

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

AGID

AGENZIA PER L'ITALIA DIGITALE

MANUALE OPERATIVO DEL SERVIZIO "DIGITPA-CA1"

CERTIFICATE PRACTICE STATEMENT

Redatto da:	Area Sistema Pubblico di connettività e cooperazione
Approvato da:	Francesco Tortorelli

DISTRIBUZIONE : Disponibile in forma Non Controllata

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Sommario

Sommario.....	2
MODIFICHE DOCUMENTO	4
DEFINIZIONI	4
RIFERIMENTI NORMATIVI	6
INTRODUZIONE.....	6
DATI IDENTIFICATIVI DEL CERTIFICATORE	7
MANUALE OPERATIVO.....	8
Dati identificativi del Manuale Operativo.....	8
Responsabile del Manuale Operativo.....	8
GENERALITÀ E APPLICABILITÀ.....	9
Certification Authority (CA)	9
Registration Authority (RA).....	10
Richiedente	10
Tipologia di certificati	10
SUPPORTO	11
Assistenza via e-mail.....	11
CONDIZIONI GENERALI DI EROGAZIONE DEL SERVIZIO	12
Obblighi del Certificatore.....	12
Obblighi del Richiedente.....	12
Responsabilità del Certificatore.....	13
Verso il Richiedente	13
Pubblicazione e directory	13
Informazioni sulla CA.....	13
CRL	13
Legge applicabile e Foro Competente	14
PROCESSI OPERATIVI	14
Registrazione dell'Organizzazione	14
Registrazione del Server	14
Verifica dei dati.....	14
Generazione del certificato.....	15
Pubblicazione del certificato.....	15
Accettazione del Certificato.....	15
Installazione del certificato.....	15
Variazione dei dati di registrazione	15
Revoca del certificato	16
Richiesta di revoca da parte del Richiedente.....	16
Richiesta di revoca da parte della CA.....	16

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Riemissione del certificato.....	16
Gestione degli archivi.....	16
Livelli di servizio	17
ASPETTI DI SICUREZZA	18
Sicurezza fisica	18
Sicurezza delle procedure.....	18
Sicurezza dei sistemi del Certificatore	18
Livello di sicurezza dei sistemi operativi degli elaboratori.....	18
Sicurezza della rete	19
Sicurezza del modulo crittografico	19
PROFILO DEI CERTIFICATI.....	20
Certificato radice "DIGITPA CA1"	20
Certificato server tipo "Posta Elettronica Certificata"	21
Certificato server tipo "Autenticazione"	22
Certificato server tipo "Web server"	23
MODULISTICA	24

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

MODIFICHE DOCUMENTO

DESCRIZIONE MODIFICA	EDIZIONE	DATA
Prima emissione	1.0	01/03/2011
Inserito il riferimento normativo D.L. 22-6-2012 nell'Introduzione	2.0	27/02/2013
<ul style="list-style-type: none"> - Modifica indirizzo Sede legale e sede operativa dell'Agenzia per l'Italia digitale. - Aggiornamento requisiti su lunghezza delle chiavi per certificati profilo WebServer e Autenticazione. - Eliminazione del fax per richiedere la revoca di un certificato. 	2.1	21/01/2014

DEFINIZIONI

Nel seguito sono invece indicati i termini specifici utilizzati nel presente Manuale Operativo.

DEFINIZIONE	DESCRIZIONE
AGID	Agenzia per l'Italia Digitale
Amministrazione	Amministrazione/Ente pubblico centrale o locale.
CA	Certification Authority
Certificatore	Soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi a quest'ultime.
CPS	Certificate Practice Statement – il presente documento
CRL	Certificate Revocation List -lista dei certificati revocati
CSR	Certificate Signing Request. Richiesta di certificazione
DigitPA	A decorrere dal 29 Dicembre 2009, a seguito del decreto 1° dicembre 2009, n. 177 il CNIPA viene riordinato con nuova denominazione DigitPA.
Gestore PEC	Società/Amministrazione/Ente che gestisce un servizio di Posta Elettronica Certificata
Manuale Operativo	Il presente documento, detto anche CPS
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

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

RSA	Rivest-Shamir-Adleman
SSL	Secure Socket Layer. Protocollo sicuro di comunicazione su una rete TCP/IP specificatamente destinata alla securizzazione dell'accesso ai siti Web.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

RIFERIMENTI NORMATIVI

Il Manuale Operativo è conforme a quanto previsto dalla legge italiana e in particolare:

RIFERIMENTO	DESCRIZIONE
[DPR44500]	DPR 28 dicembre 2000, n° 445 e successive modificazioni
[CODAMM]	Decreto Legislativo 5 marzo 2005, n.82 e successive modificazioni
[DPCM200309]	DPCM 30 marzo 2009
[CNIPACR48]	Circolare CNIPA. 6/09/2005 – n° 48
[CNIPADL4509]	Deliberazione CNIPA 21/05/2009 – n° 45
[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.

INTRODUZIONE

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 (12G0109), 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".

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

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 certificatore precedentemente assegnate a DigitPA sono riferibili e riferite ad AGID.

Il presente Manuale Operativo, altresì indicato come Certificate Practice Statement (CPS), definisce le procedure applicate dal Certificatore relativamente l’emissione di certificati digitali per server.

Le tipologie di certificati server prodotti sono tre:

- Certificati per la firma delle ricevute per la Posta Elettronica Certificata (PEC);
- Certificati per l’autenticazione ai siti Web;
- Certificati Web Server.

La prima tipologia di certificati è utilizzata dai server dei Gestori PEC per gli adempimenti previsti dalla norma.

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 destinata all’autenticazione dei server Web, sempre nell’ambito di connessioni sicure SSL. Questa categoria è a esclusivo uso di AGID.

DATI IDENTIFICATIVI DEL CERTIFICATORE

I dati identificativi relativi a AGID sono i seguenti:

Denominazione e Ragione sociale	AGID
Rappresentante legale	Agostino Ragosa
Sede legale	Via Liszt, 21 – 00144 Roma
Telefono	+39 06 852641
Fax	+39 06 85264414
Sede operativa	Via Liszt, 21 – 00144 Roma
Indirizzo E-mail	segreteriaadg@agid.gov.it
Indirizzo Internet	http://www.digitpa.gov.it

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

MANUALE OPERATIVO

Dati identificativi del Manuale Operativo

Il presente Manuale Operativo è identificato attraverso il numero di versione 2.1.

Esso si riferisce ai servizi di:

- Certificazione di chiavi pubbliche per la firma delle ricevute di Posta Elettronica Certificata.
- Certificazione di chiavi pubbliche di autenticazione del client SSL per server;
- Certificazione di chiavi pubbliche per Web Server.

Il presente Manuale Operativo è referenziato dal seguente OID (Object Identifier Number):

- 1.3.76.16.3.1 – Certificazione chiavi pubbliche server

Il corrispondente file in formato elettronico è identificato dal nome "MO_DigitPA-CA1_v2.1" ed è consultabile per via telematica all'indirizzo Internet: <http://www.digitpa.gov.it/manuali-operativi> .

Responsabile del Manuale Operativo

Il Responsabile del Manuale Operativo è:

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

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

GENERALITÀ E APPLICABILITÀ

Certification Authority (CA)

Per l'erogazione di certificati di chiave pubblica rivolti a soddisfare esigenze di sicurezza in Internet, AGID prevede l'utilizzo di una CA che consente il riconoscimento dei certificati emessi agli utenti finali con i prodotti di mercato (ad es. Internet Explorer , Firefox, Outlook, Thunderbird,...).

Dal 14/1/2011 è operativa un'infrastruttura che utilizza una chiave di certificazione denominata "DigitPA CA1". La CA con la quale sono emessi i singoli certificati per server è stata certificata dalla Autorità di Certificazione GTE Baltimore CyberTrust Root, il cui certificato radice è preinstallato nella quasi totalità dei prodotti di mercato. In questo modo, senza bisogno di alcun intervento da parte dell'utilizzatore, è possibile:

- il riconoscimento dell'attendibilità delle firme elettroniche apposte dai Gestori PEC;
- l'accesso e l'autenticazione ai siti Web mediante connessione SSL.

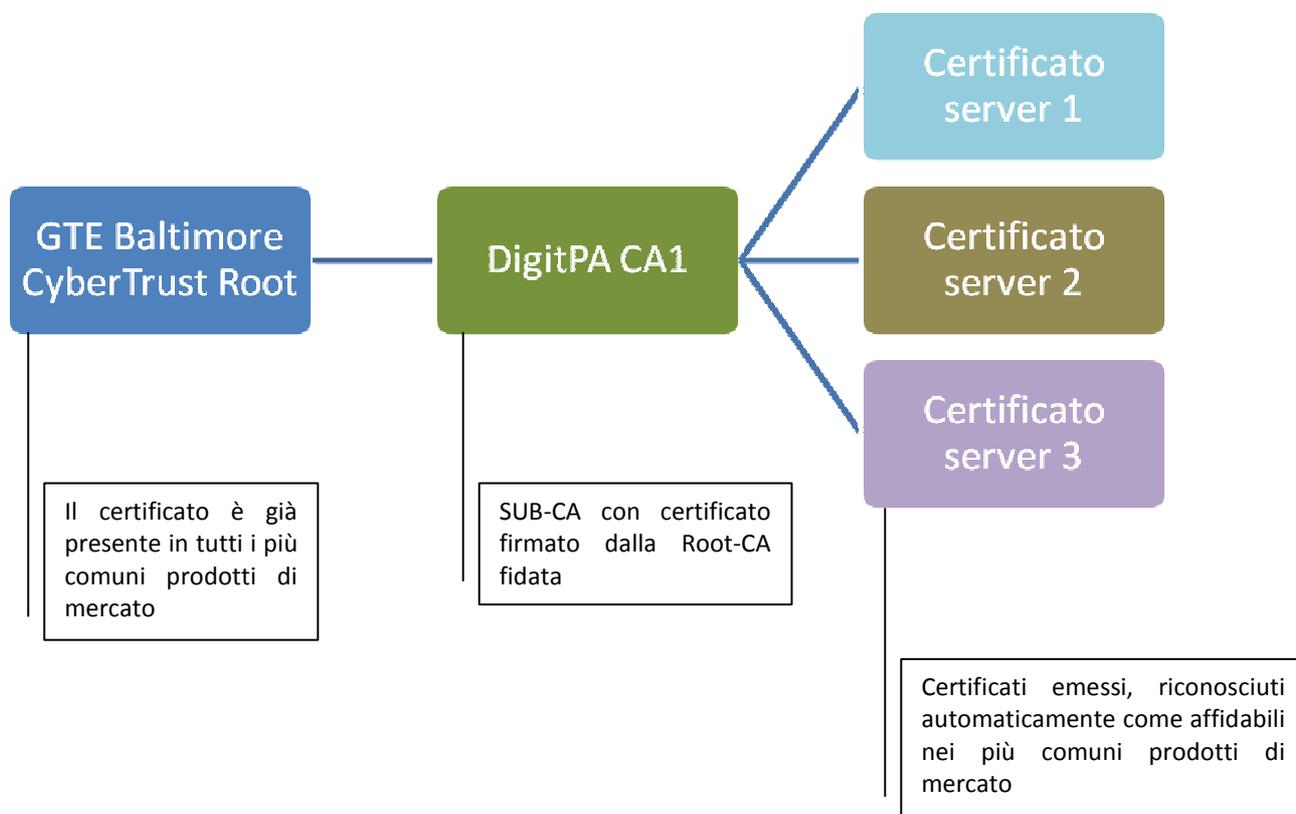


Figura 7.1–1: Gerarchia di certificazione di DIGITPA CA1

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Registration Authority (RA)

La funzione di verifica della documentazione di registrazione fornita dal Richiedente è svolta da AGID.

Richiedente

Il servizio di certificazione è svolto da AGID a favore dei soli Gestori PEC (Richiedenti).

Tipologia di certificati

Il presente CPS si riferisce all'emissione e gestione di certificati per:

- chiavi pubbliche per la firma delle ricevute di Posta Elettronica Certificata.
- chiavi pubbliche di autenticazione del client SSL per server;
- chiavi pubbliche per Web Server.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

SUPPORTO

Assistenza via e-mail

Per avere maggiori informazioni sul presente CPS o sul servizio e in caso di necessità di assistenza circa DigitPA-CA1 è possibile inviare un e-mail all'indirizzo: supportoCA@spcoop.gov.it .

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

CONDIZIONI GENERALI DI EROGAZIONE DEL SERVIZIO

La presente sezione disciplina il rapporto di servizio intercorrente tra AGID e il Richiedente il certificato.

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" e di "Nomina del Responsabile Server", 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).

Obblighi del Certificatore

AGID si impegna a:

- Verificare, secondo quanto descritto all'interno del presente CPS, la correttezza della documentazione fornita con la richiesta di certificazione;
- Rilasciare il certificato in accordo ai requisiti descritti nel presente CPS;
- Dare comunicazione, mediante pubblicazione nelle Liste di Revoca (CRL), della revoca dei certificati.

Obblighi del Richiedente

Il Richiedente è obbligato a:

- Fornire in fase di registrazione informazioni e documentazione 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 la richiesta di certificazione con le modalità indicate nel presente CPS;
- Installare il certificato digitale rilasciato da AGID in base al presente CPS unicamente sul server corrispondente al nome indicato nel medesimo certificato (relativo al campo CommonName);
- 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;
- Provvedere immediatamente a rimuovere dal server il certificato per il quale è stato richiesto la revoca.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Responsabilità del Certificatore

Verso il Richiedente

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.

Pubblicazione e directory

Informazioni sulla CA

AGID dal 14 Gennaio 2011, utilizza il certificato denominato "DigitPA CA1", operativo per i Gestori PEC dal 20 Gennaio 2011.

Per l'intero periodo di validità dei certificati server emessi in conformità al presente CPS, AGID s'impegna a pubblicare sul proprio sito web il presente CPS.

Si riportano di seguito i dati salienti dei certificati di CA dedicati al servizio descritto nel presente CPS:

DigitPA CA1

Dato	Valore
Soggetto (Subject)	CN = DigitPA CA1 OU = Ufficio interoperabilita' e cooperazione O = DigitPA C = IT
Emittente (Issuer)	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE
Periodo di validità	DA: venerdì 14 gennaio 2011 17.29 A: domenica 14 gennaio 2018 17.28.50

CRL

Le CRL sono pubblicate e aggiornate nei Directory LDAP una volta al giorno.

L'indirizzo del suddetto directory server è: **ldapca1.spcoop.gov.it**.

Le CRL potranno essere scaricate dalla seguente url:

<ldap://ldapca1.spcoop.gov.it/cn%3dDigitPA%20CA1,ou%3dUfficio%20interoperabilita%20e%20cooperazione,o%3dDigitPA,C%3dIT?certificateRevocationList>

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

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.

PROCESSI OPERATIVI

Registrazione dell'Organizzazione

Questo processo è a cura del Richiedente.

L'organizzazione che intende avvalersi dei servizi di certificazione server offerta da AGID invia tramite PEC, all'indirizzo gestoripec@cert.cnipa.it, una richiesta sottoscritta digitalmente nella quale nomina un responsabile dell'organizzazione, comunicandone i riferimenti telefonici ed e-mail, al quale sono assegnati i compiti di interfaccia attiva con AGID nelle fasi di registrazione e regolazione del ciclo di vita del certificato.

Registrazione del Server

Questo processo è a cura del Richiedente. La procedura da seguire, valida per ogni server da certificare, è la seguente:

1. Il Responsabile dell'Organizzazione compila il modulo "Nomina del Responsabile del Server" disponibile all'indirizzo: <http://www.digitpa.gov.it/manuali-operativi> ;
2. Il Responsabile del Server compila il modulo "Richiesta di Registrazione" disponibile all'indirizzo: <http://www.digitpa.gov.it/manuali-operativi> ;
3. Il Responsabile del Server genera, secondo le modalità previste dal sistema, la coppia di chiavi pubblica/privata da certificare e la relativa richiesta di certificazione (CSR). In particolare, la CSR contiene il nome del server da certificare (CommonName) che, nel caso di Web Server, dovrà corrispondere al dominio internet intestato all'Organizzazione richiedente.
4. La "Richiesta di Registrazione", unitamente alla "Nomina del Responsabile Server" e alla relativa CSR costituiscono la "Richiesta di emissione certificato".

Il Richiedente deve inviare ad AGID le richieste di emissione certificato come indicato nella "Procedura per la richiesta di emissione certificato" pubblicata all'indirizzo Internet <http://www.digitpa.gov.it/manuali-operativi>.

Verifica dei dati

Al ricevimento delle informazioni, AGID provvederà a:

1. controllare la richiesta di certificazione (CSR) e verificare la coerenza con i dati contenuti nella "Richiesta di Registrazione";
2. nel caso di certificato Web Server:
 - a. verificare l'univocità del nome di tipo X.500 (Distinguished Name, DN) nell'ambito dei propri certificati emessi;
 - b. controllare l'attribuzione del dominio internet relativo al Web Server alla Società/Ente/Amministrazione richiedente la certificazione;

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

- controllare l'autenticità della richiesta tramite verifica della firma digitale apposta sui moduli di richiesta di registrazione e nomina del responsabile server.

Se tutte le verifiche avranno avuto esito positivo seguirà la generazione del certificato.

AGID non darà corso all'emissione del certificato qualora i dati comunicati non risultino corretti e coerenti tra loro, siano incompleti in base ai riscontri delle verifiche poste in essere o non sia stata rispettata la "Procedura per la richiesta di emissione certificato".

Generazione del certificato

Se le verifiche previste hanno esito positivo, la CA genera il certificato in accordo al tipo di certificato indicato nel modulo "Richiesta di Registrazione", trascurando eventuali *usage* non previste ma presenti nel PKCS#10. In particolare il DN apparirà come valore del campo *Subject* del certificato. I tipi di certificato previsti dalla CA sono descritti nel paragrafo "Profilo dei certificati".

Se le verifiche non hanno esito positivo, AGID notifica l'evento al Richiedente, chiedendo la generazione di una nuova richiesta di certificazione.

Pubblicazione del certificato

Il certificato viene pubblicato nel Directory Server X.500 associato alla CA ed inviato all'indirizzo di posta elettronica del Responsabile dell'Organizzazione e al Responsabile del Server autorizzato.

Accettazione del Certificato

Nel caso il Richiedente riscontri eventuali imprecisioni o difetti del certificato, è tenuto ad informare immediatamente AGID tramite comunicazione all'indirizzo di posta elettronica: gestorip@cert.cnipa.it.

Se trascorsi 5 (cinque) giorni lavorativi dall'invio al Richiedente non sono pervenute segnalazioni, il certificato verrà considerato accettato.

Accettando il certificato, il Richiedente dichiara di accogliere i termini e le condizioni contenute nel presente CPS.

Installazione del certificato

Al ricevimento del certificato, il Richiedente potrà installarlo sul server, seguendo le istruzioni dello specifico prodotto utilizzato.

Variazione dei dati di registrazione

Il Richiedente deve informare tempestivamente AGID nel caso in cui sopravvengano delle variazioni dei dati contemplati nella "Richiesta di Registrazione". Se le variazioni riguardano dati presenti sul certificato, il Richiedente deve altresì richiedere per iscritto la revoca del certificato.

AGID si riserva la facoltà di revocare il certificato del Richiedente nel caso in cui la variazione dei dati di registrazione lo richieda.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Revoca del certificato

La revoca di un certificato si completa con la sua pubblicazione nella lista di revoca firmata dal Certificatore (CRL). Il certificato revocato non ha più validità ed il Richiedente deve provvedere immediatamente a rimuovere il certificato relativo dal server associato.

Richiesta di revoca da parte del Richiedente

Il Richiedente deve richiedere la revoca del certificato nelle seguenti circostanze:

- nel caso in cui le informazioni presenti sul certificato rilasciato non siano più valide;
- nel caso in cui ritenga che la sicurezza del server su cui è stato installato il certificato sia stata compromessa.

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

Per richiedere la revoca, il Richiedente deve inviare una mail contenente in allegato detta richiesta sottoscritta digitalmente all'indirizzo gestoripcc@cert.cnipa.it in cui venga esplicitamente richiesta la revoca del certificato per server con l'indicazione almeno della Ragione Sociale del Richiedente e del nome del server in oggetto. In seguito alla ricezione della email, AGID provvederà ad effettuare un controllo per verificare l'autenticità della richiesta.

La richiesta di revoca sarà verificata dalla RA che, in caso di verifica positiva, revocherà lo specifico certificato.

Il Certificato revocato sarà inserito nella CRL.

Il servizio per richiedere la revoca è attivo dal Lunedì al Venerdì, dalle ore 8:30 alle ore 17:00.

Richiesta di revoca da parte della CA

AGID può autonomamente revocare il certificato di un Richiedente solamente nelle seguenti circostanze:

- cessazione del Gestore PEC;
- evidenza della variazione dei dati contenuti nel certificato;
- evidenza dell'uso improprio del certificato.

In ogni caso, AGID, dopo aver effettuato la revoca, lo comunica al Richiedente.

Rimissione del certificato

La rimissione del certificato a seguito di variazione dati, revoca o scadenza viene gestita come emissione di un nuovo certificato.

Gestione degli archivi

AGID mantiene la documentazione di richiesta di emissione di certificato e di revoca per due anni

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

dopo la scadenza del relativo certificato.

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

Livelli di servizio

La generazione del certificato avviene entro 3 (tre) giorni lavorativi dal ricevimento della "Richiesta di emissione certificato" entro il periodo di disponibilità di tale servizio (dal Lunedì al Venerdì, dalle 8:30 alle 17:00).

La revoca del certificato avviene entro 1 (uno) giorno dal ricevimento della richiesta.

L'accesso ai Directory Server ed alle CRL è disponibile 7 giorni su 7, 24 ore su 24, salvo i fermi per manutenzione programmata.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

ASPETTI DI SICUREZZA

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.

Sicurezza delle procedure

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate nella gestione dei certificati, è previsto di affidare la gestione operativa del sistema a persone diverse con compiti separati e ben definiti.

Sicurezza dei sistemi del Certificatore

La piattaforma di gestione delle attività di certificazione è composta da vari moduli appartenenti alla suite software UniCERT della Verizon. Per garantire la sicurezza dei dati e delle operazioni, tutto il software di sistema ed applicativo utilizzati per le funzioni del Certificatore realizza le seguenti funzioni di sicurezza:

- Identificazione e autenticazione degli utenti e dei processi che richiedono di operare nel sistema;
- Controllo accessi
- 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.

Livello di sicurezza dei sistemi operativi degli elaboratori

Il sistema operativo degli elaboratori utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, sono conformi alle specifiche previste dalla classe ITSEC F-C2/E2 oppure Common Criteria EAL4, equivalenti a quella C2 delle norme TCSEC.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo “DigitPA CA1”		Edizione: 2.1 n.ro allegati: 0

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.

Sicurezza del modulo crittografico

Per la generazione delle firme digitali è utilizzato l’algoritmo RSA (Rivest-Shamir-Adleman).

Tutti i certificati emessi – a partire dai certificati relativi alle chiavi di certificazione, fino ai certificati relativi alle chiavi pubbliche dei server – vengono firmati utilizzando l’algoritmo RSA. Lo stesso algoritmo RSA deve essere utilizzato dal Richiedente per generare la propria coppia di chiavi.

Le chiavi di certificazione del certificato di CA sono lunghe 2048bit. Mentre le chiavi pubbliche dei server hanno lunghezza differente a seconda del template del certificato da emettere come descritto nel capitolo successivo.

- Per i profili “Posta elettronica certificata” la lunghezza delle chiavi deve essere pari a 1024bit
- Per i profili “Autenticazione” la lunghezza delle chiavi deve essere a 2048bit, a meno di eccezioni documentate.
- Per il profilo “WebServer” la lunghezza delle chiavi deve essere pari a 2048bit.

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

PROFILO DEI CERTIFICATI

Certificato radice "DIGITPA CA1"

Version	V3
Serial Number	07 27 48 a0
Signature	sha1RSA
Issuer	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE
Validity	DA: venerdì 14 gennaio 2011 17.29.56 A: domenica 14 gennaio 2018 17.28.50
Subject	CN = DigitPA CA1 OU = Ufficio interoperabilita' e cooperazione O = DigitPA C = IT
Alternative Subject Name	Email RFC822
Punti di distribuzione CRL	http://cdp1.public-trust.com/CRL/Omniroot2025.crl
Estensioni	
SubjectKeyIdentifier	fe 22 b7 24 e3 4f 27 d9 05 e0 cc b8 bd de f4 8d 23 fd 2f d9
AuthorityKeyIdentifier	e5 9d 59 30 82 47 58 cc ac fa 08 54 36 86 7b 3a b5 04 4d f0
Key Usage	Firma certificato, Firma CRL non in linea, Firma CRL (06)
Certificate policies OID	1.3.76.16.3.1
Certificate policies CPS URL	http://cybertrust.omniroot.com/repository.cfm
Restrizioni	Tipo oggetto=CA Limite lunghezza percorso=0

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Certificato server tipo "Posta Elettronica Certificata"

Version	V3
Serial Number	Numero di serie assegnato
Signature	sha1RSA
Issuer	CN = DigitPA CA1 OU = Ufficio interoperabilita' e cooperazione O = DigitPA C = IT
Validity	3 anni
Subject	C=IT O="User Organisation" CN="User Server name"
Estensioni	
Alternative Subject Name	Email RFC822
SubjectKeyIdentifier	SHA-1 160 bit della chiave pubblica
AuthorityKeyIdentifier	fe 22 b7 24 e3 4f 27 d9 05 e0 cc b8 bd de f4 8d 23 fd 2f d9
Key Usage	Firma digitale (80)
Certificate Policies: OID	1.3.76.16.3.1.1
Certificate Policies: URL CPS	http://www.digitpa.gov.it/manuali-operativi
Restrizioni	Tipo oggetto=End-entity Limite lunghezza percorso=0

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Certificato server tipo "Autenticazione"

Version	V3
Serial Number	Numero di serie assegnato
Signature	sha1RSA
Issuer	CN = DigitPA CA1 OU = Ufficio interoperabilita' e cooperazione O = DigitPA C = IT
Validity	3 anni
Subject	C=IT O="User Organisation" CN="User Server name"
Estensioni	
Alternative Subject Name	Email RFC822
SubjectKeyIdentifier	SHA-1 160 bit della chiave pubblica
AuthorityKeyIdentifier	fe 22 b7 24 e3 4f 27 d9 05 e0 cc b8 bd de f4 8d 23 fd 2f d9
Key Usage	Firma digitale (80), Crittografia chiave (20) (critical)
Extended Key Usage	Autenticazione client (1.3.6.1.5.5.7.3.2) Posta elettronica protetta (1.3.6.1.5.5.7.3.4)
Certificate Policies: OID	1.3.76.16.3.1.2
Certificate Policies: URL CPS	http://www.digitpa.gov.it/manuali-operativi
Restrizioni	Tipo oggetto=End-entity Limite lunghezza percorso=0

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo "DigitPA CA1"		Edizione: 2.1 n.ro allegati: 0

Certificato server tipo "Web server"

Il formato effettivo del certificato e la valorizzazione degli attributi e delle estensioni sarà deciso in base alle esigenze sistemiche del Richiedente.

Version	V3
Serial Number	Numero di serie assegnato
Signature	sha1RSA
Issuer	CN = DigitPA CA1 OU = Ufficio interoperabilita' e cooperazione O = DigitPA C = IT
Validity	3 anni
Subject	C=IT O="User Organisation" OU="User Unit name" CN="web Server domain name"
Estensioni	
SubjectKeyIdentifier	SHA-1 160 bit della chiave pubblica
AuthorityKeyIdentifier	fe 22 b7 24 e3 4f 27 d9 05 e0 cc b8 bd de f4 8d 23 fd 2f d9
Key Usage	Crittografia chiave (20)
Extended Key Usage	Autenticazione server (1.3.6.1.5.5.7.3.1)
Certificate Policies: OID	1.3.76.16.3.1.3
Certificate Policies: URL CPS	http://www.digitpa.gov.it/manuali-operativi
Restrizioni	Tipo oggetto=End-entity Limite lunghezza percorso=0

Emesso da: AGID	Tipo documento: Codice doc.: Data emissione:	Manuale Operativo MO_DigitPA-CA1 Gennaio 2014
Titolo documento: Manuale operativo “DigitPA CA1”		Edizione: 2.1 n.ro allegati: 0

MODULISTICA

Sul sito di AGID, all’indirizzo <http://www.digitpa.gov.it/manuali-operativi>, sono disponibili i moduli “Richiesta di Registrazione” e “Nomina del Responsabile Server” e la “Procedura per la richiesta di emissione certificato”, previsti dal presente CPS.