

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0



AGID

AGENZIA PER L'ITALIA DIGITALE

MANUALE OPERATIVO PER IL SERVIZIO "DIGITPA CERTIFICATI SERVER SPCoop"

CERTIFICATE PRACTICE STATEMENT

Redatto da:	
Approvato da:	

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

DISTRIBUZIONE : Disponibile in forma Non Controllata

Sommario

MODIFICHE DOCUMENTO	4
DEFINIZIONI	5
RIFERIMENTI NORMATIVI	6
INTRODUZIONE	7
DATI IDENTIFICATIVI DEL CERTIFICATORE	8
CPS	9
Dati identificativi del CPS	9
GENERALITÀ E APPLICABILITÀ.....	10
Certification Authority (CA)	10
Registration Authority (RA).....	10
Titolare.....	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 Titolare	12
Responsabilità del Certificatore.....	12
Pubblicazione e directory	13
Informazioni sulla CA	13
CRL	13
CDP della lista di revoca del certificato di CA:	13
CDP della lista di revoca dei certificati utente:	13
PROCESSI OPERATIVI	14
Registrazione	14
Generazione del certificato.....	14
Autenticazione al Portale.....	14
Porta di Dominio.....	14
Accettazione del Certificato.....	15
Variazione dei dati di registrazione	15
Revoca del certificato	15
Richiesta di revoca da parte del Titolare	15
Richiesta di revoca da parte della CA.....	16
Riemissione del certificato.....	16
LIVELLI DI SERVIZIO	18
ASPETTI DI SICUREZZA	19

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

Sicurezza fisica	19
Sicurezza delle procedure	19
Sicurezza del modulo crittografico	19
PROFILO DEI CERTIFICATI.....	20
Certificato radice "SPCoop CA1" – self-signed.....	20
Certificato utente "Porta di Dominio" – SPCoop CA1	21
Certificato utente "Autenticazione Web" – SPCoop CA1	22

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

MODIFICHE DOCUMENTO

DESCRIZIONE MODIFICA	EDIZIONE	DATA
Prima emissione	1.0	1 Febbraio 2011
Inserito il riferimento normativo D.L. 22-6-2012 nell'Introduzione	2.0	14 Marzo 2013

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

DEFINIZIONI

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

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.
CG - SICA	Centro Gestione SICA
CNIPA	Il Centro nazionale per l'Informatica nella Pubblica Amministrazione, che ha operato (fino al 28 Dicembre 2009) presso la Presidenza del Consiglio dei Ministri, è stato istituito con l'articolo 176 del Decreto legislativo n. 196 del 30 giugno 2003, in sostituzione dell'Autorità per l'informatica nella Pubblica Amministrazione. A decorrere dal 1° gennaio 2004, a seguito dell'art. 5 del decreto legislativo 5 dicembre 2003, n. 343, il CNIPA è divenuto Titolare anche dei compiti, funzioni e attività esercitate dal Centro Tecnico, tra cui quella di certificazione.
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.
Manuale operativo	Il presente documento, detto anche CPS
PKI	Infrastruttura a Chiave Pubblica (Public Key Infrastructure).
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
SICA	Servizi di Interoperabilità, Cooperazione ed Accesso
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: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 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.

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

INTRODUZIONE

Il Sistema Pubblico di Connettività e Cooperazione (SPC) si colloca nel contesto definito dal Decreto legislativo n° 82 del 7 marzo 2005, pubblicato in G.U. del 16 maggio 2005, n. 112, recante il "Codice dell'amministrazione digitale" (C.A.D.) e successive modifiche ed integrazioni. Esso istituisce il SPC, definendone gli obiettivi, le funzionalità ed il modello di governance.

Il processo di regolamentazione normativa del SPC è proseguito nel tempo, arrivando alla pubblicazione del Decreto del Presidente del Consiglio dei Ministri n.1 del 1 aprile 2008, pubblicato in G.U. del 21 giugno 2008, n. 144, recante le "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività", previste dall'art. 71, comma 1-bis, del C.A.D, con il quale viene definito il quadro tecnico di riferimento per lo sviluppo dei servizi SPC e le regole per il funzionamento e l'adesione ai servizi SPC.

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"*.

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 precedentemente assegnate a DigitPA sono riferibili e riferite ad AGID.

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

DATI IDENTIFICATIVI DEL CERTIFICATORE

I dati identificativi relativi a AGID sono i seguenti:

Denominazione e Ragione sociale	AGID
Rappresentante legale	Agostino Ragosa
Sede legale	Viale Marx, 31/49 – 00137 Roma
Telefono	+39 06 852641
Fax	+39 06 85264414
Sede operativa	Viale Marx, 31/49 – 00137 Roma
Indirizzo E-mail	segreteriaadg@agid.gov.it
Indirizzo Internet	http://www.digitpa.gov.it

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

CPS

Dati identificativi del CPS

Il presente CPS è identificato attraverso il numero di versione 2.0

Esso si riferisce ai servizi di:

- Certificazione di chiavi pubbliche per le Porte di Dominio
- Certificazione di chiavi di autenticazione ai siti Web

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

- 1.3.76.16.3.4.1.1 – Certificazione chiavi pubbliche server

Il corrispondente file in formato elettronico è identificato dal nome "MO_DigitPA_CertificatServerSPCoop_Ver2.0" ed è consultabile per via telematica all'indirizzo Internet: http://ca.SPCoop.gov.it/CPS/SPCoop_CPS.htm.

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

GENERALITÀ E APPLICABILITÀ

Certification Authority (CA)

Per l'erogazione dei certificati rivolti a soddisfare esigenze di sicurezza nell'ambito della Cooperazione Applicativa, il CG - SICA prevede l'utilizzo di una CA self-signed, in cui quindi la root CA deve essere inclusa nella lista delle Certification Authorities ritenute affidabili tramite una esplicita azione lato utente.

Registration Authority (RA)

Tutte le attività di registrazione sono svolte per il tramite del Portale SICA.

Titolare

Il Titolare è la persona fisica o l'apparato al quale è intestato il certificato. E' il soggetto che usa il certificato per gli usi consentiti e previsti dalla CA.

Tipologia di certificati

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

- chiavi pubbliche per le PDD (Porte di Dominio)
- certificati per l'autenticazione al portale SICA

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 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: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

CONDIZIONI GENERALI DI EROGAZIONE DEL SERVIZIO

La presente sezione disciplina il rapporto di servizio intercorrente tra il CG - SICA ed il Titolare del certificato.

Il Titolare prima di richiedere l'emissione di un certificato è tenuto a leggere ed approvare le condizioni generali di erogazione del servizio riportate all'interno del CPS.

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

Obblighi del Certificatore

Il CG - SICA 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 Titolare

Il Titolare 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 dal CG - SICA in base al presente CPS unicamente sul server corrispondente al nome indicato nel medesimo certificato (relativo al campo CommonName);
- Informare tempestivamente il CG - SICA nel caso in cui le informazioni presenti nel certificato rilasciato non siano più valide, richiedendo la revoca del certificato stesso;
- Informare tempestivamente il CG - SICA 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 stata richiesta la revoca.

Responsabilità del Certificatore

Il CG - SICA non è responsabile, nei confronti del Titolare 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 del CG - SICA, 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

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

limitazione.

Publicazione e directory

Informazioni sulla CA

Il CG - SICA dal 24 Gennaio 2011, utilizza il certificato denominato "SPCoop CA1", contestualmente reso operativo per i gestori.

Per l'intero periodo di validità dei certificati server emessi in conformità al presente CPS, il CG-SICA si 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:

SPCoop CA1

Dato	Valore
Soggetto (Subject)	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Emittente (Issuer)	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Periodo di validità	DA: lunedì 24 gennaio 2011 11.08.32 A: domenica 24 gennaio 2021 12.08.32

CRL

Le CRL sono pubblicate e aggiornate nei Directory LDAP una volta al giorno e potranno essere scaricate dai seguenti CDP, indicato anche all'interno del certificato di CA e dei certificati emessi:

CDP della lista di revoca del certificato di CA

<ldap://ldapca2.spcoop.gov.it/cn%3DSPCoop%20CA1,ou%3DServldap://ldapca2.spcoop.gov.it/cn%3DSPCoop%20CA1,ou%3DServizi%20di%20sicurezza%20e%20certificazione,o%3DDigitPA,C%3DIT?authorityRevocationList>

CDP della lista di revoca dei certificati utente

<ldap://ldapca2.spcoop.gov.it/cn%3DSPCoop%20CA1,ou%3DServldap://ldapca2.spcoop.gov.it/cn%3DSPCoop%20CA1,ou%3DServizi%20di%20sicurezza%20e%20certificazione,o%3DDigitPA,C%3DIT?certificateRevocationList>

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

PROCESSI OPERATIVI

Registrazione

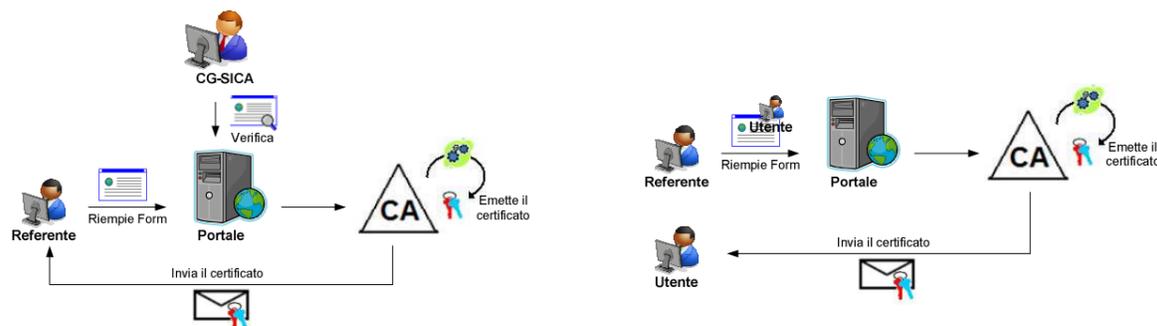
La procedura di registrazione coincide con la procedura di registrazione al Portale SICA.

Generazione del certificato

Autenticazione al Portale

Non è necessaria nessuna richiesta. La generazione del certificato di autenticazione avviene in automatico a fronte di una registrazione al Portale SICA.

Al ricevimento delle informazioni di registrazione al Portale, il CG-SICA, qualora si stia registrando un Referente di Amministrazione, effettuerà tutti i riscontri formali. Se le verifiche avranno avuto esito positivo, sarà autorizzata la generazione del certificato di autenticazione al Portale.



La registrazione degli altri utenti al Portale, verrà effettuata dal Referente che garantisce la validità dei dati inseriti. In questo caso sarà autorizzata automaticamente la generazione del certificato per l'utente registrato.

Il certificato prodotto sarà inviato al Titolare (Referente/utente) all'indirizzo di posta elettronica indicato in fase di registrazione.

Porta di Dominio

L'emissione del certificato di *Porta di Dominio* avviene a conclusione del processo di qualificazione.

la CA verificherà la correttezza del formato della CSR. Se le verifiche previste hanno esito positivo, la CA genera il certificato in accordo al profilo descritto nel paragrafo "Profilo dei certificati". Nel caso in cui nella richiesta CSR siano contenuti elementi o estensioni non previste

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

dallo specifico profilo, l'operazione procederà comunque con la generazione del certificato ignorando i dettagli non predefiniti nel profilo suddetto.
Al titolare sarà restituita quindi la CSR firmata, il certificato di CA necessario per la costruzione della catena di trust e le eventuali anomalie riscontrate.

Il Certificatore e AGID declinano da ogni responsabilità l'uso improprio dei certificati.
Si fa presente che tutti i certificati emessi tramite CSR, potranno essere riemessi, senza fornire elementi aggiuntivi alla richiesta stessa se non quelli necessari all'individuazione del certificato da rimettere. Il certificato, infatti, sarà rigenerato sulla base della CSR già presente negli archivi della CA [Vedi riemissione del certificato].

Accettazione del Certificato

Il Titolare è tenuto a verificare la correttezza delle informazioni contenute nel Certificato consegnato e segnalare immediatamente eventuali errori al Certificatore

Se trascorsi 5 (cinque) giorni lavorativi dall'invio al Titolare non sono pervenute segnalazioni, da inoltrare all'indirizzo supportoCA@spcoop.gov.it, il certificato verrà considerato accettato. Accettando il certificato, il Titolare dichiara di accogliere i termini e le condizioni contenute nel presente CPS.

Variazione dei dati di registrazione

Il Titolare, per il tramite del Portale SICA, deve informare tempestivamente il CG-SICA nel caso in cui sopravvengano delle variazioni dei dati contemplati nella fase di registrazione. Se le variazioni riguardano dati presenti sul certificato, il Richiedente deve altresì richiedere la revoca del certificato e il rinnovo (che verrà inteso come una riemissione) dello stesso.

Il CG-SICA si riserva la facoltà di revocare il certificato del Titolare nel caso in cui la variazione dei dati di registrazione lo richieda.

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, qualora lo stesso fosse utilizzato da una Porta di Dominio, a rimuoverlo immediatamente dal server.

Richiesta di revoca da parte del Titolare

La revoca di un certificato di autenticazione avviene in modo automatico a fronte di una revoca dello stesso utente all'utilizzo del Portale.

Negli altri casi, come:

- si vuole cessare il rapporto con il CG-SICA;
- le informazioni presenti sul certificato rilasciato non sono più valide;
- in cui si ritenga che la riservatezza della chiave privata del certificato sia stata compromessa o violata.

la richiesta dovrà pervenire all'indirizzo supportoCA@spcoop.gov.it e dovrà contenere le [seguenti informazioni](#)

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

- [il nome ed il cognome del richiedente della revoca.](#)
- [il codice IPA dell'amministrazione a cui è stato rilasciato il certificato.](#)
- [il seriale del certificato che si vuole revocare](#)
- [il Common Name \(CN\) del certificato che si vuole revocare](#)
- [la motivazione della revoca](#)
- [indicare se si vuole rimettere il certificato \(vedi il caso di revoca per motivi di sicurezza\).](#)

Ogni Utente può revocare solo il proprio certificato di autenticazione, mentre i Referenti saranno in grado di revocare i certificati degli utenti che appartengono alla propria Amministrazione. Tutti gli utenti possono revocare il certificato della Porta di Dominio della propria Amministrazione.

Durante la richiesta di revoca il sistema tratterà l'operazione per stabilire le corrette responsabilità in caso di richieste improprie, per le quali il CG-SICA non assume alcuna responsabilità.

Richiesta di revoca da parte della CA

Il CG-SICA può autonomamente revocare il certificato di un Richiedente solamente nelle seguenti circostanze:

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

In ambedue i casi, il CG-SICA, dopo aver effettuato la revoca, lo comunica al Titolare.

Rimissione del certificato

La richiesta di riemissione di un certificato potrà essere inoltrata all'indirizzo supportoCA@spcoop.gov.it.

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

Nel caso in cui la riemissione si renda necessaria per la scadenza del certificato in possesso la procedura di rinnovo sarà automatica,

Ogni utente può rimettere solo il proprio certificato di autenticazione, mentre i Referenti saranno in grado di richiedere una riemissione dei certificati intestati agli utenti che appartengono alla propria Amministrazione. Tutti gli utenti possono richiedere la riemissione del certificato della propria Porta di Dominio.

Ogni utente o Porta di Dominio può avere un unico certificato, pertanto la procedura di riemissione prevede che entro 30gg giunga una richiesta di revoca del certificato sostituito. In caso di rinnovo non è necessario procedere con la revoca poiché il certificato scadrà naturalmente.

Durante la richiesta di riemissione il sistema tratterà l'operazione per stabilire le corrette responsabilità in caso di richieste improprie, per le quali il CG-SICA non assume alcuna responsabilità.

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

LIVELLI DI SERVIZIO

La revoca del certificato avviene entro 2 (due) giorni lavorativi dal ricevimento della richiesta, entro il periodo di disponibilità del servizio (dal Lunedì al Venerdì, dalle 8:30 alle 17:00).

L'accesso ai Directory Server che pubblicano le CRL è reso disponibile 7 giorni su 7, 24 ore su 24, salvo i fermi per manutenzione programmata o interruzioni dovute cause di forza maggiore, caso fortuito, eventi catastrofici (incendi, terremoti, esplosioni).

Servizio	Disponibilità
L'accesso ai Directory Server ed alle CRL	7 giorni su 7, 24 ore su 24
Emissioni/Rinnovi/Revoche dei certificati	dal Lunedì al Venerdì, dalle 8:30 alle 17:00
• Emissioni di un certificato	3gg lavorativi
• Rinnovo di un certificato	3gg lavorativi
• Revoca	2gg lavorativi

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

ASPETTI DI SICUREZZA

Sicurezza fisica

L'ambiente CED del Certificatore prevede una serie di accorgimenti atti a garantire la sicurezza dei sistemi ivi presenti, con riferimento 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 del modulo crittografico

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

Tutti i certificati emessi vengono firmati utilizzando l'algoritmo RSA. Lo stesso algoritmo RSA deve essere utilizzato dal Richiedente per generare la propria coppia di chiavi, nel caso in cui la richiesta venga inviata sotto forma di CertificateSigningRequest in formato #PKCS10. Le chiavi pubbliche dei certificati emessi hanno lunghezza pari a 1024 bit, le chiavi di certificazione sono lunghe 2048 bit.

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

PROFILO DEI CERTIFICATI

Certificato radice "SPCoop CA1" - self-signed

Profilo del certificato di root della CA denominata "SPCoop CA1" che rilascerà tutti i certificati per la Cooperazione Applicativa. Essendo una CA self-signed deve essere inclusa nella lista delle Certification Authorities ritenute affidabili tramite una esplicita azione lato utente.

Version	V3
Serial Number	01
Signature	sha1RSA
Public Key Information	RSA 2048 bits
Issuer	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Validity	DA: lunedì 24 gennaio 2011 11.08.32 A: domenica 24 gennaio 2021 12.08.32
Subject	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Punti di distribuzione CRL	ldap://ldapca2.spcoop.gov.it/cn%3DSPCoop%20CA1,ou%3DServizi%20di%20sicurezza%20e%20certificazione,o%3DDigitPA,C%3DIT?authorityRevocationList
Estensioni	
SubjectKeyIdentifier	0b e1 2f 63 c8 02 65 44 1e 00 bd e9 91 8a 43 ce b3 6f 5e 19
AuthorityKeyIdentifier	0b e1 2f 63 c8 02 65 44 1e 00 bd e9 91 8a 43 ce b3 6f 5e 19
Key Usage	Firma certificato, Firma CRL non in linea, Firma CRL (06)
Certificate policies OID	1.3.76.16.3.4.1
Certificate policies CPS URL	http://ca.SPCoop.gov.it/CPS/SPCoop_CPS.htm
Restrizioni	Tipo oggetto=CA Limite lunghezza percorso=nessuno

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

Certificato utente "Porta di Dominio" – SPCoop CA1

Profilo del certificato rilasciato alle Porte di Dominio (il certificato è intestato ad un server). Ne è consentito l'uso per la Client/Server Authentication (SSL), Firma digitale e Cifra dati.

Version	V3
Serial Number	01
Signature	sha1RSA
Public Key Information	RSA 1024 bits
Issuer	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Validity	3 anni
Subject	CN = <SoggettoSPCoop>.spcoop.gov.it OU = <SoggettoSPCoop> O = SPCoop C = IT
Punti di distribuzione CRL	ldap://ldapca2.spcoop.gov.it/cn%3dSPCoop%20CA1,ou%3dServizi%20di%20sicurezza%20e%20certificazione,o%3dDigitPA,C%3dIT?certificateRevocationList
Estensioni	
SubjectKeyIdentifier	SHA-1 160 bit della chiave pubblica
AuthorityKeyIdentifier	0b e1 2f 63 c8 02 65 44 1e 00 bd e9 91 8a 43 ce b3 6f 5e 19
Key Usage	Firma digitale (80), Crittografia chiave (20), Crittografia dati (b0)
Certificate policies OID	1.3.76.16.3.4.1.1
Certificate policies CPS URL	http://ca.SPCoop.gov.it/CPS/SPCoop_CPS.htm

Emesso da: AGID	Tipo documento: Manuale Operativo Codice doc.: MO_Certificati ServerSPCoop Data emissione: Marzo 2013
Titolo documento: Manuale operativo per il servizio "DigitPA Certificati Server SPCoop"	Edizione: 2.0 n.ro allegati: 0

Certificato utente "Autenticazione Web" - SPCoop CA1

Profilo del certificato rilasciato agli utenti che hanno accesso al SICA (il certificato è intestato ad una persona). Ne è consentito l'uso solo per la Client Authentication (SSL).

Version	V3
Serial Number	01
Signature	sha1RSA
Public Key Information	RSA 1024 bits
Issuer	CN = SPCoop CA1 OU = Servizi di Sicurezza e Certificazione O = DigitPA C = IT
Validity	3 anni
Subject	CN = Utente OU = <SoggettoSPCoop> O = SPCoop C = IT
Punti di distribuzione CRL	ldap://ldapca2.spcoop.gov.it/cn%3dSPCoop%20CA1,ou%3dServizi%20di%20sicurezza%20e%20certificazione,o%3dDigitPA,C%3dIT?certificateRevocationList
Estensioni	
SubjectKeyIdentifier	SHA-1 160 bit della chiave pubblica
AuthorityKeyIdentifier	0b e1 2f 63 c8 02 65 44 1e 00 bd e9 91 8a 43 ce b3 6f 5e 19
Key Usage	Firma digitale (80), Crittografia chiave (20)
Extended Key Usage	Autenticazione client (1.3.6.1.5.5.7.3.2)
Certificate policies OID	1.3.76.16.3.4.1.2
Certificate policies CPS URL	http://ca.SPCoop.gov.it/CPS/SPCoop_CPS.htm