AGID
Agenzia per l'Italia Digitale
Area Soluzioni per la Pubblica Amministrazione

AgID - AGENZIA PER l'ITALIA DIGITALE

MANUALE OPERATIVO DEL SERVIZIO "AgID CA"

CERTIFICATION PRACTICE STATEMENT

Versione 6.0

Redatto da:	Area Soluzioni per la Pubblica Amministrazione
Approvato da:	Francesco Tortorelli

DISTRIBUZIONE: PUBBLICA

Sommario

Storia delle modifiche

Descrizione delle modifiche	Versione	Data
Prima emissione	1.0	18/10/2017
Par. 4.4.1 – Eliminato riferimento al WHOIS (non più usato) Par. 8.4 – Durata dei certificati per sito web limitata a 2 anni	2.0	28/02/2018
Par. 2.2.1 – Precisazione: la AgID CA1 è "technically constrained" Par. 5.3 – Introdotta la Certificate Transparency obbligatoria per i certificati SSL Server emessi dopo il 30 aprile 2018 Par. 8.4 – Introdotta estensione Elenco CST nel certificato SSL Server	3.0	27/04/2018
Par. 5.1 – Revisione della procedura Par. 8.4 – Durata dei certificati per sito web limitata a 1 anno	4.0	17/09/2020
Tutto il documento: eliminati i riferimenti ai certificati per siti web (SSL Server). Ristrutturazione intero documento per conformità alla RFC3647. Aggiunto riferimento alla Mozilla Root Store Policy.	5.0	22/06/2021
Tutto il documento: reintrodotti i riferimenti ai certificati per siti web (SSL Server) emessi da una CA intermedia a ciò dedicata.	6.0	29/11/2021

1 Introduzione

1.1 Scopo del documento

Con Decreto 1° dicembre 2009, n. 177 il CNIPA è stato riorganizzato in un nuovo ente, denominato DigitPA che subentra al CNIPA nelle attività di certificazione.

Con il D.P.R. 11 febbraio 2005, n. 68 ed il Decreto del Ministro per l'Innovazione e le Tecnologie del 2 novembre 2005, contenente le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata", è attribuito in via esclusiva al CNIPA (e quindi a DigitPA) il compito di rilasciare ai Gestori PEC i certificati server automaticamente riconosciuti dai prodotti di mercato.

In base al DECRETO-LEGGE 22 giugno 2012, n. 83 "Misure urgenti per la crescita del Paese", art. 19 - Istituzione dell'Agenzia per l'Italia digitale - è istituita "l'**Agenzia per l'Italia Digitale**, sottoposta alla vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato, del Ministro dell'economia e delle finanze, del Ministro per la pubblica amministrazione e la semplificazione, del Ministro dello sviluppo economico e del Ministro dell'istruzione, dell'università e della ricerca".

In base al medesimo Decreto Legge, art. 20 "l'Agenzia svolge, altresì, (...), le funzioni di coordinamento, di indirizzo e regolazione affidate a DigitPA dalla normativa vigente". Le funzioni di AgID sono state successivamente confermate e integrate dall'art. 14 bis del Decreto legislativo 7 marzo 2005 n. 82 e s.m.i; pertanto le funzioni di certificatore precedentemente assegnate a DigitPA sono riferibili e riferite ad AGID.

Il presente **Certification Practice Statement** (CPS), anche denominato "Manuale Operativo", definisce le procedure applicate dalla CA dell'AgID per l'emissione e gestione di certificati digitali per sistemi server. In particolare, sono emessi tre tipi di certificato:

- per **firma elettronica** (per es. firma delle Ricevute PEC, firma di file LDIF, …)
- per **autenticazione** verso server SSL (ovvero per SSL client authentication)
- per **SSL Server**, ossia l'attivazione del protocollo SSL/TLS sui siti web

La prima tipologia di certificati è utilizzata principalmente dai Gestori PEC per gli adempimenti previsti dalla normativa sulla PEC, nonché da altri attori del circuito PEC (inclusa per es. la stessa AgID).

La seconda tipologia può essere utilizzata per autenticare un sistema che funge da client nell'ambito di un colloquio SSL in cui si richiede l'autenticazione di entrambe le parti coinvolte. In particolare, nell'ambito del servizio PEC, sono utilizzati per l'accesso all'Indice dei Gestori PEC (IGPEC).

La terza tipologia è utilizzata per attivare il protocollo SSL/TLS su siti web gestiti dall'AgID o comunque su domini che ricadono sotto il controllo dell'AgID.

Questo CPS è strutturato in accordo con la specifica pubblica RFC 3647 [CPF].

L'hosting e la gestione operativa del servizio di certificazione dell'AgID sono affidati al Raggruppamento Temporaneo di Imprese (RTI) aggiudicatario della Gara CONSIP CIG 6049538CAC, avente per mandataria la società Fastweb S.p.A. (in seguito, per brevità, solo "RTI").

1.2 Identificazione del documento

Il presente CPS è identificato attraverso il numero di versione indicato nella prima pagina.

Il presente CPS è referenziato dal seguente OID (Object Identifier) all'interno dei certificati emessi, nella estensione CertificatePolicies:

1.3.76.16.3.1 – Certificazione chiavi pubbliche server

Questo CPS è pubblicato in formato PDF sul sito web del Certificatore al seguente URL:

http://www.agid.gov.it/cps-ca

1.3 Partecipanti alla PKI

1.3.1 Certification Authority

Dal 20/11/2017 è operativa un'infrastruttura di CA che utilizza una chiave di certificazione di AgID denominata "**AgID CA1**". Dal 25/11/2021 è inoltre utilizzata anche una seconda chiave di certificazione denominata "**AgID CA SSL SERVER**". Queste due chiavi di CA, con le quali sono emessi i certificati server, sono a loro volta certificate dalla Root CA di Actalis S.p.A., preinstallata nei più diffusi ambienti operativi e browser di mercato. In questo modo, senza bisogno di intervento da parte dell'utilizzatore finale, è possibile:

- il riconoscimento dell'attendibilità delle firme elettroniche apposte dai Gestori PEC;
- l'accesso sicuro (autenticato e cifrato) ai siti web mediante protocollo HTTPS.

Nel seguito del presente documento, col termine "**AgID CA**" si farà riferimento a entrambe le CA laddove non sia necessario distinguere.

La PKI su cui si basa il servizio descritto nel presente CPS è schematizzata nella seguente figura:

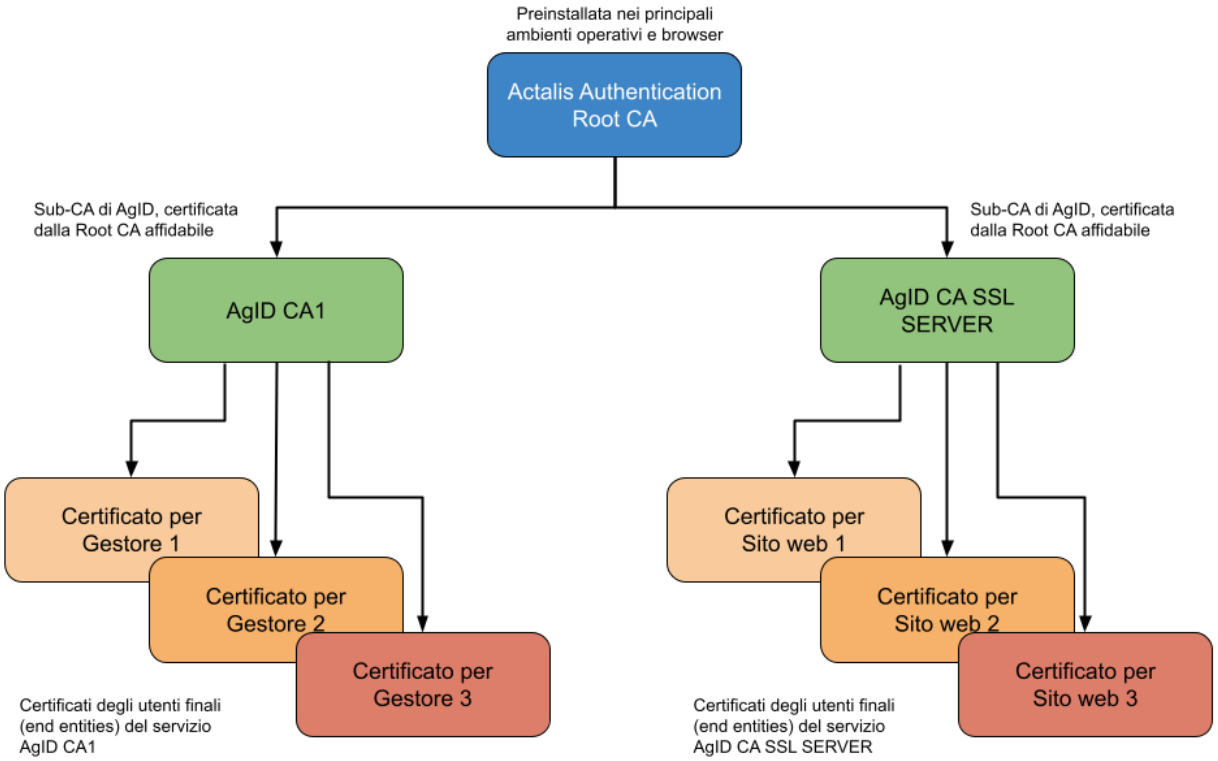

Figura 1: Schema della PKI di riferimento

Entrambe le CA emittenti, **AgiD CA1** ed **AgID CA SSL SERVER**, operano sotto la responsabilità dell'**AgID**, della quale si riportano di seguito i principali dati identificativi e di contatto:

Denominazione ufficiale	Agenzia per l'Italia Digitale (AgID)
Direttore Generale	Francesco Paorici
Sede legale	Via Liszt, 21 – 00144 Roma
Object Identifier	1.3.76.16
Telefono	+39 06 852641
Sede operativa	Via Liszt, 21 – 00144 Roma
Indirizzo E-mail	protocollo@pec.agid.gov.it
Sito web principale	http://www.agid.gov.it

Di seguito si riportano i dati identificativi dei certificati delle due CA emittenti dell'AgID:

Dato	Valore
Titolare (Subject)	**CN** = AgID CA1 **OU** = Area Soluzioni per la Pubblica Amministrazione **O** = Agenzia per l'Italia Digitale **L** = Roma **C** = IT
Emittente (Issuer)	**CN** = Actalis Authentication Root CA **O** = Actalis S.p.A./03358520967 **L** = Milan **C** = IT
Identificatore chiave (Subject Key Identifier)	A5FD85050EC3F1D6654A206CE2DB4D60932B8AA0
Periodo di validità	**DA**: 21/09/2021 **A**: 22/09/2030

Dato	Valore
Titolare (Subject)	**CN** = AgID CA SSL SERVER **OU** = Area Soluzioni per la Pubblica Amministrazione **O** = Agenzia per l'Italia Digitale **L** = Roma **C** = IT
Emittente (Issuer)	**CN** = Actalis Authentication Root CA **O** = Actalis S.p.A./03358520967 **L** = Milan **C** = IT
Identificatore chiave (Subject Key Identifier)	2AB7A610B6863F43B8FDCF4AFA88BF329323CFB4
Periodo di validità	**DA**: 24/11/2021 **A**: 22/09/2030

Poiché la "AgID CA1", con la quale sono emessi i certificati destinati ai Gestori PEC, è una Certification Autority "technically constrained", qualora un Gestore volesse attivare una nuova Provider Unit dovrà preventivamente notificarlo, tramite PEC, alla casella PEC richiesta-certificati@pec-ic.agid.gov.it, inviando tutti i dati relativi alla nuova Provider Unit.

Anche la "AgID CA SSL SERVER" è una Certification Autority "technically constrained" e come tale può emettere certificati solo per l'AgID.

1.3.2 Registration Authority (RA)

I compiti di Registration Authority sono svolti dal RTI.

1.3.3 Utenti (titolari)

- I certificati di **Firma** sono forniti esclusivamente ai Gestori accreditati di Posta Elettronica Certificata[1] ed altri attori del circuito PEC, inclusa per es. la stessa AgID;
- I certificati di **Autenticazione** sono forniti esclusivamente ai Gestori accreditati di PEC ed altri attori del circuito PEC, inclusa per es. la stessa AgID (cfr. punto precedente);
- • I certificati **SSL Server** sono rilasciati esclusivamente per domini sotto il controllo di AgID.

1.3.4 Relying Parties

Le "Relying Parties" (RP) sono tutti i soggetti che fanno affidamento sulle informazioni contenute nei certificati emessi secondo questo CPS. Per esempio (elenco non esaustivo):

- coloro che inviano o ricevono messaggi di PEC, in quanto ricevono "Ricevute PEC" firmate con certificati emessi secondo questo CPS;
- i soggetti gestori dei server che accettano una SSL client authentication basata su certificati di autenticazione emessi secondo questo CPS;
- coloro che accedono a siti web sui quali sono installati certificati SSL Server emessi secondo questo CPS;

1.4 Uso dei certificati

Come anticipato, questo CPS riguarda l'emissione e gestione di certificati dei seguenti tipi:

- certificati di Firma (S/MIME);
- certificati di Autenticazione;
- certificati per siti web (SSL Server).

I certificati emessi secondo questo CPS devono essere utilizzati solamente per gli scopi sopra indicati (secondo il tipo di certificato).

1.5 Responsabile del CPS

Il Responsabile del presente CPS è:

Responsabile del CPS	
Nome	Francesco
Cognome	Tortorelli
Telefono	+39 06 852641
E-mail	tortorelli@agid.gov.it

[1] L'elenco ufficiale dei Gestori PEC accreditati è pubblicato sul sito web dell'AgID all'indirizzo http://www.agid.gov.it/infrastrutture-sicurezza/pec-elenco-gestori

1.6 Definizioni e acronimi

Nel seguito sono indicati i termini specifici e le abbreviazioni utilizzati nel presente CPS:

Definizione	Descrizione
AgID	Agenzia per l'Italia Digitale
AgID CA1	Nome della Certification Authority dell'AgID che emette certificati per il circuito PEC; opera sotto la responsabilità dell'AgID; il servizio viene erogato in outsourcing dal RTI.
AgID CA SSL SERVER	Nome della Certification Authority dell'AgID che emette certificati per siti web; opera sotto la responsabilità dell'AgID; il servizio viene erogato in outsourcing dal RTI.
Amministrazione	Amministrazione/Ente pubblico
CA	Certification Autority
Certificatore	Soggetto che presta servizi di certificazione di chiavi pubbliche o che fornisce altri servizi connessi a quest'ultime.
CPS	Certification Practice Statement - il presente documento
CRL	Certificate Revocation List - lista dei certificati revocati
CSR	Certificate Signing Request - richiesta di certificazione secondo RFC2314
FQDN	Fully-Qualified Domain Name
Gestore PEC	Società/Amministrazione/Ente che gestisce un servizio di Posta Elettronica Certificata ai sensi delle norme vigenti, accreditato dall'AgID.
HSM	Hardware Security Module (modulo crittografico hardware)
PEC	Posta Elettronica Certificata di cui al D.P.R. 11 febbraio 2005, n. 68
PKI	Infrastruttura a Chiave Pubblica (Public Key Infrastructure).
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
RTI	Raggruppamento Temporaneo di Imprese
SSL	Secure Sockets Layer. Protocollo sicuro di comunicazione su una rete TCP/IP specificatamente destinata alla securizzazione dell'accesso ai siti Web.
TLS	Trasport Layer Security. Nome attuale del protocollo precedentemente noto come SSL (cfr.)

1.7 Riferimenti normativi

Di seguito si elencano le norme di legge di riferimento per questo CPS:

Riferimento	Descrizione
[CAD]	Decreto Legislativo 5 marzo 2005, n.82 e successive modificazioni
[DPCM200309]	DPCM 22 febbraio 2012: "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", GU n.117 del 21-5-2013
[DLVO19603]	Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"
[DM020704]	Decreto Ministeriale 2 luglio 2004
[DPR6805]	D.P.R. 11 febbraio 2005, n. 68
[DMPEC]	Decreto del Ministro per l'Innovazione e le Tecnologie, contenente le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" del 2 novembre 2005
[CNIPACR56]	Circolare CNIPA. 21/05/2009 – n° 56

[D-L 22 giugno 2012, n. 83]	Misure urgenti per la crescita del Paese (12G0109) Gazz. Uff. 26 giugno 2012, n.147, S.O.

1.8 Altri riferimenti

Di seguito si elencano ulteriori norme tecniche e regolamenti di riferimento per questo CPS:

[BR]	CAB Forum: "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ", https://cabforum.org/baseline-requirements-documents/
[CPF]	RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", https://www.ietf.org/rfc/rfc3647.txt
[CSR]	RFC 2314: "PKCS #10: Certification Request Syntax - Version 1.5", https://www.ietf.org/rfc/rfc2314.txt
[CPROF]	RFC 5280: "Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile", https://www.ietf.org/rfc/rfc5280.txt
[OCSP]	RFC6960: "X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP", https://tools.ietf.org/rfc/rfc6960.txt
[MRSP]	Mozilla Root Store Policy, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

2 Pubblicazioni e repository

2.1 Informazioni pubblicate

AgID pubblica almeno la seguente documentazione sul proprio sito web, relativa al servizio di CA descritto in questo CPS, all'indirizzo http://www.agid.gov.it/cps-ca:

- Certification Practice Statement (CPS) – il presente documento
- la procedura di richiesta di emissione certificato
- la modulistica di richiesta certificati
- i certificati di CA (Root CA, AgiD CA1, AgID CA SSL SERVER)

AgiD, inoltre, pubblica le CRL sul proprio directory server (cfr. più sotto).

2.1.1 Modulistica

Sul sito di AGID, all'indirizzo http://www.agid.gov.it/cps-ca, è disponibile il modulo "Richiesta di Registrazione" che l'Organizzazione richiedente deve compilare ed inviare alla CA nel rispetto della "Procedura per la richiesta di emissione certificato".

2.1.2 CRL

Le CRL sono pubblicate e aggiornate nei Directory LDAP una volta al giorno. L'indirizzo del suddetto directory server è: ldap://ca1.agid.gov.it.

La CRL è inoltre pubblicata con http ai seguenti URL:

- http://ca1.agid.gov.it/CRL (certificati di firma e autenticazione)
- http://ca1.agid.gov.it/SSLCRL (certificati SSL Server)

Gli indirizzi LDAP ed HTTP della CRL sono riportati all'interno dei certificati stessi, nell'estensione CRLDistributionPoints (cfr. il cap. 7).

3 Identificazione e autenticazione

In generale, i certificati emessi secondo il presente CPS contengono informazioni atte a identificare chiaramente il titolare. Non sono ammessi pseudonimi né identificativi generici e/o ambigui.

3.1 Regole di naming

In particolare, si applicano le seguenti regole:

- L'attributo **countryName** ("**C**") del Subject è sempre obbligatorio e contiene il codice a 2 lettere (ISO 3166-1 alpha-2) del paese dove ha sede legale l'Organizzazione titolare del certificato;
- L'attributo **stateOrProvinceName** ("**ST**") del Subject è sempre obbligatorio e contiene il nome (non la sigla) della Provincia dove ha sede legale l'Organizzazione titolare del certificato;
- L'attributo **localityName** ("**L**") del Subject è sempre obbligatorio e contiene il nome della loca- lità (città) dove ha sede legale l'Organizzazione titolare del certificato;
- L'attributo **organizationName** ("**O**") del Subject è sempre obbligatorio e contiene il nome ufficiale dell'Organizzazione titolare del certificato;
- L'attributo **organizationalUnitName** ("**OU**") del Subject è opzionale; se presente, contiene una stringa a discrezione dell'Organizzazione richiedente, purché non sia tale da indurre in errore le Relying Parties circa l'identità del titolare;
- L'attributo **commonName** ("**CN**") del Subject è sempre obbligatorio; in particolare:
  - nel caso dei certificati per Sito web (**SSL Server**), contiene uno degli FQDN inclusi nella estensione **SubjectAlternativeNames**;
  - nel caso dei certificati di **Firma** (S/MIME), contiene lo stesso indirizzo di posta elettronica incluso nell'estensione SubjectAlternativeNames oppure una stringa a discrezione della Organizzazione richiedente, purché non sia tale da poter indurre in errore le Relying Parties circa l'identità del titolare; questa stringa non può essere un nome di dominio (per es. host.dominio.it o simile);
  - nel caso dei certificati di **Autenticazione**, contiene una stringa a discrezione dell'Organizzazione richiedente, purché non sia tale da poter indurre in errore le Relying Parties circa l'identità del titolare; questa stringa non può essere un nome di dominio;
- L'estensione **SubjectAlternativeNames** (SAN), sempre presente, è valorizzata come segue:

- Certificati **SSL Server**: uno o più nomi di dominio completi (FQDN);
- Certificati per **Firma** PEC: un indirizzo di posta elettronica;
- Certificati di **Autenticazione**: un indirizzo di posta elettronica.

Non sono emessi certificati SSL Server per indirizzi interni (internal server names), ossia appartenenti a reti private. Gli indirizzi di siti web che possono comparire nei certificati SSL Server devono essere FQDN (Fully Qualified Domain Names). Inoltre, non sono emessi certificati SSL Server per indirizzi IP.

3.2 Validazione iniziale dell'identità

3.2.1 Verifica di possesso della chiave privata

La dimostrazione del possesso, da parte del soggetto 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 [CSR]. La CA verifica che la firma digitale contenuta nella CSR sia valida.

3.2.2 Validazione dell'organizzazione richiedente

Prima di accettare una richiesta di certificato, la CA verifica che l'Organizzazione richiedente, come dichiarata nella documentazione di richiesta certificato (vedere il par. 5.1), sia effettivamente denominata come dichiarato dal richiedente, a meno di dettagli non significativi. A tal fine, la CA consulta fonti di informazione pubbliche affidabili come ad es. l'Indice Nazionale delle PA, l'Agenzia delle Entrate, ecc., secondo i casi.

3.2.3 Validazione dell'identità dei richiedenti

Prima di accettare una richiesta di certificato, la CA verifica che la richiesta sia autentica; a tal fine, la CA verifica che la **firma digitale** (ovvero **firma elettronica qualificata**) apposta sulla documentazione di richiesta (vedere il par. 5.1) sia una firma elettronica qualificata valida secondo le norme vigenti (in particolare secondo il [CAD]). È inoltre richiesto che il certificato del firmatario contenga l'attributo **organizationName** (O) nel campo Subject e che il valore di tale attributo corrisponda al nome dell'organizzazione richiedente.

3.2.4 Ulteriori verifiche svolte dalla CA

3.2.4.1 Per i certificati SSL Server

Per i certificati di tipo SSL Server, la CA verifica che i domini Internet da includere nei certificati siano sotto il controllo dell'organizzazione richiedente, ovvero che quest'ultima ne abbia la titolarità o che ne abbia il controllo di fatto.

Inoltre, si verifica che la chiave RSA contenuta nella CSR non sia una "weak key".

3.2.4.2 Per i certificati di Firma e di Autenticazione

Per i certificati di Firma e di Autenticazione, la CA verifica che l'Organizzazione richiedente abbia il controllo dell'indirizzo di posta elettronica da includere nel certificato.

3.2.5 Informazioni non verificate dalla CA

In generale, la CA non verifica la correttezza delle informazioni ricevute dal richiedente che non sono destinate ad essere incluse nel certificato e che non sono necessarie per l'emissione del certificato.

3.2.6 Identificazione e autenticazione delle richieste di rinnovo

Il processo di rinnovo è simile al processo di prima emissione: consiste nella generazione di una nuova coppia di chiavi, da parte del titolare, sostitutiva di quella in scadenza e nella richiesta alla CA di un corrispondente nuovo certificato, con le stesse modalità della prima emissione. Per il rinnovo sono seguiti gli stessi processi di identificazione ed autenticazione che si applicano alla prima emissione.

3.2.7 Identificazione e autenticazione delle richieste di revoca

L'organizzazione titolare di un certificato può richiederne la revoca mediante invio alla CA di un messaggio di PEC (vedere il par. 4.9.2 per i dettagli operativi). L'autenticazione delle richieste di revoca si basa sul fatto che devono essere trasmesse mediante PEC.

4 Requisiti operativi di gestione dei certificati

4.1 Richiesta del certificato

Per ogni certificato da emettere, il soggetto richiedente deve inviare all'Agenzia per l'Italia Digitale una richiesta di emissione certificato applicando la seguente procedura:

1) Il Responsabile dell'Organizzazione utilizza il modulo elettronico "**Richiesta di Registrazione**", reperibile sul sito web della CA (http://www.agid.gov.it/cps-ca) e lo compila. Il nome del file **.doc** così generato deve avere la seguente struttura: <NomeOrganizzazione>–<tipo certificato>–<progressivo>–<data>–RR.doc. Il <tipo certificato> può assumere i seguenti valori: "firma", "autenticazione", "ssl server"; la <data> deve avere il seguente formato: AAAAMMGG.

2) Il Responsabile dell'Organizzazione **firma digitalmente** il documento ottenuto al punto 1, ottenendo un file con estensione **p7m**.

3) Il Responsabile del Server (indicato nel modulo di cui al punto 1), genera la richiesta di certificazione CSR per il server da certificare, in formato PKCS#10. Il nome del file CSR deve avere la seguente struttura: <NomeOrganizzazione>–<tipo certificato>–<progressivo>–<data>.csr. Il <tipo certificato> può assumere i valori indicati al punto 1). La <data> deve avere il formato AAAAMMGG. Per generare la propria coppia di chiavi, deve essere utilizzato l'algoritmo **RSA**, con lunghezza delle chiavi di **2048 bit**.

4) Il Responsabile dell'Organizzazione genera un file archivio di nome <Nome Organizzazione>–<tipo certificato>–<progressivo>–<data>–Richiesta Certificato.zip contenente il file **p7m** generato al punto 1 ed il file CSR generato al punto 3.

Tutte le Richieste di emissione certificato (ossia i file .zip ottenuti al punto 4) vengono inviate in allegato ad un messaggio di PEC indirizzato a richiesta-certificati@pec-ic.agid.gov.it che deve avere come oggetto:

"**AgID-CA-Richiesta Certificato <Nome Organizzazione>**"

4.2 Elaborazione delle richieste

Alla ricezione di una richiesta di certificazione, la CA svolge le seguenti attività:

- svolge le verifiche descritte nel par. 4.3, tenendo conto dei vincoli di cui al par. 4.2;
- svolge le ulteriori verifiche descritte nel par. 4.4, secondo il tipo di certificato richiesto;

Se le verifiche sopra citate non hanno esito positivo, la CA segnala gli eventuali problemi al Richiedente, via PEC, e sospende la procedura di emissione in attesa della eventuale risoluzione dei problemi rilevati.

Dopo una settimana dalla segnalazione dei problemi, in assenza di riscontro da parte dell'organizzazione richiedente la pratica viene chiusa e l'organizzazione richiedente, se desidera ancora ottenere il certificato, deve trasmettere alla CA una nuova richiesta di certificazione come descritto al par. 5.1.

4.3 Emissione e consegna del certificato

Se le verifiche di cui alla sezione precedente sono superate, la CA svolge le seguenti attività:

- verifica che la CSR sia correttamente codificata e non contenga informazioni impreviste;
- verifica che le informazioni contenute nella CSR siano coerenti con quelle indicate nel modulo "Richiesta di Registrazione" (vedere il par. 5.1);
- verifica il possesso, da parte del richiedente, della chiave privata corrispondente alla CSR, come descritto nel par. 3.2.1.

Se le precedenti verifiche sono superate, l'operatore di CA:

- provvede alla registrazione del richiedente nel database della CA[2];
- genera il certificato e lo trasmette, assieme al certificato della CA intermedia, dalla casella PEC emissione-certificati@pec-ic.agid.gov.it alla casella PEC dell'Organizzazione titolare dalla quale è pervenuta la richiesta del certificato e, per conoscenza, alla casella di posta elettronica del responsabile del server indicata sul modulo "Richiesta di Registrazione".

Se invece le verifiche non hanno esito positivo, la CA segnala gli eventuali problemi alla casella PEC utilizzata dall'Organizzazione per richiedere il certificato, utilizzando la casella PEC emissione-certificati@pec-ic.agid.gov.it, e sospende la procedura di emissione in attesa della eventuale risoluzione dei problemi rilevati.

Dopo una settimana dalla segnalazione dei problemi, in assenza di riscontro da parte dell'organizzazione richiedente la pratica viene chiusa e l'organizzazione richiedente, se desidera ancora ottenere il certificato, deve trasmettere alla CA una nuova richiesta di certificazione come descritto al par. 4.1.

I certificati SSL Server sono conformi ai requisiti di Certificate Transparency secondo la specifica RFC 6962. Quando un certificato per sito web (dunque di tipo SSL Server) sta per essere emesso, un pre-certificato viene anzitutto generato e sottoposto ad un numero adeguato di CT log qualificati, in base alla Chromium CT Policy

[2] La registrazione del richiedente consiste nella memorizzazione, nel database della CA, dei dati identificativi dell'organizzazione richiedente ed altri dati necessari per la generazione del certificato.

di Google. 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).

4.3.1 Installazione del certificato

L'installazione del certificato è a cura dell'organizzazione titolare.

4.4 Accettazione del certificato

Nel caso il Richiedente riscontri eventuali imprecisioni o difetti del certificato, è tenuto ad informare immediatamente la CA tramite PEC all'indirizzo emissione-certificati@pec-ic.agid.gov.it.

Trascorsi 5 (cinque) giorni lavorativi dalla data di consegna del certificato, in mancanza di comunicazioni da parte del Titolare il certificato si considera accettato.

4.5 Riemissione del certificato

La riemissione del certificato a seguito di variazione dati, revoca o scadenza viene gestita come l'emissione di un nuovo certificato e richiede una nuova CSR (contenente una nuova chiave pubblica).

4.6 Modifica del certificato

Per rimediare ad eventuali errori nella generazione del certificato (per es. errori operativi da parte della CA oppure errori da parte del soggetto Richiedente nella compilazione della richiesta) è necessario emettere un nuovo certificato. A tal fine, il Richiedente deve fornire una nuova CSR (contenente una nuova chiave pubblica). In ogni caso, un certificato contenente informazioni errate sarà revocato dalla CA non appena ne venga a conoscenza.

4.7 Rigenerazione della chiave

Per ottenere un nuovo certificato, il titolare deve generare una nuova coppia di chiavi.

4.8 Revoca del certificato

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 e si completa con la sua pubblicazione nella Lista dei Certificati Revocati (CRL) pubblicata dal Certificatore. Il titolare di un certificato revocato deve rimuovere (de-installare) prontamente il certificato stesso dal server associato.

4.9 Circostanze per la revoca del certificato

Le condizioni che richiedono la revoca sono ad esempio (elenco non esaustivo[3]):

- richiesta da parte del Titolare;
- provvedimento dell'autorità giudiziaria;
- compromissione della chiave privata del Titolare (*);

[3] Per un elenco esaustivo dei casi in cui è necessaria la revoca dei certificati, si rimanda ai [BR].

- cessazione dell'attività del Titolare del certificato (*);
- il certificato contiene informazioni errate o non più valide (*);
- compromissione della chiave privata della CA emittente;
- il Titolare non ha rispettato una o più delle disposizioni del presente CPS (*);
- l'uso di un dominio contenuto nel certificato non è più consentito al Titolare (*);
- l'uso di un indirizzo di e-mail contenuto nel certificato non è più consentito al Titolare (*);
- nel caso di certificati di firma e dei certificati di Autenticazione: il Titolare è stato rimosso dall'elenco dei Gestori PEC accreditati e/o dall'IGPEC e/o non ha più diritto ad utilizzare il certificato a giudizio dell'AgID;
- cessazione del servizio di CA erogato dall'AgID in base a questo CPS, in mancanza di una CA sostitutiva che si faccia carico del servizio di revoca e pubblicazione delle informazioni sullo stato dei certificati;
- il certificato viene usato in modo improprio e/o illecito[4] (*);
- il certificato non rispetta la Root Store Policy di Mozilla [MRSP]; (*)
- il certificato non rispetta il presente CPS (*);
- il certificato non è conforme ai Requisiti [BR] (*).

In tutti questi casi, previo accertamento del loro effettivo verificarsi, la AgID CA revoca il certificato **entro 24 ore** e ne dà comunicazione al Titolare.

(*) Non importa il modo in cui, e su segnalazione di chi, la CA viene a conoscenza di queste situazioni: se la situazione è confermata, la CA revoca il certificato (vedere anche il paragrafo 4.13).

NB: Qualora la CA scopra che il certificato viene usato dal titolare per attività illecite (es. "Phishing", distribuzione di malware, ecc.) la CA effettuerà una revoca *immediata* e senza preavviso del certificato. Analogamente nel caso in cui la CA scopra che il certificato contiene erroneamente CA=TRUE nella estensione KeyUsage.

4.9.1 Chi può richiedere la revoca

La revoca può essere richiesta (secondo i casi):

- dal Titolare del certificato;
- dall'AgID in quanto CA;
- dall'autorità giudiziaria;
- dalla Root CA (Actalis).

Inoltre, chiunque può segnalare alla CA fatti o circostanze che (se confermate) possono, secondo i casi, giustificare la revoca del certificato (si rimanda al paragrafo 4.13),

[4] Non importa il modo in cui, e su segnalazione di chi, la CA viene a conoscenza di queste situazioni (vedere anche il paragrafo 4.13): se la situazione è confermata, la CA revoca il certificato

Si tenga presente che, in alcune circostanze, il Titolare ha l'obbligo di richiedere prontamente la revoca del certificato (vedere il cap. 9).

4.9.2 Modalità di richiesta revoca

Il Titolare può richiedere la revoca del proprio certificato per qualsiasi ragione, ma deve richiedere la revoca del certificato nelle seguenti circostanze:

- il certificato contiene informazioni errate o non più valide;
- la chiave privata corrispondente al certificato risulta compromessa.

Quest'ultima circostanza deve essere prontamente comunicata alla CA; in ogni caso, AgID non assume alcuna responsabilità per l'uso improprio della chiave privata associata alla chiave pubblica certificata.

Per richiedere la revoca di un certificato, il richiedente (che può essere il Titolare oppure la stessa AgID) deve inviare alla CA un messaggio di **PEC** all'indirizzo emissione-certificati@pec-ic.agid.gov.it con oggetto "**AgID-CA Richiesta di revoca**" (diversamente il messaggio non verrà preso in considerazione).

Il messaggio deve contenere informazioni sufficienti a identificare il certificato da revocare, per es.:

- il Subject DN ed il numero di serie del certificato
- oppure il certificato stesso (come file allegato).

Inoltre, il messaggio deve precisare il motivo della richiesta di revoca, per es.

- certificato non più necessario,
- chiave privata compromessa,
- ecc.

Nel caso in cui le informazioni siano incomplete o errate, la CA segnala il problema al richiedente, via PEC, restando in attesa delle necessarie precisazioni.

Se la richiesta è chiara e completa, la CA procede alla revoca del certificato nei tempi previsti, quindi conferma l'avvenuta revoca al richiedente via PEC.

Il servizio per richiedere la revoca è attivo dal Lunedì al Venerdì, dalle ore 8:00 alle ore 20:00 e Sabato dalle ore 8:00 alle ore 14:00, festivi esclusi. Per i soli certificati SSL Server, il servizio per richiedere la revoca è attivo 7x24.

4.10 Servizi informativi sullo stato dei certificati

Lo stato dei certificati (attivo, sospeso, revocato) è reso disponibile a tutti gli interessati mediante pubblicazione della Certificate Revocation List (CRL) col formato definito nella specifica [RFC5280].

Per i certificati di tipo SSL Server, inoltre, è disponibile un servizio di verifica on-line basato sul protocollo OCSP (On-line Certificate Status Protocol) e conforme alla specifica [RFC6960]. Questo servizio è esposto ai seguenti URL:

- http://ca1.agid.gov.it/OCSP (certificati di firma e di autenticazione)
- http://ca1.agid.gov.it/SSLOCSP (certificati SSL Server)

4.11 Gestione degli archivi

La CA conserva tutta la documentazione di richiesta di emissione di certificato (inclusa l'evidenza delle verifiche svolte) e di revoca per 7 anni dopo la scadenza del relativo certificato.

Traccia delle informazioni operative è inoltre mantenuta nel database della CA di cui viene effettuato il backup giornaliero.

4.12 Livelli di servizio

L'emissione del certificato avviene normalmente entro 3 giorni lavorativi dal ricevimento della "Richiesta di emissione certificato" entro il periodo di disponibilità di tale servizio (dal Lunedì al Venerdì, dalle 8:00 alle 20:00, Sabato dalle 8:00 alle 14:00, festivi esclusi), a condizione che la richiesta sia corretta.

La revoca del certificato avviene normalmente entro 24 ore dal ricevimento della richiesta, a condizione che la richiesta sia corretta.

L'accesso alle CRL è disponibile 7x24, salvo i fermi per manutenzione programmata.

4.13 Segnalazione di problemi

La CA mette a disposizione di tutte le parti interessate una casella di PEC che consente di segnalare alla CA, in qualsiasi momento, eventuali problemi relativi ai certificati già emessi (e già in uso), tali da poter giustificare una revoca anche immediata:

alert@pec-ic.agid.gov.it

Esempi di problemi che possono essere segnalati attraverso questo canale:

- compromissione della chiave privata
- uso illecito del certificato

Il segnalatore deve fornire almeno le seguenti informazioni, o la segnalazione sarà ignorata:

- nome e cognome;
- numero di telefono personale / diretto;
- organizzazione di appartenenza (se applicabile)
- descrizione (il più possibile dettagliata) del presunto problema;
- informazioni sufficienti per identificare il certificato oggetto della segnalazione. Le segnalazioni devono essere redatte in Italiano oppure in Inglese.

La CA si impegna a prendere in carico entro 24 ore le segnalazioni correttamente formulate, avviare le indagini sul problema segnalato (per accertarne la sussistenza) e prendere i necessari provvedimenti, secondo i casi e la severità del problema (cfr. il paragrafo 5.9.2). La priorità assegnata alla segnalazione dipenderà da:

- la natura del presunto problema;
- l'identità del segnalatore (per es. eventuali segnalazioni da parte dell'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 segnalato sia confermato, la CA deciderà 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.

5 Misure di sicurezza fisica ed operativa

L'infrastruttura tecnologica della AgID CA è gestita dal RTI per conto di AgID. In particolare, i sistemi di elaborazione della AgID CA sono installati presso i seguenti data center di Fastweb S.p.A.:

- via Caracciolo 51, Milano (sito primario)
- Via Fosso della Magliana 18, Roma (DR)

5.1 Sicurezza fisica

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a:

- Caratteristiche dell'edificio e della costruzione;
- Sistemi anti-intrusione attivi e passivi;
- Controllo degli accessi fisici;
- Alimentazione elettrica e condizionamento dell'aria;
- Protezione contro gli incendi;
- Protezione contro gli allagamenti;
- Modalità di archiviazione dei supporti magnetici;
- Siti di archiviazione dei supporti magnetici.

5.2 Sicurezza delle procedure

Il RTI definisce e mantiene un Piano della Sicurezza che analizza gli asset della AgID CA, i rischi a cui sono esposti e descrive le misure tecniche ed organizzative atte a garantire un adeguato livello di sicurezza delle operazioni. L'analisi dei rischi viene rivista periodicamente (almeno annualmente).

5.3 Copie di sicurezza (backup)

Una copia di sicurezza (backup) dei dati, delle applicazioni, dei log, di ogni altro file necessario al completo ripristino del servizio viene effettuata quotidianamente.

5.4 Disaster recovery

Per "disastro" s'intende un evento dannoso le cui conseguenze determinano l'indisponibilità del servizio in condizioni ordinarie, come per esempio nel caso di guasti e/o indisponibilità di una o più delle attrezzature (elaboratori, HSM, cablaggi, sale tecniche, alimentazione elettrica, ecc.) necessarie per erogare i servizi di certificazione della AgID CA. In questi casi sono previste apposite procedure finalizzate al ripristino (recovery) del servizio di certificazione AgID CA nel più breve tempo possibile. Tali procedure sono descritte nel Piano della Sicurezza.

6 Misure di sicurezza tecnica

6.1 Requisiti di sicurezza logica dei sistemi della CA

La piattaforma di CA è composta da vari moduli software. Per garantire la sicurezza dei dati e delle operazioni, tutto il software di sistema ed applicativo utilizzato per le funzioni di CA implementa le seguenti funzioni di sicurezza:

- controllo accessi;
- identificazione e autenticazione degli utenti e dei processi;
- imputabilità ed audit di ogni evento riguardante la sicurezza;
- gestione delle risorse di memorizzazione volta ad impedire la possibilità di risalire alle informazioni in precedenza contenute o registrate da altri utenti;
- autodiagnostica ed integrità dei dati e del software (controllo allineamento tra le copie operative e quelle di riferimento, controllo della configurazione del software, protezione dai virus);
- configurazione hardware e software per garantire la continuità del servizio.

6.2 Requisiti di sicurezza degli elaboratori

I sistemi operativi degli elaboratori utilizzati a supporto della infrastruttura di CA sono conformi alle specifiche previste dalla classe ITSEC F-C2/E2 oppure Common Criteria EAL4, equivalenti a quella C2 delle norme TCSEC.

6.3 Standard di sicurezza dei moduli crittografici

Le chiavi delle due CA emittenti di AgID ("AgID CA1" ed "AgID CA SSL SERVER") sono generate e custodite all'interno di un modulo crittografico hardware (HSM) dotato almeno della certificazione di sicurezza FIPS PUB 140 Level 3.

6.4 Algoritmi e lunghezza delle chiavi

Tutte le coppie di chiavi crittografiche (della CA e dei Titolari) sono di tipo RSA.

Le chiavi RSA delle due CA emittenti di AgID ("AgID CA1" ed "AgID CA SSL SERVER") hanno una lunghezza di 2048 bit.

Le chiavi RSA dei Titolari rispettano i seguenti requisiti:

- per i certificati di Firma, la lunghezza delle chiavi è di 2048 bit;
- per i certificati di Autenticazione, la lunghezza delle chiavi è di 2048 bit;
- per i certificati SSL Server, la lunghezza delle chiavi è di 2048 bit.

6.5 Sicurezza della rete

Il servizio di certificazione gode di un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi di firewalling e del protocollo SSL in modo da realizzare un canale sicuro tra tutti i soggetti abilitati all'accesso ai sistemi delle CA. Il sistema è altresì supportato da specifici prodotti di sicurezza (anti-intrusione di rete, monitoraggio, protezione da virus) e da tutte le relative procedure di gestione.

Inoltre, viene svolto almeno annualmente un vulnerability assessment (CA), avvalendosi di specialisti indipendenti, che copre anche i servizi on-line esposti dalla CA, per valutare l'opportunità di interventi di rinforzo della sicurezza.

6.6 Riferimento temporale

Tutti i sistemi di elaborazione usati dalla CA sono mantenuti allineati con l'ora esatta fornita da un time- server preciso ed affidabile.

7 Profilo dei certificati, CRL e OCSP

7.1 Certificato della CA che emette certificati per il circuito PEC

Il certificato della CA emittente che emette certificati per i Gestori PEC (certificati di firma e di autenticazione) ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<Include almeno 8 random bytes>
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	(non stipulata)
Subject	CN = AgID CA1 OU = Area Soluzioni per la Pubblica Amministrazione O = Agenzia per l'Italia Digitale L = Roma C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della Root CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true, pathLen=0
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
CertificatePolicies	PolicyOID = 1.3.76.16.3.1 CPS-URI = <URL di questo CPS sul sito dell'AgID>
NameConstraints	<come stabilito dalla Root CA>
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.2 Certificato della CA che emette certificati SSL Server per siti web sotto il controllo di AGID

Il certificato della CA emittente che emette certificati SSL Server per siti web sotto il controllo di AGID ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<Include almeno 8 random bytes>
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	(non stipulata)
Subject	CN = AgID CA SSL SERVER OU = Area Soluzioni per la Pubblica Amministrazione O = Agenzia per l'Italia Digitale L = Roma C = IT
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della Root CA>
Estensione	**Valore**
Basic Constraints	critico: CA=true, pathLen=0
AuthorityKeyIdentifier (AKI)	<valore dell'estensione della Root CA>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica>
KeyUsage	critico: keyCertSign, cRLSign
CertificatePolicies	PolicyOID = 1.3.76.16.3.1 CPS-URI = <URL di questo CPS sul sito dell'AgID>
NameConstraints	<come stabilito dalla Root CA>
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) serverAuth (1.3.6.1.5.5.7.3.1)
SubjectAlternativeName (SAN)	<assente>
AuthorityInformationAccess (AIA)	<indirizzo HTTP del servizio OCSP >
CRLDistributionPoints (CDP)	<indirizzo HTTP della ARL> <indirizzo LDAP della ARL>

7.3 Certificato di Firma

Il Certificato di Firma ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<Include almeno 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente: vedere il §7.1>
Validity	<3 anni>
Subject	C = <paese dove ha sede l'organizzazione> ST = <provincia dove ha sede l'organizzazione> L = <località dove ha sede l'organizzazione> O = <nome ufficiale dell'organizzazione> OU = <opzionale > CN = <nome comune del titolare>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature
ExtendedKeyUsage (EKU)	emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	PolicyOID = 1.3.76.16.3.1.1 CPS-URI = <URL di questo CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	rfc822Name=<indirizzo di posta elettronica di proprietà / sotto il controllo dell'organizzazione titolare del certificato>
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>

7.4 Certificato per Autenticazione

Il Certificato di Autenticazione ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<Include almeno 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente: vedere il §7.1>
Validity	<3 anni>
Subject	C = <paese dove ha sede l'organizzazione> ST = <provincia dove ha sede l'organizzazione> L = <località dove ha sede l'organizzazione > O = <nome ufficiale dell'organizzazione> OU = <opzionale > CN = <…>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies	PolicyOID = 1.3.76.16.3.1.2 CPS-URI = <URL di questo CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	rfc822Name=<indirizzo di posta elettronica di proprietà / sotto il controllo dell'organizzazione titolare del certificato>
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>

7.5 Certificato per sito web (SSL Server)

Il certificato per sito web (SSL Server) ha il seguente profilo:

Campo	**Valore**
Version	V3 (2)
SerialNumber	<Include almeno 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject della CA emittente: vedere il §7.2>
Validity	<1 anno>
Subject	C = IT ST = <provincia dove ha sede l'organizzazione> L = <località dove ha sede l'organizzazione > O = <nome ufficiale dell'organizzazione> OU = <opzionale > CN = <FQDN contenuto nella estensione SAN>
SubjectPublicKeyInfo	<chiave pubblica RSA da 2048 bit>
SignatureValue	<firma della CA emittente>
Estensione	**Valore**
Basic Constraints	(assente)
AuthorityKeyIdentifier (AKI)	<valore dell'estensione SKI della CA emittente>
SubjectKeyIdentifier (SKI)	<digest SHA1 della chiave pubblica secondo RFC5280>
KeyUsage	critico: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	clientAuth (1.3.6.1.5.5.7.3.2) serverAuth (1.3.6.1.5.5.7.3.1)
CertificatePolicies	PolicyOID = 2.23.140.1.2.2 PolicyOID = 1.3.76.16.3.1.3 CPS-URI = <URL di questo CPS sul sito dell'AgID>
SubjectAlternativeName (SAN)	<Uno o più FQDN, in conformità a [BR]>
CRLDistributionPoints (CDP)	<indirizzo HTTP di accesso alla CRL> <indirizzo LDAP di accesso alla CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	Elenco di Signed Certificate Timestamps secondo RFC 6962

7.6 Profilo delle CRL

Le CRL emesse dalla "AgID CA" sono conformi alla specifica pubblica RFC 5280 [CPROF].

7.7 Profilo OCSP

Il servizio OCSP erogato per la "AgID CA" è conforme alla specifica pubblica RFC 6960 [OCSP].

8 Verifiche di conformità

8.1 Frequenza e modalità delle verifiche

Con frequenza almeno trimestrale, viene svolta a cura della Root CA una verifica su almeno il 3% dei certificati emessi nel periodo, per verificare che i certificati esaminati rispettino il presente CPS.

8.2 Gestione delle eventuali non-conformità

Nel caso si rilevino certificati che non rispettano il presente CPS, tali certificati saranno revocati e, se necessario, sostituiti con nuovi certificati corretti.

9 Condizioni generali del servizio

La presente sezione disciplina il rapporto di servizio intercorrente tra AgID e i Titolari dei certificati emessi secondo questo CPS.

Il Richiedente, prima di chiedere l'emissione di un certificato, è tenuto a leggere ed approvare le condizioni generali di erogazione del servizio riportate all'interno del CPS. Con la sottoscrizione dei moduli di "Richiesta di Registrazione", di cui al paragrafo Processi Operativi, il firmatario dichiara di aver preso conoscenza e approvare tali condizioni.

I rapporti per l'erogazione dei servizi di certificazione per server sono sottoposti alla legge italiana. AgID, nell'erogazione dei propri servizi, opera conformemente alla normativa sulla protezione dei dati personali (privacy).

9.1 Obblighi del Certificatore

Il Certificatore si impegna a:

- Operare nel pieno rispetto del presente CPS.
- Ottenere dall'organizzazione richiedente, prima di emettere un certificato, l'accettazione delle condizioni generali del servizio AgID CA.
- Verificare la provenienza ed autenticità delle richieste di emissione certificato.
- Verificare che ogni richiesta di certificato sia autorizzata dall'Organizzazione richiedente.
- Verificare che il titolare possedeva, al momento dell'emissione del certificato, la corrispondente chiave privata.
- Garantire che, al momento dell'emissione di un certificato di Firma, il richiedente aveva la titolarità o il controllo dell'indirizzo di email incluso nel certificato.

- Garantire che le informazioni contenute nei certificati erano corrette e veritiere al momento dell'emissione dei certificati.
- Fornire un servizio efficiente, disponibile 7x24, per la revoca dei certificati.
- Per i certificati di tipo SSL Server, erogare un servizio online efficiente, disponibile 7x24, di consultazione sullo stato (valido oppure revocato) dei certificati emessi e non ancora scaduti.
- Trattare i dati personali dei Titolari nel rispetto delle norme vigenti.
- Revocare prontamente i certificati nelle circostanze previste in questo CPS.

9.2 Obblighi del Titolare

Il Titolare è obbligato a:

- Prima di richiedere un certificato, leggere con attenzione questo CPS.
- Fornire alla CA, in fase di richiesta e registrazione, informazioni esatte e veritiere.
- Generare e conservare la propria chiave privata in sicurezza, adottando le necessarie precauzioni per evitare danni, alterazioni o usi non autorizzati della stessa.
- Inviare alla CA la richiesta di certificazione con le modalità indicate nel presente CPS.
- Installare e utilizzare il certificato solo dopo aver controllato che esso contenga informazioni corrette.
- Non usare mai, per nessuna ragione, la propria chiave privata per emettere certificati.
- Utilizzare il certificato solo per gli scopi previsti nel presente CPS, e solo per finalità lecite.
- Informare tempestivamente AGID nel caso in cui le informazioni presenti nel certificato rilasciato non siano più valide, richiedendo la revoca del certificato stesso.
- Informare tempestivamente AGID nel caso in cui ritenga che la sicurezza del server su cui è stato installato il certificato possa essere stata compromessa, richiedendo la revoca del certificato stesso.
- Rimuovere prontamente dal server un certificato che sia stato revocato.
- Rispondere tempestivamente alle richieste della CA relative al possibile uso improprio del certificato o compromissione della chiave.

Il Titolare accetta che la CA, qualora e non appena scopra che un certificato SSL Server (per sito web) viene usato dal Titolare per attività illecite (es. "Phishing", distribuzione di malware, ecc.) e/o per l'emissione di altri certificati, effettuerà una revoca immediata e senza preavviso del certificato.

9.3 Obblighi delle Relying Parties

Si definisce "Relying Party" chiunque faccia affidamento su un certificato per prendere decisioni (come ad esempio: fornire informazioni confidenziali al titolare del certificato, considerare attendibili ed utilizzare le informazioni fornite o trasmesse dal titolare del certificato, ecc.). Per quanto riguarda i certificati emessi secondo questo CPS, le relying parties hanno l'obbligo di:

- compiere uno sforzo ragionevole per acquisire sufficienti informazioni sul funzionamento dei certificati e delle PKI in generale;

- verificare lo stato dei certificati emessi da AgID sulla base di questo CPS, accedendo ai servizi informativi descritti nella sezione 5.10;
- fare affidamento su un certificato solo se esso non è scaduto, sospeso o revocato.

9.4 Responsabilità del Certificatore

AGID non è responsabile, nei confronti del Richiedente o di utenti terzi, per eventuali danni, di qualsiasi tipo, derivanti dalla mancata emissione del certificato o da un uso improprio del certificato.

La responsabilità di AGID, nei confronti del Richiedente o di terzi, è comunque limitata al costo di emissione del certificato, fatti salvi i casi in cui l’art. 1229 del Codice Civile non consente tale limitazione.

9.5 Esclusione di garanzie

La CA non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente indicato in questo CPS o previsto dalle norme vigenti.

9.6 Comunicazioni e assistenza

Per avere maggiori informazioni sul presente CPS o sul servizio di CA qui descritto, si prega di inviare un e-mail all’indirizzo: richiesta-certificati@pec-ic.agid.gov.it.

9.7 Legge applicabile e Foro Competente

Le presenti Condizioni Generali sono soggette alla legge italiana. Per le controversie che dovessero insorgere tra le parti circa le disposizioni del presente CPS, competente a giudicare sarà esclusivamente il Foro di Roma.