinguished Name

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

- L'attributo **commonName** (OID 2.5.4.3) del Subject DN, se presente, deve contenere un singolo FQDN (Fully Qualified Domain Name) tra quelli inclusi nell'estensione SAN (vedere il paragrafo precedente). Se un FQDN è troppo lungo (>64 caratteri), questo attributo sarà omesso.
- Nessun altro attributo del Subject DN è presente.
- Il campo Subject può essere vuoto nei certificati DV TLS Server, ad esempio, quando non può contenere un FQDN molto lungo (più lungo di 64 caratteri).

Per i certificati **TLS Server OV**, si applicano le seguenti regole:

L'attributo **commonName** (OID 2.5.4.3) del Subject DN, se presente, deve contenere un singolo indirizzo IP o FQDN (Fully Qualified Domain Name) tra quelli contenuti nell'estensione SAN (vedere il paragrafo precedente);

- 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 TLS, 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 **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 **TLS Server EV**, 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.

Per i **Qualified Website Authentication Certificates** (**QWAC**), si applicano anche le seguenti regole aggiuntive:

- L'attributo **organizationIdentifier** (OID 2.5.4.97) del DN del soggetto dev'essere popolato secondo le [EVGL];
- L'estensione **cabfOrganizationIdentifier** (OID 2.23.140.3.1) è altresì inclusa nel certificato (si veda anche il paragrafo 7.1.2.3.6) ed è valorizzata in conformità alle disposizioni delle [EVGL].

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].
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).

7.2.1 Numeri di versione

La versione delle CRL è v2 (1).

7.2.2 Estensioni della CRL

In corrispondenza di ogni singola voce (entry) della CRL è presente l'estensione *reasonCode* a indicare la motivazione della sospensione o revoca.

Per i certificati TLS emessi a partire dal 1° ottobre 2022, quando un certificato TLS viene revocato per uno dei seguenti motivi, il CRLReason specificato viene incluso nell'estensione reasonCode della voce CRL corrispondente. In caso contrario, il codice CRLReason viene *omesso*:

- *keyCompromise* (1)
- *affiliationChanged* (3)
- *superseded* (4)
- *cessationOfOperation* (5)
- *privilegeWithdrawn* (9)

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 emette i certificati e gestisce la propria infrastruttura PKI in conformità alla normativa applicabile, nonché nel rispetto dei requisiti previsti dai CA/Browser Forum Baseline Requirements [BR] e delle linee guida contenute nelle Extended Validation Guidelines [EVGL].

Actalis garantisce la continuità della copertura di audit delle proprie attività di Certification Authority, senza interruzioni, a decorrere dalla generazione della coppia di chiavi della Certification Authority e fino a quando il relativo certificato di CA non sia più considerato attendibile (trusted), sia scaduto o revocato, secondo quanto applicabile, ovvero fino alla distruzione del corrispondente materiale crittografico, qualora tale distruzione sia richiesta, osservata e attestata da un auditor qualificato.

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.

Actalis rende pubblicamente disponibili le attestazioni di audit applicabili e trasmette al CCADB le informazioni di audit richieste entro e non oltre novantadue (92) giorni di calendario dalla data di riferimento (point-in-time date) o dalla data di conclusione del periodo di audit, a seconda dei casi.

Le attestazioni di audit pubblicate da Actalis costituiscono la documentazione ufficiale (autoritativa), sono ricercabili mediante testo (text-searchable) e sono rese disponibili in lingua inglese. Esse contengono tutte le informazioni richieste dalla CCADB Policy e dalle policy applicabili dei Root Store Programs, incluse: il nome del CA Owner, l'identità e le qualifiche dell'auditor, le sedi sottoposte ad audit, le impronte SHA-256 dei certificati di Root CA e delle CA subordinate rientranti nell'ambito dell'audit (ivi compresi gli eventuali certificati cross), gli standard di audit applicati e le relative versioni, il periodo di audit ovvero la point-in-time date, la data di emissione dell'attestazione, i documenti di policy oggetto di riferimento, nonché gli incidenti o i rilievi (findings) verificatisi, ancora aperti o segnalati nel corso 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 ai requisiti [BR] ed [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 emessi nel periodo che inizia immediatamente dopo l'ultima autovalutazione, anche utilizzando tecniche e strumenti di *linting*.

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 “Responsabile 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 TLS 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 SubjectAltName (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;
- 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 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 o di Condizioni d'Uso (Terms of Use). Come parte dell'Accordo 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 rimuovere prontamente il certificato dai server sui quali esso è installato;
- cessare ogni utilizzo del certificato dopo la data di scadenza dello stesso.

Il Titolare è inoltre tenuto a installare il certificato esclusivamente sui server raggiungibili tramite i nomi indicati nell'estensione subjectAlternativeName del certificato e a utilizzare tali server unicamente secondo le modalità consentite dal presente CPS e per finalità lecite.

Il Titolare prende atto e accetta che la Certification Authority, qualora venga a conoscenza dell'utilizzo del certificato per finalità illecite (quali, a titolo esemplificativo, attività di phishing, attacchi Man-in-the-Middle, distribuzione di malware o analoghe condotte) ovvero per l'emissione di ulteriori certificati, procederà all'immediata revoca del certificato, senza obbligo di preavviso.

Il Titolare è tenuto a collaborare tempestivamente con Actalis affinché quest'ultima possa rispettare i termini di revoca dei certificati previsti dai TLS Baseline Requirements del CA/Browser Forum e dalle policy applicabili dei Root Store Program.

Il Titolare prende atto che i certificati TLS Server pubblicamente trusted possono essere soggetti a obblighi di revoca entro termini particolarmente brevi e si impegna pertanto a non utilizzarli in sistemi o ambienti nei quali non sia possibile procedere tempestivamente alla loro sostituzione.

Qualora ciò sia necessario per consentire la revoca di certificati, la gestione di un incidente, l'esecuzione di una revoca massiva (revoca massiva) o il rispetto dei requisiti applicabili, il Titolare è tenuto a sostituire tempestivamente i certificati interessati, cessarne immediatamente l'utilizzo, fornire le informazioni richieste da Actalis e adottare ogni altra ragionevole misura richiesta dalla stessa

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.

9.6.5 Dichiarazioni e garanzie degli altri partecipanti

Nessuna stipula.

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 particolare, Aruba PEC risponde dei danni causati a qualsiasi persona fisica o

giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente, nei casi ed entro i limiti previsti dall'art. 13 del Regolamento.

Con specifico riferimento ai Certificati EV, l'eventuale limite monetario della responsabilità di Actalis nei confronti di ciascun Titolare o di ciascuna Parte Facente Affidamento, per pretese risarcitorie giuridicamente riconosciute e comprovabili, non può essere inferiore a 2.000 USD (duemila dollari statunitensi) per ciascun Titolare o Parte Facente Affidamento e per ciascun Certificato EV.

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:

9. cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni, scioperi, sommosse, ecc.); e/o
10. 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

Actalis riconosce e accetta che i Fornitori di Software Applicativo che abbiano in essere con Actalis, in qualità di Root CA, un accordo per la distribuzione dei certificati di Root CA non assumono, né possono essere considerati aver assunto, alcun obbligo o responsabilità, anche potenziale, spettante ad Actalis.

In particolare, la distribuzione o l'inclusione dei certificati di Root CA nei software o nei relativi archivi fiduciari non comporta il trasferimento ai Fornitori di Software Applicativo di alcun obbligo o responsabilità derivante dall'emissione, dalla gestione o dal mantenimento di tali certificati da parte di Actalis, né dall'affidamento riposto negli stessi dalle Terse Parti.

Actalis si impegna ad assumere la difesa, indennizzare, manlevare e tenere indenne ciascun Fornitore di Software Applicativo rispetto a qualsiasi domanda, azione, pretesa, danno o perdita subiti dal medesimo e comunque connessi a un certificato emesso da Actalis, indipendentemente dalla causa dell'azione, dal titolo della responsabilità o dal fondamento giuridico invocato.

Gli obblighi di difesa, indennizzo e manleva sopra indicati non si applicano alle domande, alle azioni, alle pretese, ai danni o alle perdite direttamente causati dal software del Fornitore di Software Applicativo che:

- rappresenti come non affidabile (*non trusted*) un certificato ancora valido;
- rappresenti come affidabile (*trusted*) un certificato scaduto; oppure
- rappresenti come affidabile (*trusted)* un certificato revocato, a condizione che lo stato di revoca sia, al momento rilevante, reso disponibile online da Actalis e che il software applicativo abbia omesso di verificarlo oppure abbia ignorato l'indicazione dello stato di revoca.

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. Se invece il certificato è stato acquistato da un Rivenditore, l'assistenza deve essere richiesta a quel Rivenditore. Le modalità per la richiesta di assistenza sono pubblicate sul sito web della CA nonché sul portale di acquisto e/o di richiesta dei certificati.

La segnalazione di problemi relativi a *certificati già emessi ed installati*, invece, deve essere fatta con le modalità descritte nel paragrafo 1.5.2.

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

Qualora il Titolare o il Richiedente del certificato rivesta la qualifica di Professionista ai sensi del Decreto Legislativo 6 settembre 2005, n. 206 ("Codice del Consumo"), ogni controversia derivante dal Contratto sarà devoluta alla cognizione di un Collegio Arbitrale composto da tre membri, di cui uno nominato da Actalis, uno nominato dal Contraente e il terzo, con funzioni di Presidente, nominato di comune accordo dai primi due.

Qualora una delle Parti non provveda alla nomina del proprio Arbitro entro venti (20) giorni dal ricevimento della comunicazione di nomina dell'Arbitro effettuata dall'altra Parte, il relativo Arbitro sarà nominato, su richiesta della Parte più diligente, dal Presidente del Tribunale di Arezzo. Analogamente, qualora i due Arbitri nominati dalle Parti non raggiungano un accordo sulla nomina del terzo Arbitro entro venti (20) giorni dalla nomina del secondo Arbitro, quest'ultimo sarà nominato dal Presidente del Tribunale di Arezzo, su istanza della Parte più diligente.

L'arbitrato avrà natura rituale e gli Arbitri decideranno secondo diritto, ai sensi degli articoli 806 e seguenti del Codice di procedura civile.

La sede dell'arbitrato sarà 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

Appendice A – Storico 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 TLS 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.	AS

			Precisazioni sugli obblighi del titolare.	
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. 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.	AS
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 Transparency 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 certificati.	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 TLS 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 TLS Server di classe EV non sono ammessi indirizzi IP. Introdotta la CT obbligatoria, dopo il 30 Aprile 2018, su tutte le classi di certificati TLS 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 TLS 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
15 luglio 2020	5.7	4.1.2, 4.9.5, 6.1.5, 6.3.2, 9.11	Aggiornamento e precisazioni sulle modalità di richiesta del certificato. Precisazione sui tempi di revoca. Precisazioni su algoritmi e lunghezza chiavi dei Titolari. Validità massima dei certificati TLS Server ridotta a 398 giorni. Precisazioni sull'assistenza.	AS
5 Ottobre 2020	5.8	1.3.1.2, 1.4.2, 3.2.2.4	Aggiornamento elenco delle CA intermedie. Inserito avvertimento sul certificate pinning. Aggiornato l'elenco dei metodi di DCV supportati (aggiunto ACME http-01)	AS
22 aprile 2021	5.9	1.1, 1.7, 6.1.2, 6.1.3, 6.1.5, 6.2.1, 9.6.1, 9.6.3, 3.2.2.1	Inserito riferimento ai Code Signing Baseline Requirements. Aggiornamenti per i certificati di Code Signing. Inserito riferimento alla lista delle approved incorporating agencies.	AS
24 agosto 2021	5.10	1.5.3, 3.2.2.4, 3.2.2.8 4.9.12, 9.8	Aggiunta AgID ai soggetti per idoneità CPS Allineamento con la Mozilla Root Policy. Recepimento del Ballot SC45 del CABF. Recepimento del Ballot SC46 del CABF. Precisate le modalità per segnalare alla CA una chiave privata compromessa. Aggiornamento alle limitazioni di responsabilità.	AS
29 Aprile 2022	5.11	3.2.2.1; 3.2.2.3; 7.1.4.2.1; 7.1.4.2.2	Aggiornamento alla validazione dell'identità Allineamento nella numerazione dei capitoli Aggiornamento delle policy SAN e FQDN	AS
10 Ottobre 2022	5.12	4.1.2 4.9.1.1	Aggiornamento delle modalità di sottoscrizione della richiesta dei certificati EV Aggiornamento circostanze per la revoca del certificato del Titolare	AS
17 Maggio 2023	5.13	1.3.1.2, 3.1, 4.1.2, 5.5.2, 6.1, 6.2, 6.8, 7.1.2, 7.1.3, 7.1.4, 7.2, 9.6.1	Correzione di piccoli refusi. Aggiornata la lista delle SubCA. Rimossi i riferimenti all'attributo "organizationalUnitName" (OU). Aggiunti chiarimenti sul processo di enrollment dei certificati Code Signing. Corretto il profilo del certificato QWAC. Chiarito che il Subject può essere vuoto nei	AS

			certificati TLS DV. Requisiti modificati per la protezione e la verifica della chiave privata nel caso di certificati Code Signing. Aggiunte informazioni sulla TSA di Actalis. Chiarito l'uso della CRLReason nelle voci della CRL. Modificati gli identificatori degli algoritmi. Periodo di conservazione modificato per gli archivi delle evidenze.	
16 Maggio 2024	5.14	1.3.1.2, 1.6, 3.2.2.9, 3.2.5, 4.2.1, 6.2.7.4, 7.1, 7.1.2.2	Revisione annuale del documento. Aggiunta la CA subordinata "Actalis DV Server ACME CA G1". Adeguamento a BR 2.0.4 e EVGL 2.0.1. Correzione refusi. Precisazioni sui certificati di Code Signing.	AS, EDF
09 Luglio 2024	5.15	1.1, 2.1, 4.2.1, 4.10.1, 6.7, 7	Correzione refusi e precisazioni.	AS, EDF
15 Gennaio 2025	5.16	3.2.2.1, 3.2.2.4, 3.2.2.8, 4.3.1, 4.9.1, 4.9.9, 4.9.10, 5, 6.1.1, 6.1.6, 6.6.1, 7.2, 8.7.	Correzione numero di protocollazione, refusi e precisazioni. Integrazioni riguardo l'aggiornamento della lista delle fonti autorevoli consultate dalla CA. Rimozione dell'utilizzo del protocollo WHOIS in fase di autenticazione dei domini. Integrazioni nelle cause di revoca d'ufficio da parte della CA. Inserimento delle verifiche di conformità dei certificati (linting) pre-emissione e in fase di self-audit. Restyling dei paragrafi 4.9.9 e 4.9.10. Integrazioni riguardo la generazione e la lunghezza delle chiavi di CA. Modifiche di formattazione al par 7.2. Riviste le informazioni pubbliche relative alle misure di sicurezza della CA.	AS, NP
11 Marzo 2025	5.17	1.4.2, 3.2.2.1, 3.2.2.9, 4.5, 4.7, 4.8, 4.9.1.1, 7.2	Integrazioni riguardo gli standard applicabili, integrazioni al par 3.2.2.1, introduzione MPIC, ristrutturazione paragrafi 4.5, 4.8, 4.9 e 7.2 in accordo con RFC-3647, integrazioni alle motivazioni di revoca.	AS, NP
18 Giugno 2025	5.18	1.3.1.2, 3.2.2.4, 4.9.3, 6.1.5, 6.2.1, 6.2.7	Rimozione della SubCA *Actalis Client Authentication CA G1,* rimozione del metodo di validazione del dominio previsto in BR# 3.2.2.4.2, previsione di scenari di revoca massiva, Integrazioni riguardo la generazione e la lunghezza delle chiavi di CA, specifica riguardo la certificazione dei moduli crittografici, correzione di refusi nel documento.	AS, NP
27 Novembre 2025	5.19	4.2.2, 4.9.9, 4.10.1, 5.2, 5.4.1, 5.7.1,	Modifica minore al par. 4.2.2, Integrazione relativa al protocollo OCSP,	AS, NP

		6.7	Specifica sul partizionamento delle CRL, Aggiunta specifica riguardo l'inventario degli asset, Specifica riguardo le tracciature delle configurazioni dei firewall, Aggiunti requisiti sulla gestione della revoca massiva	
18 Dicembre 2025	5.20	1.3, 6.3.2, 7.1.2	Integrazioni all'infrastruttura PKI con l'inserimento di nuovi certificati di RootCA e SubCA	AS, BS, NP
15 marzo 2026	5.21	3.2.2.5, 4.2.2, 4.3.1, 6.3.2	Rimozione del metodo di convalida della ricerca inversa dell'indirizzo IP, integrazione controlli pre-emissione, integrazione dei contenuti, modifica durata certificati	AS, FM, NP
29 Maggio 2026	6.0	Intero documento	Revisione completa del documento al fine di disciplinare esclusivamente la gestione dei certificati TLS Server.	AS, FM, NP
09 Novembre 2026	6.1	1.1, 1.3, 1.4.2, 1.5.4, 1.7, 3.1.1, 3.2.2, 4.2.2, 4.9, 5.1.6, 5.1.7, 5.4.8, 5.8, 6.1.6, 6.1.7 6.2.7, 6.5.1 6.7, 6.8, 7.1, 9.8, 9.9.1	Integrazioni di carattere generale e aggiornati il codice univoco della CA, l'ambito geografico di commercializzazione dei certificati, l'utilizzo dei certificati in infrastrutture critiche, la procedura di approvazione del manuale e i riferimenti normativi. Razionalizzati i contenuti relativi alla denominazione dei soggetti e integrate le modalità di verifica del Richiedente, i controlli MPIC, l'utilizzo delle liste di esclusione e l'elaborazione dei parametri *accounturi* e *validationmethods*. Precisati i codici motivo di revoca e le circostanze di revoca dei certificati delle CA subordinate. Integrate le disposizioni sulla dismissione dei supporti di memoria, sullo smaltimento dei rifiuti, sulla gestione e risoluzione delle vulnerabilità e sulla conservazione delle evidenze in caso di cessazione delle attività della CA. Precisati i criteri di generazione delle chiavi crittografiche e integrate le disposizioni sull'utilizzo delle chiavi della CA, sulla certificazione degli HSM e sulla gestione e sincronizzazione dell'ora. Aggiornati e allineati i profili dei certificati ai requisiti dei Root Program e integrate le disposizioni sulle limitazioni di responsabilità per i certificati EV e sugli indennizzi.	AS, NP