



Qualificazione della Porta di Dominio con il concorso degli Enti Regionali

Versione 1.0



Nome doc.:

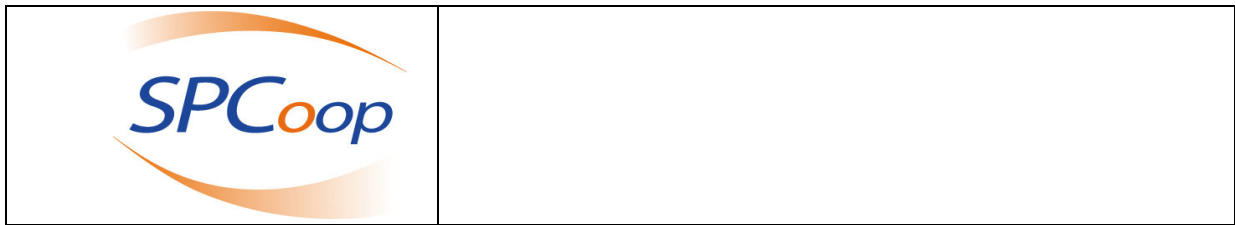
**SPCcoop-Qualificazione della Porta
di Dominio Enti Regionali_V1.0**

Versione: **1.0**

Data emissione:

21 Ottobre 2009

Stato: **pubblicato**



INDICE

1.	PREFAZIONE	3
1.1.	Autori	3
1.2.	Modifiche Documento	3
1.3.	Riferimenti	4
1.4.	Acronimi e Definizioni.....	4
2.	OBIETTIVI E CONTESTO DI RIFERIMENTO.....	5
2.1.	Scopi del documento.....	7
2.2.	Note di lettura del documento	7
2.3.	Note sul Copyright	8
3.	PROCESSO DI QUALIFICAZIONE PER GLI ENTI REGIONALI	9
3.1.	Introduzione al processo	9
3.2.	Schema di processo	10
3.3.	Definizione dei ruoli delle Regioni e degli enti territoriali	13
4.	ALLEGATI	14
	Allegato 1	14
	Allegato 2.....	15
	Allegato 3.....	17
	Allegato 4.....	18
	Allegato 5.....	19
	Allegato 6.....	20
	Allegato 7.....	21



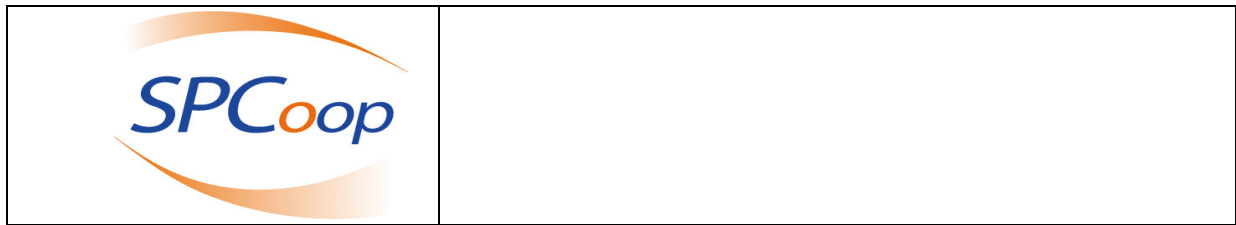
1. PREFERENZA

1.1. Autori

Redatto da:	Alfio Raia	CNIPA
	Alessandro Vinciarelli	CNIPA
Verificato da:	Alfio Raia	CNIPA
Revisione a cura di:	Giovanni Olive	CNIPA
Validato da:	Francesco Tortorelli	CNIPA

1.2. Modifiche Documento

Descrizione Modifica	Edizione	Data
Emissione Prima Versione	0.9	02/09/2009
Revisione impaginazione finale	1.0	21/10/2009



1.3. Riferimenti

Codice	Titolo

1.4. Acronimi e Definizioni

Sigla	Descrizione



2. OBIETTIVI E CONTESTO DI RIFERIMENTO

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.

Parallelamente, come previsto dal modello condiviso di cooperazione applicativa per la P.A. italiana *SPCoop*, è stato avviato e portato a termine lo sviluppo dei *Servizi Infrastrutturali di interoperabilità, cooperazione ed accesso (SICA)* e del centro di gestione per l'erogazione di tali servizi (CG-SICA), infrastruttura condivisa a livello nazionale che abilita l'interoperabilità e la cooperazione applicativa fra le Amministrazioni pubbliche nonché l'accesso ai servizi applicativi da queste sviluppati e resi disponibili su SPC.

L'evoluzione dello scenario di riferimento e la disponibilità di servizi di infrastruttura per la cooperazione applicativa, hanno reso necessaria la definizione e pubblicazione di una serie di documenti che specificassero in dettaglio le modalità tecniche per l'interoperabilità e la cooperazione applicativa e l'utilizzo dei servizi SICA, come peraltro prevista dalle succitate regole tecniche.

Gli ultimi documenti tecnici relativi al SPCoop rilasciati alla fine del 2005, infatti, definivano un livello di condivisione che consentiva sia la stabilità del modello nel tempo rispetto al contesto organizzativo e tecnologico di riferimento, sia i necessari gradi di libertà per la sua implementazione; ciò a scapito del dettaglio tecnico necessario, invece, nel momento in cui si fa riferimento ad una specifica implementazione del modello ed a specifici servizi infrastrutturali.

Questo specifico documento è stato redatto dal CNIPA, in maniera complementare agli altri documenti dell'insieme che sono stati invece redatti dal Raggruppamento Temporaneo di Imprese (IBM-Sistemi Informativi), incaricato dello sviluppo e dell'implementazione del Centro di Gestione dei servizi SICA, con la supervisione ed il supporto del CNIPA, e nasce dalla necessità di definire, in ottemperanza a quanto previsto dal DPCM 1 Aprile 2008, una modalità per la qualificazione della porta di dominio che prevede il concorso delle regioni come organismi di attuazione e controllo del Sistema Pubblico di Connettività.



L'insieme di documenti prodotti specifica i modelli, le modalità, i dettagli tecnici di realizzazione, gestione ed utilizzo dei servizi SICA, le modalità di interfacciamento, le procedure qualificazione e gestione dei componenti infrastrutturali SPCoop, sulla base di quanto già previsto e definito nei documenti precedentemente condivisi e nel rispetto delle succitate regole tecniche.

Titolo Documento
1. Introduzione ai servizi SICA
2. Specifiche di nomenclatura in SPCoop
3. Specifiche di utilizzo del Servizio di Registro SICA
4. Modalità di funzionamento del Client SICA
5. Struttura dell'Accordo di Servizio e dell'Accordo di Cooperazione
6. Descrizione delle specifiche di sicurezza negli Accordi di Servizio
7. Aspetti di sicurezza applicativa nella cooperazione fra servizi
8. Modalità di funzionamento del Catalogo Schemi e Ontologie
9. Interfacce applicative tra Registro SICA generale e Registri SICA secondari
10. Modalità di Qualificazione del Registro SICA secondario
11. Modalità di Qualificazione della Porta di Dominio
12. Schema d'interoperabilità IndicePA
13. Guida ai servizi IndicePA
14. Modello di Gestione Federata delle Identità Digitali (GFID)
15. Modalità di accreditamento alla GFID
16. Modello di funzionamento dell'Indice dei Soggetti
17. Modello di funzionamento della Certification Authority

A cui si sono aggiunti, nel tempo, i seguenti documenti:

Titolo Documento
18. Qualificazione della Porta di Dominio con il concorso degli Enti Regionali



2.1. Scopi del documento

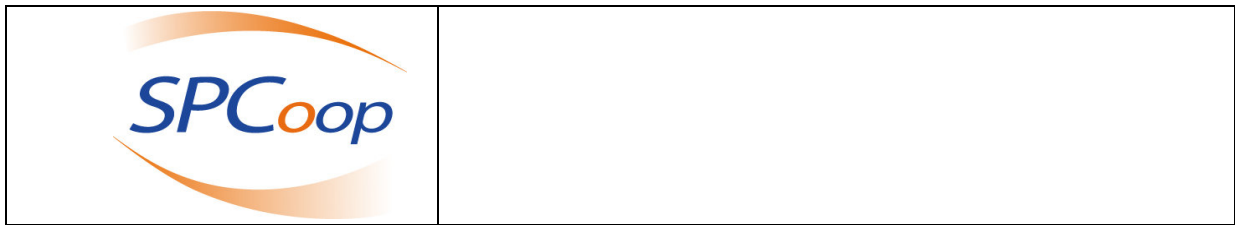
Obiettivo del documento è definire una modalità per la qualificazione della porta di dominio che prevede, in ottemperanza a quanto previsto dal DPCM 1 Aprile 2008, il concorso delle regioni, come organismi di attuazione e controllo del Sistema Pubblico di Connettività.

Tale modalità consente un più rapido espletamento delle procedure previste per la qualificazione grazie alle intermediazione delle regioni, per mezzo dei propri centri di competenza tecnologica, nei confronti degli enti territoriali ed esse afferenti che hanno la necessità di qualificare la propria porta di dominio e non dispongono di adeguate strutture per portare avanti autonomamente le attività.

2.2. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con [RFC2119]. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'è proibizione assoluta di implementazione di un determinato elemento di specifica.

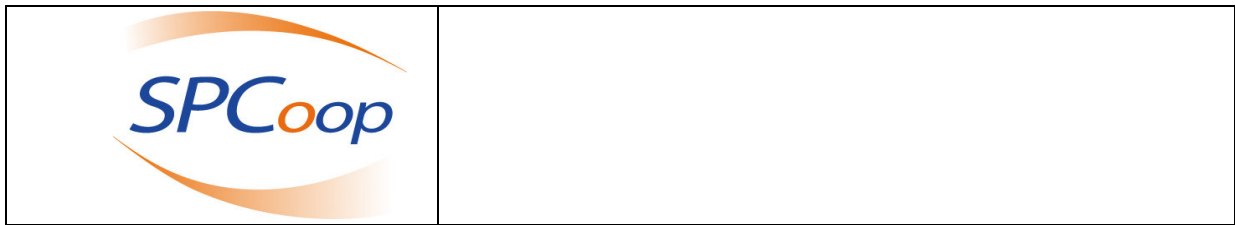


2.3. Note sul Copyright

Il presente documento ed i suoi contenuti sono di proprietà del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) e sono protetti dalle norme sul diritto d'autore e dalle altre norme applicabili.

Il presente documento ed i suoi contenuti sono messi a disposizione sulla base dei termini della licenza d'uso disponibile al seguente indirizzo:

http://www.cnipa.gov.it/site/_files/SPCoop-LicenzaUso_v1.0_20051014.pdf



3. PROCESSO DI QUALIFICAZIONE PER GLI ENTI REGIONALI

3.1. Introduzione al processo

La procedura discende dai commi 2 e 4 del DPCM 1 Aprile 2008 “Regole tecniche e di sicurezza per il funzionamento del sistema pubblico di connettività” di seguito riportati

Art29 comma 2

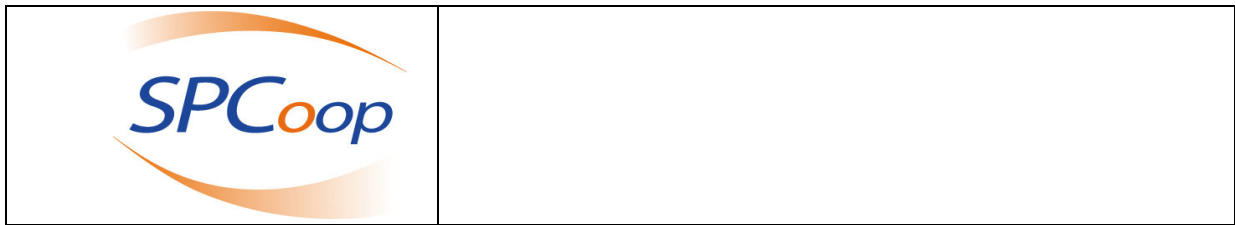
“Il processo di qualificazione della porta di dominio prevede la verifica dell'interoperabilità tra le porte di dominio, il rispetto dei requisiti funzionali previsti per le stesse, come definiti nella documentazione tecnica di cui all'art. 13, comma 3 ed il rilascio del certificato digitale, associato alla porta qualificata, attraverso il servizio di certificazione di cui all'art. 15, comma 4, lettera e)”

Art29 comma 4

“Le Amministrazioni che intendano utilizzare una tipologia di porta di dominio già qualificata, possono richiederne, anche per il tramite degli Organismi di attuazione e controllo, la pubblicazione direttamente attraverso il servizio di registro SICA.”

Gli enti regionali, qualificando la loro porta secondo il processo attualmente operativo per il tramite del servizio erogato dal Centro Gestione SICA, definiscono una tipologia di porta, che a norma dell'art. 29 comma 4 può essere adottata da altre amministrazioni.

Gli stessi enti regionali, come Organismi di Attuazione e Controllo, richiedono, per conto delle amministrazioni che intendono adottare la loro tipologia di porta qualificata, la pubblicazione della stessa attraverso il registro SICA, come prevede sempre dell'art. 29 comma 4. Questa richiesta determina l'iscrizione nell'elenco delle porte qualificate ed il rilascio da parte del Centro Gestione SICA del certificato digitale in ottemperanza all'art. 29 comma 2.



Le porte così qualificate seguono lo stesso ciclo di vita della porta regionale del cui modello rappresentano una istanza, in quanto per queste porte le verifiche di interoperabilità discendono implicitamente da quelle sostenute dalla porta regionale. In forza di ciò le regioni che concedono l'impiego del modello di porta qualificata sono i responsabili dal punto di vista tecnologico, relativamente all'aspetto dell'interoperabilità, della piattaforma durante tutto il suo ciclo di vita. In merito al dispiegamento poi si impegnano a rilasciare l'istanza del modello nella stessa configurazione adottata in fase di qualifica, compreso il servizio di test utilizzato per le prove tecniche, nonché a tenerla allineata ad ogni aggiornamento eventualmente apportato al modello originario.

Nella gestione del ciclo di vita delle porte qualificate, è previsto periodicamente un controllo a campione sulle porte in produzione, eseguito remotamente dal CG-SICA, attraverso la l'esecuzione della sequenza dei test già sostenuti in fase di qualificazione. Le porte dispiegate secondo il procedimento descritto sono soggette alla stessa tipologia di controllo.

Infine, poiché la pubblicazione della porta presso il registro SICA avviene mediante IPA, la richiesta da parte di una amministrazione comporta implicitamente l'iscrizione all'IPA della stessa, qualora non sia già iscritta.

3.2. Schema di processo

1. L'ente regionale dispiega presso le amministrazioni richiedenti istanze di porta di dominio sul modello di porta qualificata e configurate secondo il profilo già adottato dall'ente regionale stesso (a meno dei parametri eventualmente riferiti alla nomenclatura). Tale sistema deve ospitare il servizio di test utilizzato per la qualificazione della porta regionale.
2. L'ente regionale comunica al CG-SICA
 - a. tutte le informazioni ad esso relative in particolare:
 - Nome esteso dell'Ente Regionale,
 - Codice IPA dell'Ente Regionale
 - Nome amministratore della porta di dominio per l'Ente Regionale,
 - Cognome amministratore della porta di dominio per l'Ente Regionale,
 - Indirizzo e-mail amministratore della porta di dominio per l'Ente Regionale,
 - b. l'elenco delle porte dispiegate riportando per ciascuna di esse:
 - tutte le informazioni necessarie per l'accreditamento dell'amministrazione presso i servizi del GC-SICA a seconda se la stessa risulta già essere accreditata presso l'IPA oppure non presente.



Nel primo caso le informazioni da riportare sono le seguenti¹:

- Nome esteso Amministrazione,
- Nome referente per l'Amm.ne,
- Cognome referente,
- Codice Fiscale referente,
- Indirizzo e-mail referente,
- Telefono referente,

Nel secondo in aggiunta alle prime dovranno essere riportate :

- Indirizzo sede legale Amm.ne,
- CAP sede legale Amm.ne,
- Città sede legale Amm.ne,
- Provincia sede legale Amm.ne,
- Regione sede legale Amm.ne,
- Nome responsabile,
- Cognome responsabile,
- Titolo del responsabile,
- Indirizzo del sito istituzionale,
- Indirizzo e-mail dell'amministrazione,
- Dominio di Posta Elettronica Certificata,

- tutte le informazioni necessarie per la richiesta di accreditamento al servizio di qualificazione:

- Codice IPA (Se disponibile),
- Identificativo Soggetto SPCoop (proposto),

¹ Ai sensi del D. Lgs. 30 giugno 2003, n. 196 sulla tutela dei dati personali, il trattamento dei dati avviene con procedure idonee a tutelare la riservatezza dell'Utente e consiste nella loro raccolta, registrazione, organizzazione, conservazione, elaborazione degli stessi unicamente per le finalità connesse all'erogazione del servizio



- Identificativo Soggetto SPCoop (definitivo),
- Descrizione,
- Nome Amministratore (coincide con quello del referente PA),
- Cognome Amministratore (coincidente con quello del referente PA),
- Casella di posta elettronica (coincidente con quello del referente PA),
- EndPoint,
- EndPoint risposta,
- Common Name Certificato.
- Modalità richiesta PKCS10/PKCS12
- File name PKCS10

I dati vengono comunicati al CG-SICA tramite un messaggio di posta elettronica alla casella *helpdesk@spcoop.gov.it* contenente in allegato un foglio elettronico sul modello riportato in appendice. Il CG-SICA fornisce, al momento della ricezione, un messaggio di risposta con valore di presa in carico. Successivamente, in seguito al processamento, il foglio in allegato viene restituito con i dati validati (*Codice IPA*, per le amministrazioni di nuova iscrizione all'Indice delle Pubbliche Amministrazioni, e *Identificativo Soggetto SPCoop validato*).

3. Il CG-SICA spedisce al referente dell'amministrazione indicato alla casella di posta indicata nel campo *Indirizzo e-mail referente* le UserId & Password per l'accesso al portale dei servizi, con un messaggio secondo il modello indicato in Allgato 3.
4. Il CG-SICA rilascia all'ente regionale i certificati per le porte dispiegate e iscrive le porte presso l'elenco delle porte qualificate. Per ogni ente territoriale per il quale si richiede la qualificazione, il certificato e la relativa passphrase vengono recapitati all'amministratore della porta di dominio per l'Ente Regionale della regione richiedente, con due distinti messaggi di posta alla casella indicata nel campo *Indirizzo e-mail amministratore della porta di dominio per l'Ente Regionale*. (Allegati 4 e 5). Per tali messaggi occorre fornire risposta a i del riscontro di avvenuta ricezione.
5. L'ente regione, man mano che procede all'installazione dei certificati, verifica, in collaborazione con il CG-SICA², la raggiungibilità³ delle porte dallo stesso CG-SICA.

² Previa precedente pianificazione sulle date delle attività



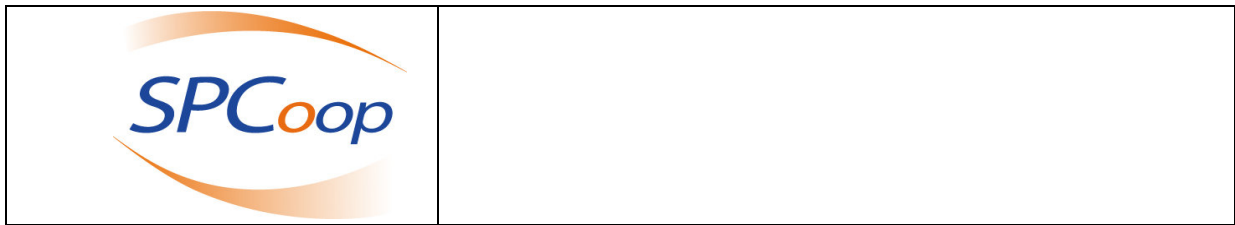
L'avvenuta messa in produzione delle porte dovrà poi essere confermata per mezzo di messaggio di posta elettronica che accluda una tabella sul modello indicato nell'Allegato 6.

3.3. Definizione dei ruoli delle Regioni e degli enti territoriali

Il processo proposto determina l'adesione degli enti territoriali a SPCoop, in particolare comporta l'iscrizione presso l'Indice Nazionale delle PA per tutti quelli precedentemente non presenti. Spetterà quindi all'ente territoriale la gestione di tutte le attività previste (pubblicazione accordi di servizio, popolamento IPA ed Indice dei Soggetti etc.) e a tal fine il referente PA dell'ente, referenziato nelle richiesta delle Regioni, riceverà all'indirizzo e-mail, riportato nella stessa, le credenziali per l'accesso al portale dei servizi. Le credenziali fornite di default saranno UserId e Password, successivamente su esplicita richiesta saranno fornite le credenziali X509 (certificati di autenticazione) che consentiranno la piena operatività.

Alle regioni che opereranno il dispiegamento resta sempre e comunque l'onere del mantenimento della piattaforma operante come Porta di Dominio per tutta il periodo della sua permanenza in produzione, pertanto l'amministratore della Porta di Dominio dell'ente regione è da considerarsi a tutti gli effetti amministratore della porta di dominio dell'ente territoriale, anche se quest'ultimo dovesse, come nelle sue prerogative, nominarne uno proprio.

³ Si vedano le raccomandazioni contenute in allegato 7



4. ALLEGATI

Allegato 1

Tabella ente regionale

Riferimenti ente regionale

Nome esteso dell'Ente Regionale	
Codice IPA dell'Ente Regionale*	
Nome amministratore della porta di dominio per l'Ente Regionale	
Cognome amministratore della porta di dominio per l'Ente Regionale	
Indirizzo e-mail amministratore della porta di dominio per l'Ente Regionale	

* reperibile presso il portale IPA come da nota



Allegato 2

Tabella ente territoriale

Informazioni per l'accreditamento ai servizi SICA

Nome esteso Amministrazione	
Nome referente per l'Amm.ne	
Cognome referente	
Codice Fiscale referente	
Indirizzo e-mail referente	
Telefono referente	
Indirizzo sede legale Amm.ne*	
CAP sede legale Amm.ne*	
Città sede legale Amm.ne*	
Provincia sede legale Amm.ne*	
Regione sede legale Amm.ne*	
Nome responsabile*	
Cognome responsabile*	
Titolo del responsabile*	
Indirizzo del sito istituzionale*	
Indirizzo e-mail dell'amministrazione*	
Dominio di Posta Elettronica Certificata*	



Informazioni per la richiesta qualificazione Porta di Dominio

Codice IPA**	
Identificativo Soggetto SPCoop ***	
Identificativo Soggetto SPCoop validato****	
Descrizione	
Nome Amministratore (coincide con quello del referente PA)	
Cognome Amministratore (coincidente con quello del referente PA)	
Casella di posta elettronica (coincidente con quello del referente PA)	
EndPoint	
EndPoint risposta	
Common Name Certificato	
Modalità richiesta (PKCS10/PKCS12)	
File name PKCS10	

- * riportare nel caso di amministrazione non presente in IPA
- ** riportare nel caso di amministrazione già presente in IPA e reperibile presso il portale IPA come da nota
- *** proposta soggetta a validazione da parte del CG-SICA
- **** identificativo validato da parte del CG-SICA

Informativa sulla tutela dei dati personali

Ai sensi del D. Lgs. 30 giugno 2003, n. 196 sulla tutela dei dati personali, il trattamento dei dati avviene con procedure idonee a tutelare la riservatezza dell'Utente e consiste nella loro raccolta, registrazione, organizzazione, conservazione, elaborazione degli stessi unicamente per le finalità connesse all'erogazione del servizio



Nome doc.:

SPCoop-Qualificazione della Porta di Dominio Enti Regionali_V1.0

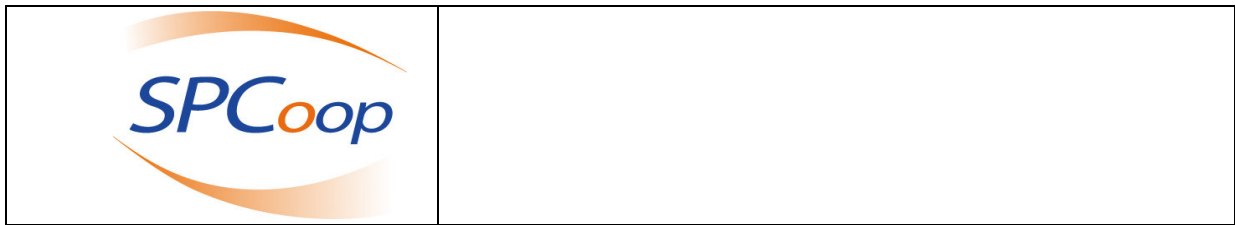
Versione: **1.0**

Data emissione:

21 Ottobre 2009

Stato: **pubblicato**

Pagina 16 di 21



Allegato 3

Modello messaggio per il referente PA

Oggetto: Accredитamento all'Indice PA

Gentile NomeReferenteAmministrazione CognomeReferenteAmministrazione,
con la presente intendiamo comunicarLe l'avvenuto accredитamento dell'amministrazione
Amministrazione_Esempio presso l'Indice delle Pubbliche Amministrazioni.

In tale sede è stato assegnato all'amministrazione il codice 'CodiceIPA' da utilizzare come
identificativo della stessa nell'ambito del servizio di Indice ed ai fini della segnatura di
protocollo (art.9, comma 1, DPCM 31/10/2000).

Sul sito <http://www.indicepa.gov.it>, potrà trovare tutte le istruzioni e la documentazione
necessaria per comunicare nei formati e nei modi previsti i dati, relativi alla Struttura
organizzativa, alle Aree Organizzative Omogenee ed alle modifiche dell'Amministrazione,
che intenderà pubblicare sull'Indice delle PA.

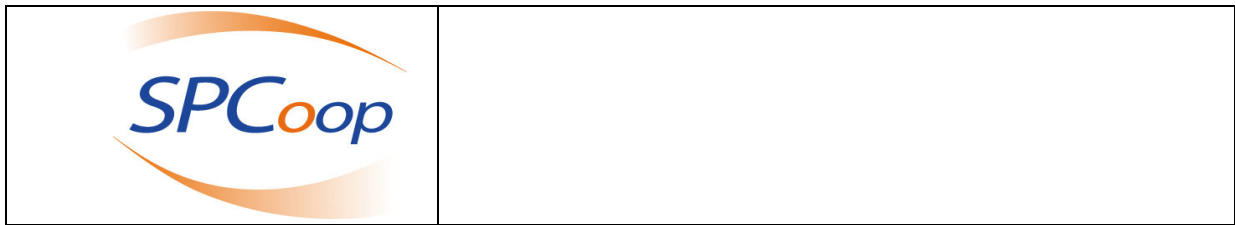
A tale proposito Le vengono fornite le seguenti credenziali di accesso all'area riservata del
sito:

Nome utente: CodiceIPA-NCognomeReferenteAmministrazione
Password: password

La invitiamo a cambiare la Sua password dopo il primo accesso utilizzando le procedure
disponibili on-line.

Per qualsiasi problema può utilizzare le procedure di contatto con il Gestore dell'iPA,
presenti nell'area riservata.

Cordiali saluti,
Gestore iPA



Allegato 4

Modello messaggio di consegna certificato Porta di Dominio

Gentile utente,

la presente per informarla che abbiamo provveduto all'emissione dell'allegato certificato digitale.

Di seguito riportiamo i principali dettagli del certificato:

DN= <DN del server>

Certificatore: C=IT O=Centro Nazionale per l'Informatica nella PA OU=Servizi di Sicurezza e Certificazione CN=CNIPA CA4

In allegato al presente messaggio è presente anche il certificato radice dell'Autorità di Certificazione emittente. Entrambi i certificati, secondo le modalità del vostro sistema, devono essere installati al fine di consentirne il corretto utilizzo.

Per motivi di sicurezza è stata modificata l'estensione degli allegati in “.dat”

E' necessario rinominare l'estensione in .cer

Distinti saluti.

L'Autorita' di Certificazione del

Centro Nazionale per l' Informatica nella Pubblica Amministrazione



Allegato 5

Modello messaggio di consegna passphrase certificato Porta di Dominio

La presente per informarla che la passphrase relativa al certificato emesso con
DN= <DN del server>

è la seguente:

Passphrase è <PassPhrase>

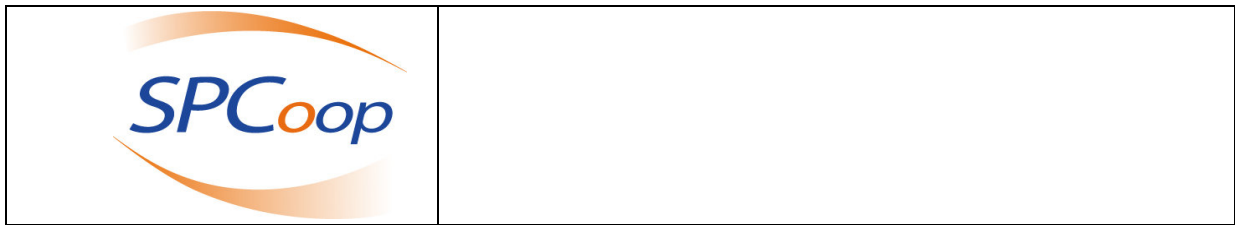
Le ricordo inoltre che il certificato inizierà a funzionare a 3 ore dalla creazione.

Alleghiamo la procedura di installazione del certificato

Distinti Saluti

Centro di Gestione SICA

Tel. 064123132 - Fax. 064193895



Allegato 7

Raccomandazioni per la raggiungibilità del CG-SICA

Per la comunicazione delle porte di dominio, vengono utilizzati dal CG-SICA gli indirizzi IP sulla rete infranet SPC sotto indicati:

In (verso SICA) - **89.97.133.185:80**

Out (da SICA) - **89.97.133.211**

Inoltre l'accesso al portale dei servizi è possibile alla URL <https://sica.spcoop.gov.it> corrispondente all'indirizzo IP, appartenente sempre alla rete SPC-Infranet, **89.97.133.189**

Per permettere l'accesso agli end-point sopraindicati è necessario effettuare opportune configurazioni sui firewall del CG-SICA, pertanto per poter procedere occorre preventivamente comunicare le informazioni seguenti:

- tutti gli indirizzi IP, sia in ingresso che in uscita, specificando la direzione, e le relative porte (se diverse dalla porta 80) con cui la Porta di dominio si presenta al firewall del SICA;
- gli URI completi degli EndPoint della Porta di dominio.

Gli URI completi del CG-SICA da cui sono accessibili i servizi necessari per la periodica verifica delle porte qualificate sono i seguenti:

<http://89.97.133.185/ErogatoreQualificazioneWEB/services/QualificazionePDDWS>

<http://89.97.133.185/FruitoreQualificazioneWEB/services/QualificazionePDDCorrelatoWS>