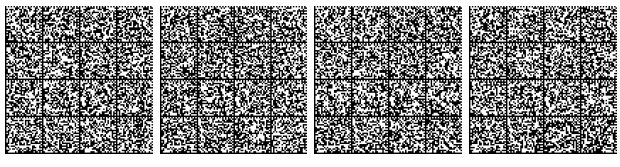
ALLEGATO A

REGOLE PROCEDURALI DI CARATTERE TECNICO OPERATIVO PER L'ACCESSO AI SERVIZI DISPONIBILI IN COOPERAZIONE APPLICATIVA TRAMITE LA TECNOLOGIA WEB SERVICE

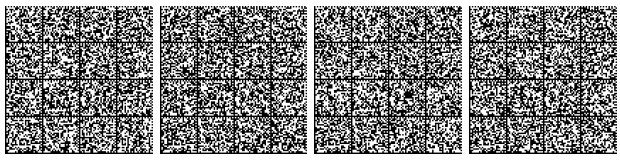
SOMMARIO



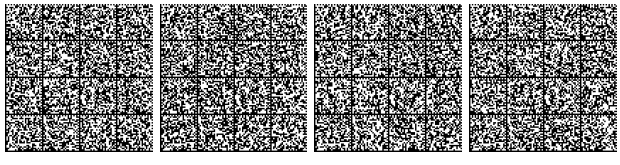
1 Definizioni ed acronimi

Nel presente capitolo è riportata la descrizione dei termini, degli acronimi e delle abbreviazioni usate nel documento.

Definizione/Acronimo	Descrizione
Accordo di servizio	Definisce le prestazioni del servizio e le modalità di erogazione/fruizione, ovvero le funzionalità del servizio, le interfacce di scambio dei messaggi tra erogatore e fruitore, i requisiti di qualità di servizio dell'erogazione/fruizione, ed i requisiti di sicurezza dell'erogazione/fruizione. Inoltre mantiene un riferimento all'ontologia/schema concettuale che definisce la semantica dell'informazione veicolata dal servizio.
Anagrafe delle sanzioni amministrative dipendenti da reato	Insieme dei dati relativi a provvedimenti giudiziari definitivi che applicano, agli enti con personalità giuridica e alle società e associazioni anche prive di personalità giuridica, le sanzioni amministrative dipendenti da reato, ai sensi del decreto legislativo 8 giugno 2001, n. 231.
CA	Certification Authority, letteralmente Autorità Certificativa, è un ente di terza parte (*trusted third party*), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conformi alla normativa europea e nazionale in materia.
Casellario giudiziale	Insieme dei dati relativi a provvedimenti giudiziari e amministrativi definitivi riferiti a soggetti determinati.
CERPA - WEB	Sito web messo a disposizione dall'Ufficio del casellario centrale, per la fruizione dei servizi del sistema CERPA.
Certificato ex articolo 39 T.U.	Certificato rilasciato alle amministrazioni pubbliche e ai gestori di pubblici servizi, contenente tutte le iscrizioni presenti nel sistema al nome di una determinata persona, nelle ipotesi di cui al comma 10 dell'articolo 1 del decreto dirigenziale CERPA
Certificato selettivo ex articolo 39 T.U.	Certificato rilasciato alle amministrazioni pubbliche e ai gestori di pubblici servizi contenente le iscrizioni presenti nelle banche dati del casellario giudiziale e dell'anagrafe delle sanzioni amministrative dipendenti da reato al nome di una determinata persona o ente, selezionate dal SIC attraverso una procedura appositamente realizzata in base a quanto stabilito in apposita convenzione. La certificazione riporta tra l'altro gli estremi della convenzione.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.



Definizione/Acronimo	Descrizione
CNIPA, già DigitPA, ora Agenzia per l'Italia Digitale	Centro nazionale per l'informatica nella pubblica amministrazione è l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196.
Codice identificativo	Codice fiscale o il codice individuato ai sensi dell'articolo 43 del T.U..
Codice CATASTALE	Codice unico identificativo assegnato ad ogni comune italiano che ha lo scopo di rendere possibile l'espressione in forma abbreviata ed univoca delle denominazioni dei Comuni d'Italia ad uso catastale.
Firma digitale	Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni).
https	Hypertext Transfer Protocol over Secure Socket Layer è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti HTTP. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti che potrebbero essere effettuati tramite la tecnica del man in the middle.
PA	Pubbliche Amministrazioni e i gestori di pubblici servizi che hanno diritto di ottenere i certificati del casellario giudiziale e dell'Anagrafe delle sanzioni amministrative dipendenti da reato, quando tale certificato è necessario per l'esercizio delle loro funzioni.
PDF	Portable Document Format è un formato documentale elettronico definito dallo standard internazionale ISO/IEC 32000.
PEC	Posta Elettronica certificata è un sistema di posta elettronica nel quale e' fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, così come disciplinata nel Decreto del Presidente della Repubblica 11 febbraio 2005 n. 68.
Porta di dominio	Elemento che sposa i principi di cooperazione applicativa, emanati dalla pubblica amministrazione, separando la logica delle funzioni interne di un Sistema Informativo dalle comunicazioni standard di soggetti eterogenei. Il principio è quello di un adattatore non invasivo, basato su tecnologie web service che implementa un servizio di messaggistica garantendo requisiti di sicurezza e identificabilità delle fonti. Essendo un' interfaccia verso il SPCoop assume pertanto un ruolo indipendente dalla piattaforma su cui opera. Fondamentalmente si occupa dell'imbustamento-sbustamento del messaggio di E-gov instradando richieste/risposte verso il servizio corretto.



Definizione/Acronimo	Descrizione
Porta di dominio qualificata	Porta di dominio cha ha superato tutti i test previsti dalla procedura di qualificazione della DigitPA per verificarne la piena compatibilità con gli standard SPCoop
RUG	Rete Unitaria della Giustizia è l'infrastruttura telematica che interconnette tra loro i sistemi informatici interni al Dominio Giustizia.
RUPA ora Sistema Pubblico di Connettività – SPC -	Rete Unitaria per la Pubblica Amministrazione è l'insieme dei Domini, ciascuno inteso come l'insieme delle risorse hardware, di comunicazione e software che cadono sotto le competenze di una determinata amministrazione. I singoli domini si interconnettono, attraverso la Porta di Rete, al Dominio della Rete Unitaria che consente alle reti delle diverse amministrazioni di interoperare e che, tramite il Centro di Gestione per l'Interoperabilità, consente di accedere ai relativi servizi.
SIC	Sistema informativo automatizzato del casellario giudiziale, del casellario dei carichi pendenti, dell'anagrafe delle sanzioni amministrative dipendenti da reato, dell'anagrafe dei carichi pendenti degli illeciti amministrativi dipendenti da reato (articolo 3).
Sistema CERPA	Sistema di Certificazione Pubbliche Amministrazioni, insieme dei servizi, attivabili tramite una delle modalità indicate nell'articolo 4 comma 2, che provvedono alla ricezione delle richieste di consultazione trasmesse con le modalità di cui agli articoli 7 e 8, alla ricerca dei soggetti sulle banche dati del SIC e alla produzione dei certificati con firma digitale. Il sistema provvede inoltre alla verifica di conformità agli standard, definiti nel presente decreto, delle richieste di consultazione e all'attivazione del sistema di autorizzazione.
SOAP	Simple Object Access Protocol è un protocollo leggero per lo scambio di informazioni in un ambiente distribuito e decentrato. Tale scambio di informazioni avviene mediante messaggi codificati in un formato XML.
SPC	Sistema Pubblico di Connettività è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.
SPCoop	Sistema Pubblico di Cooperazione, che costituisce l'infrastruttura abilitante per le comunicazioni applicative tra gli Enti Pubblici, è un insieme di specifiche gestite dalla DigitPA che normano le modalità di comunicazione ed organizzative relative alle comunicazioni applicative tra gli Enti, quella che comunemente viene chiamata Cooperazione Applicativa.

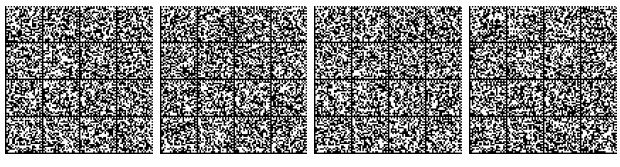
Definizione/Acronimo	Descrizione
T.U.	Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, di cui al D.P.R. 14 novembre 2002, n. 313.
Web service	Sistema software progettato per supportare l'interoperabilità tra diversi elaboratori su di una medesima rete; caratteristica fondamentale di un Web Service è quella di offrire un'interfaccia software utilizzando la quale altri sistemi possono interagire con il Web Service stesso attivando le operazioni descritte nell'interfaccia tramite appositi "messaggi" inclusi in una "busta" SOAP: tali messaggi sono, solitamente, trasportati tramite il protocollo HTTP e formattati secondo lo standard XML.
XML	eXtended Markup Language, linguaggio derivato dall'SGML (Standard Generalized Markup Language) il metalinguaggio, che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.
UDDI	Universal Description Discovery and Integration è una base dati ordinata ed indicizzata, basato su XML ed indipendente dalla piattaforma hardware, che permette la pubblicazione dei propri dati e dei servizi offerti su internet.
WSDL	Il Web Services Description Language è un linguaggio formale in formato XML utilizzato per la creazione di "documenti" per la descrizione di Web Service.

2 Obiettivi del documento

Obiettivo del documento è descrivere l'architettura generale e le regole procedurali di carattere tecnico operativo per l'accesso ai servizi disponibili in cooperazione applicativa tramite la tecnologia web service in merito agli articoli 7 e 9 del decreto dirigenziale del del 05/12/2012 ai sensi dell'articolo 39 D.P.R. 14 novembre 2002, N. 313.

Il documento è così strutturato:

1. Descrizione del contesto di applicazione del documento;
2. Descrizione generale dell'infrastruttura di riferimento su cui è basata la realizzazione dei servizi di certificazione offerti (Cfr. capitolo 4);
3. Descrizione dei web service che implementano i servizi di certificazione (Cfr. capitolo 5).



3 Contesto

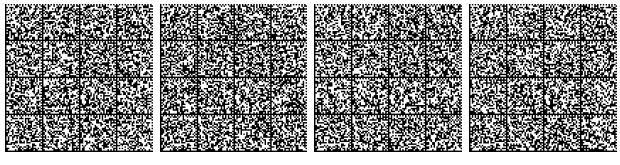
Il sistema *Certificazione Pubbliche Amministrazioni* (CERPA) nasce dalla necessità di attuare l'articolo 39 del Testo Unico (T.U.) al fine di consentire la consultazione diretta del sistema da parte delle amministrazioni pubbliche e dei gestori di pubblici servizi per l'acquisizione dei certificati di cui agli articoli 28 e 32 in materia di Casellario Giudiziale e dell'anagrafe delle sanzioni amministrative dipendenti da reato.

La cooperazione tra CERPA e le PA, si basa su due soluzioni software:

1. Un Software di Cooperazione Applicativa che permette lo scambio di dati tra SIC e i singoli sistemi di ogni PA, utilizzando una porta di dominio per la trasmissione e ricezione dei dati adottando la tecnologia Web Service (*XML*, *SOAP*, *WSDL*) su protocollo HTTP.
2. Una soluzione che prevede la richiesta da parte della PA ed una risposta da parte del Casellario tramite utilizzo di *Posta Elettronica Certificata* (PEC).

In questo documento si descrivono l'architettura generale e le regole procedurali di carattere tecnico operativo per la fruizione dei servizi offerti dal sistema CERPA attraverso la prima modalità, ovvero attraverso i web service esposti attraverso la specifica porta di dominio.

Per quanto riguarda la modalità di richiesta tramite l'utilizzo della PEC si rimanda all'Allegato B del DECRETO DIRIGENZIALE ARTICOLO 39 D.P.R. 14 NOVEMBRE 2002, N. 313.



4 L'infrastruttura

4.1 La cooperazione applicativa

Lo scambio dati tra il SIC e il sistema di ogni singola PA avviene tramite l'adozione, nelle sue caratteristiche più generali, del paradigma della **cooperazione applicativa**, definito nei documenti di progettazione della Rete Unitaria della Pubblica Amministrazione (RUPA), ora denominato *Sistema Pubblico di Connettività* (SPC)..

La cooperazione applicativa è realizzata attraverso un canale di interscambio e cooperazione software basato su web service, che permette lo scambio di messaggi tra i domini.

Gli standard tecnici di riferimento che il sistema di cooperazione applicativa deve adottare sono conformi alle specifiche e alle raccomandazioni emanate dai principali organismi internazionali operanti nel settore, quali il *World Wide Web Consortium* (W3C) per la famiglia di protocolli *XML*, per *SOAP*, per *WSDL*, per le architetture web, e per le architetture e le tecnologie web service, le specifiche *Universal Description Discovery and Integration* (UDDI), e l'architettura web service.

4.1.1 Porte di Dominio

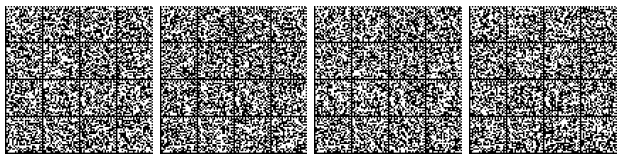
Il concetto di cooperazione applicativa nel sistema della Pubblica Amministrazione attiene alla capacità di interconnessione sicura tra tutte le Pubbliche Amministrazioni, rispettando quelle che sono le linee guida del *Sistema Pubblico di Connettività* (SPC).

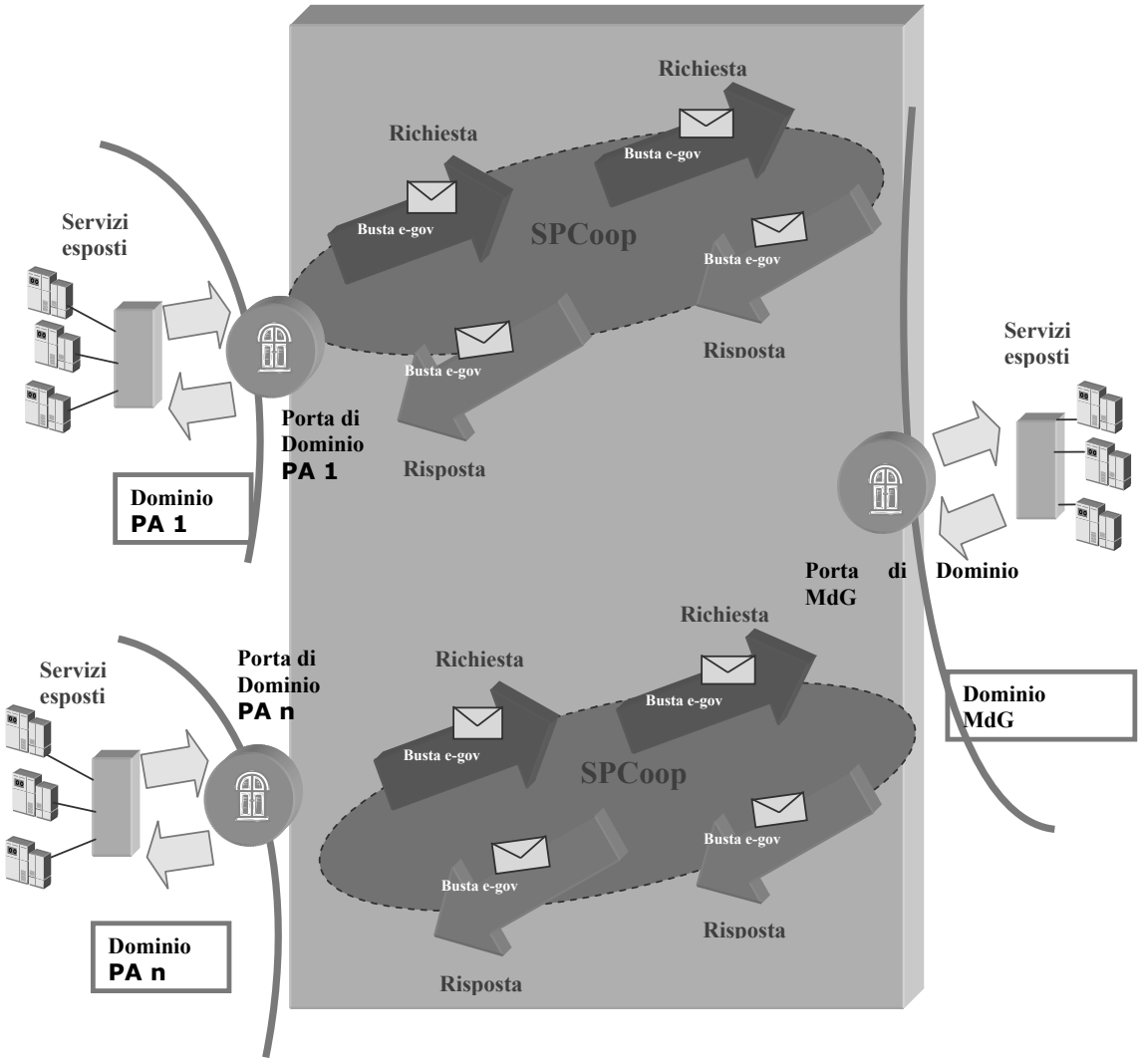
La cooperazione applicativa, nell'ambito della rete nazionale della Pubblica Amministrazione, secondo le linee guida redatte dal CNIPA, è realizzata tramite le *porte di dominio*. Gli standard del CNIPA prevedono l'utilizzo della Busta di e-Government, dove è specificato il formato dei messaggi scambiati tra le Porte di Dominio nelle interazioni di cooperazione applicativa e ne costituisce di fatto l'elemento informativo di base, come descritto nel doc. "Sistema Pubblico di Cooperazione: BUSTA DI E-GOV Pubblicato V. 1.1 del 14/10/2005" pagina 9.

Le **Porte di Dominio** sono l'elemento tecnologico chiave dell'architettura di Cooperazione applicativa nell'ambito della Rete Nazionale. Esse corrispondono all'insieme delle funzionalità software attivabili in ciascun dominio come **proxy unico** ed esclusivo per l'accesso alle risorse applicative di altri domini attraverso la rete, e viceversa, senza introdurre variazioni significative agli ambienti esistenti.

L'architettura del modello di cooperazione applicativa si basa sui seguenti elementi fondamentali:

- la cooperazione applicativa avviene attraverso lo scambio di "messaggi applicativi" e sulla base di *accordi di servizio* che esplicitano l'accordo stipulato sull'erogazione/fruizione delle prestazioni del servizio in questione;
- ogni amministrazione gestisce i flussi di cooperazione applicativa con le altre amministrazioni per il tramite di un unico punto (logico) del proprio sistema informativo denominato *Porta di Dominio* dei Servizi Applicativi;
- le amministrazioni che cooperano fra loro possono dar luogo a *Domini di Cooperazione* in cui siano stabiliti i servizi erogati, i relativi livelli di servizio e le responsabilità nel mantenimento di tali livelli;
- è definita una infrastruttura unitaria di *servizi di interoperabilità e di cooperazione e accesso (SICA)* che garantisce l'erogazione di servizi tecnologici di base, comuni a tutti i Domini di Cooperazione.





La seguente tabella riporta le informazioni identificative della porta di dominio del Ministero della Giustizia dedicata ai servizi di certificazione offerti alle PA:

	URL
Indirizzo della porta di dominio per il servizio di Certificazione Casellario	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneCasellario
Indirizzo della porta di dominio per il servizio di Certificazione Sanzioni	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneSanzioni

5 I Web Service

Nel panorama dello sviluppo in ambiente Internet il web service rappresenta la tecnologia di riferimento per lo sviluppo e l'integrazione di applicazioni. Questa tecnologia, oltre a consentire interoperabilità, permette di realizzare dei servizi ad hoc personalizzabili secondo le esigenze degli utenti. Un web service rappresenta infatti un insieme di operazioni accessibili attraverso una rete sulla quale si realizza lo scambio di appositi messaggi codificati secondo un determinato formato (XML). I messaggi viaggiano inclusi in una 'busta' con formalismo SOAP (Simple Object Access Protocol) e sono trasportati tramite il protocollo https. Un servizio web è determinato tramite la descrizione del servizio che circostanzia in modo formale tutte le informazioni necessarie per la sua invocazione. Caratteristica principale di questo tipo di servizio è l'indipendenza dell'applicazione dalla piattaforma di implementazione e la possibilità di utilizzarlo per comunicazioni e scambi di informazioni in modo automatico e sicuro realizzando una interazione tra applicazioni.

5.1 Panoramica generale

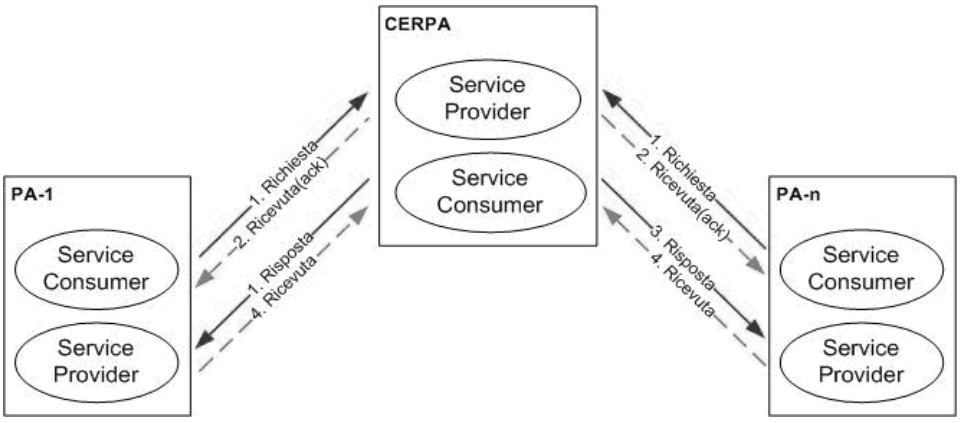
Le modalità di colloquio adottate tra i sistemi CERPA e quelli esposti dalle singole PA possono essere di due tipi:

1. "Sincrona" comunicazione tra porte di Dominio: la Porta di Dominio mittente invia un messaggio (richiesta) alla Porta di Dominio destinataria, quindi il messaggio è ricevuto ed elaborato con la formazione del messaggio di risposta.

2. "Asincrona Simmetrica" comunicazione tra moduli web service.

5.1.1 Comunicazione "Asincrona Simmetrica" tra i moduli web service.

La comunicazione tra i moduli "web service", del sistema CERPA e quelli di ciascuna PA, avviene attraverso lo scambio di due messaggi, così come mostra la figura di seguito.



Ogni servizio esposto dal sistema CERPA, ricevuta una richiesta, restituisce immediatamente una notifica di accettazione, identificata dalla stringa "ACK", abbreviazione del termine inglese "Acknowledged" (Accettato), seguita dall'identificativo che il sistema assegna automaticamente alla richiesta pervenuta, separati dal carattere | (pipe), es.

"ACK|1464". Tale identificativo è un'informazione aggiuntiva, utilizzabile dalla PA per effettuare eventuali comunicazioni.
La richiesta, corredata da un identificatore univoco della PA mittente, è accodata per essere gestita in maniera asincrona. Dopo i controlli di cui al paragrafo 3.4, la richiesta è effettivamente elaborata dal sistema CERPA, che provvede ad estrarre la lista dei nominativi e ad effettuare, per ciascuno di essi, un ulteriore controllo formale sui dati. Se i controlli formali non soddisfano i requisiti il nominativo non è oggetto di ricerca in banca dati e viene quindi restituito dal sistema con un codice esito indicante l'anomalia. Se invece i controlli formali sono superati il sistema effettua una ricerca sulle banche dati del SIC, al termine della quale restituisce un codice esito indicante il risultato della ricerca e produce comunque un certificato. Completata l'elaborazione di tutti i nominativi contenuti nella richiesta, il sistema produce la risposta spedita alla PA mittente tramite l'invocazione dell'apposito servizio

5.2 Servizi esposti

In questo capitolo sono trattati in modo dettagliato i flussi che caratterizzano i diversi servizi previsti per il sistema di cooperazione CERPA.
Il sistema CERPA espone i servizi web di seguito indicati e a sua volta invoca il servizio esposto da ogni singola PA per inviare le risposte.
Per l'invocazione di tali servizi, in entrambe le direzioni, è stata concordata un'unica struttura dati per ciascuna area di riferimento del servizio esposto:certificazione relativa al casellario giudiziale - certificazione relativa all'anagrafe delle sanzioni amministrative.
La descrizione dettagliata della struttura dati è rimandata al capitolo 6.

I servizi sono così suddivisi:

1. Certificazione Casellario con Service Name *CertificazioneCasellarioService* e Port Name *CertificazioneCasellario* che espone i seguenti metodi:
    - RichiestaCertificazioneArt21
    - RichiestaCertificazioneArt28Civ
    - RichiestaCertificazioneArt28Gen
    - RichiestaCertificazioneArt28Pen
    - RichiestaCertificazioneArt29
    - RichiestaCertificazioneArt39
2. Certificazione Sanzioni con Service Name *CertificazioneSanzioniService* e Port Name *CertificazioneSanzioni* che espone i seguenti metodi:
    - RichiestaCertificazioneArt32
    - RichiestaCertificazioneArt39

Nella seguente tabella sono riportati gli indirizzi presso i quali sono reperibili i file WSDL e XSD che sono alla base dell'implementazione dei servizi web esposti dal sistema CERPA.

	URL
WSDL CertificazioneCasellario	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneCasellario?wsdl
WSDL CertificazioneSanzioni	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneSanzioni?wsdl
Schema XSD CertificazioneCasellario	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneCasellario?xsd=1
Schema XSD CertificazioneSanzioni	https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneSanzioni?xsd=1

I predetti file sono inoltre reperibili sul sito CERPA-WEB.

5.2.1 Servizio di Richiesta Certificati - Casellario Giudiziale

Questo servizio permette, alle PA autorizzate, di inviare, relativamente alla banca dati del casellario giudiziale, la richiesta di certificazione di interesse per uno o più nominativi contemporaneamente.
Le informazioni necessarie per l'utilizzo di tale servizio sono:

- Dati Richiesta
- Lista Nominativi

I dati della richiesta servono all'identificazione univoca della stessa nell'ambito della medesima PA e sono dettagliati all'articolo 9 del decreto dirigenziale CERPA.
La lista dei nominativi deve contenere il riferimento ad almeno un soggetto.
In particolare il servizio espone i metodi per la richiesta dei certificati di cui agli articoli 28 (generale, penale e civile) 29 (elettorale) 21 (in relazione all'articolo 38 d.lgs. 163/2006) e 39 T.U.

5.2.2 Servizio di Richiesta Certificati - Sanzioni Amministrative

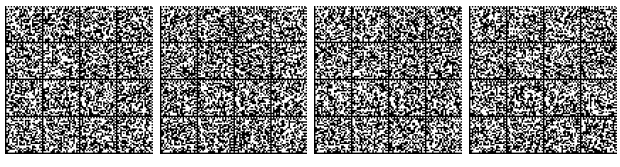
Questo servizio permette, alle PA autorizzate, di inviare, relativamente alla banca dati anagrafe sanzioni amministrative dipendenti da reato , la richieste di certificazione di interesse per uno o più nominativi contemporaneamente.
Le informazioni necessarie per l'utilizzo di tale servizio sono:

- Dati Richiesta
- Lista Nominativi

I dati della richiesta servono all'identificazione univoca della stessa nell'ambito della medesima PA e sono dettagliati all'articolo 9 del decreto dirigenziale CERPA.
La lista dei nominativi deve contenere il riferimento ad almeno un soggetto.
In particolare il servizio espone i metodi per la richiesta dei certificati di cui agli articoli 32 e 39 T.U.

5.3 Modalità chiamata del servizio

Per effettuare la chiamata ai servizi esposti è necessario implementare un web service client a partire dai rispettivi descrittori wsdl, indicati nella tabella presente al capitolo 5.2, ovvero presenti e scaricabili dal sito CERPA-WEB. Gli ambienti di sviluppo più comuni, come Eclipse e Netbeans, forniscono strumenti validi per la generazione di web service client a partire dal descrittore wsdl; in pochi passaggi sono generate le interfacce e gli oggetti per la corretta invocazione dei web service desiderati. Una volta generati tutti gli artefatti opportuni, è necessario creare una struttura dati consistente ed inviarla al Casellario. Un esempio di metodo per effettuare la chiamata al servizio è descritto nel blocco di codice sottostante:

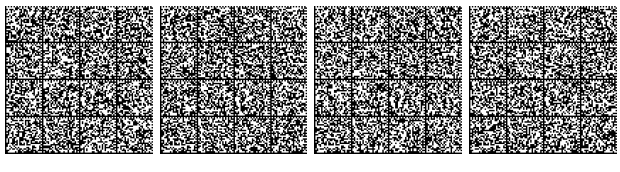


```
private String callService(RichiestaServizio richiestaServizio, String tipoCertificato)
throws MalformedURLException, JAXBException, IOException, RichiestaCertificazioneException{

        // costruisco un'istanza del client del servizio
        CertificazioneCasellarioService client = new CertificazioneCasellarioService(
        "https://MinisteroGiustizia.spcoop.gov.it/openspcoop/PA/MG/CertificazioneCasellario?wsdl"
,               new QName("http://cg.ws.cerpa.mig.it/", "CertificazioneCasellarioService"));

        // ottengo dal client il port type
        CertificazioneCasellario port = client.getCertificazioneCasellario();

        // in base al tipo Certificato costruisco l'oggetto opportuno ed invoco il
        // relativo servizio sul port type
        if (tipoCertificato.equals("GPA")){
                RichiestaCertificazioneArt28Gen rc = new RichiestaCertificazioneArt28Gen();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt28Gen(rc);
        }
        if (tipoCertificato.equals("PPA")){
                RichiestaCertificazioneArt28Pen rc = new RichiestaCertificazioneArt28Pen();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt28Pen(rc);
        }
        if (tipoCertificato.equals("CPA")){
                RichiestaCertificazioneArt28Civ rc = new RichiestaCertificazioneArt28Civ();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt28Civ(rc);
        }
        if (tipoCertificato.equals("LPA")){
                RichiestaCertificazioneArt29 rc = new RichiestaCertificazioneArt29();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt29(rc);
        }
        if (tipoCertificato.equals("APA")){
                RichiestaCertificazioneArt39 rc = new RichiestaCertificazioneArt39();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt39(rc);
        }
        if (tipoCertificato.equals("BPA")){
                RichiestaCertificazioneArt21 rc = new RichiestaCertificazioneArt21();
                rc.setRichiestaServizio(richiestaServizio);
                return port.richiestaCertificazioneArt21(rc);
        }
        throw new IllegalArgumentException("Tipo certificato non valido");
}
```

5.4 Controlli

5.4.1 Controllo autenticità dell'utente/mittente e integrità delle richieste

Al fine di garantire l'autenticità dell'utente/mittente e l'integrità delle richieste pervenute, i messaggi di richiesta del servizio, intesi come SOAP Body della busta di e-gov, sono firmati dalla PA richiedente attraverso un dispositivo di riconoscimento di firma elettronica ai sensi dell'articolo 24 del Codice Amministrazione Digitale. Il dispositivo di riconoscimento è fornito dal Ministero della Giustizia, che adotta lo standard di sicurezza PKI per la firma dei documenti elettronici basato sulla generazione di una coppia di chiavi (pubblica e privata) che garantiscono l'autenticità e l'integrità del file inviato.
Le indicazioni per la generazione delle chiavi di firma, riconosciute nel sistema informatico del Casellario, sono fornite al paragrafo 8.

5.4.2 Controlli di obbligatorietà

La richiesta XML, deve rispettare l'obbligatorietà dei campi ove previsto, in base a quanto stabilito nel file schema XSD. Ad esempio verificare che un campo previsto numerico contenga proprio un numero, oppure il campo sesso contenga M o F e nessun altro valore.

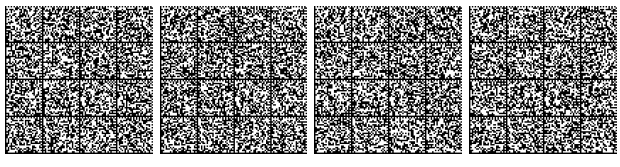
5.4.3 Controlli testata richiesta

I dati relativi alla testata della richiesta, contenuti nell'oggetto DatiRichiesta, la versione del file schema XSD e l'indirizzo IP del mittente sono oggetto di controlli, superati i quali viene registrata la richiesta in banca dati. Nel caso in cui i controlli di testata non siano superati l'intera richiesta non sarà processata. I controlli previsti riguardano:

- la corrispondenza tra il tipo certificato richiesto e il web service invocato
- la versione del file schema XSD, che deve corrispondere alle versioni implementate
- l'abilitazione alla produzione del certificato richiesto da parte dell'ente richiedente
- l'univocità dell'identificativo della richiesta all'interno dell'ente richiedente

5.4.4 Controlli nominativi

I dati relativi ai nominativi sono oggetto di controlli formali; se un nominativo non supera tali controlli, il sistema restituisce il corrispondente codice errore senza produrre il certificato. L'elaborazione, invece, avviene per tutti i nominativi per i quali non si sono verificati errori nei controlli. Un esempio di errore può essere un codice nazione non valido, non presente in banca dati, oppure l'assenza del codice catastale del comune se la nazione selezionata è ITALIA. Un altro caso molto importante da considerare è la validità della finalità per il tipo certificato richiesto e l'abilitazione dell'ente a richiedere la produzione del certificato per tale finalità. I nominativi inseriti potranno presentare caratteri diacritici. Il codice fiscale è obbligatorio per soggetti italiani.



5.4.5 Soggetti minorenni

Le richieste di certificazione effettuate per soggetti minorenni, sono accettate soltanto nel caso in cui le richieste stesse siano per fini elettorali. Per tutte le altre tipologie non è possibile richiedere la certificazione.

5.4.6 Controllo finalità certificato

La finalità per la quale è richiesto il certificato deve corrispondere a quella indicata nella relativa convenzione. Quindi in relazione ad una richiesta di certificato per un nominativo riferito ad una finalità, per la quale la PA non è abilitata, è restituito con un codice errore opportuno, e non porta alla generazione di alcun certificato

5.4.7 Controllo firma certificato

Sul certificato PDF, prima di essere inserito all'interno della risposta XML e spedito alla PA richiedente, è apposta la firma digitale del Direttore dell'Ufficio del casellario centrale, al fine di garantirne l'autenticità e l'integrità.

5.5 Modalità di risposta

Il risultato dell'elaborazione di una richiesta è restituito dal sistema CERPA tramite invocazione del web service di risposta che ogni PA deve esporre attraverso la propria porta di dominio.

Nello specifico, la PA che effettua richieste di certificazione per il Casellario Giudiziale, dovrà esporre il servizio di risposta certificazione corrispondente. Tale servizio è definito nel WSDL CertificazioneCasellario, con nome *RispostaCertificazioneCasellarioService* e porta *RispostaCertificazioneCasellario*.
La precedente porta definisce le seguenti operazioni:

- RispostaCertificazione
- NotificaElaborazioneFallita

Di seguito il diagramma del servizio e della porta appena descritti:

La PA che effettua richieste di certificazione per le Sanzioni Amministrative, dovrà esporre il servizio di risposta certificazione corrispondente. Tale servizio è definito nel WSDL CertificazioneSanzioni, con nome *RispostaCertificazioneSanzioniService* e porta *RispostaCertificazioneSanzioni*.
La precedente porta definisce le seguenti operazioni:

- RispostaCertificazione
- NotificaElaborazioneFallita

Di seguito il diagramma del servizio e della porta appena descritti:

Nei paragrafi successivi vengono descritte le operazioni previste dai servizi di risposta.

5.5.1 RispostaCertificazione

Nel caso in cui la richiesta sia elaborata correttamente, la soap operation che il sistema CERPA invocherà per l'invio della risposta è RispostaCertificazione. In base a ciò il web service di risposta, erogato dalla PA, dovrà esporre un metodo corrispondente a tale soap operation. Sarà quindi restituita alla PA la struttura dati contenente la risposta. La ricezione della risposta da parte della PA deve essere confermata tramite la restituzione della stringa "ACK". Eventuali errori occorsi a seguito della ricezione devono essere comunicati tramite il sollevamento di un SOAPFault. In tal caso sarà tentato un invio fino al buon esito dell'operazione. Ad esempio, se la PA salva le risposte su file system e lo spazio su disco esaurisce, il salvataggio della risposta causerà un errore che deve essere notificato al sistema CERPA, il quale tenterà nuovamente l'invio ad intervalli regolari fino al buon esito dell'operazione.

5.5.2 NotificaElaborazioneFallita

Nel caso di errori durante l'elaborazione della richiesta, il sistema CERPA deve essere in grado di notificare alla PA, l'errore verificatosi. La soap operation che il sistema CERPA invocherà per la notifica della fallita elaborazione è NotificaElaborazioneFallita. In base a ciò il web service di risposta, erogato dalla PA, dovrà esporre un metodo corrispondente a tale soap operation. Sarà restituito alla PA l'identificativo della richiesta la cui elaborazione è fallita. La ricezione della notifica da parte della PA deve essere confermata tramite la restituzione della stringa "ACK". Eventuali errori occorsi a seguito della notifica devono essere comunicati tramite il sollevamento di un SOAPFault.

5.6 Diagrammi di sequenza

Di seguito sono presentati i diagrammi di sequenza per i casi più significativi, del colloquio con le PA, tramite l'utilizzo della porta di dominio.

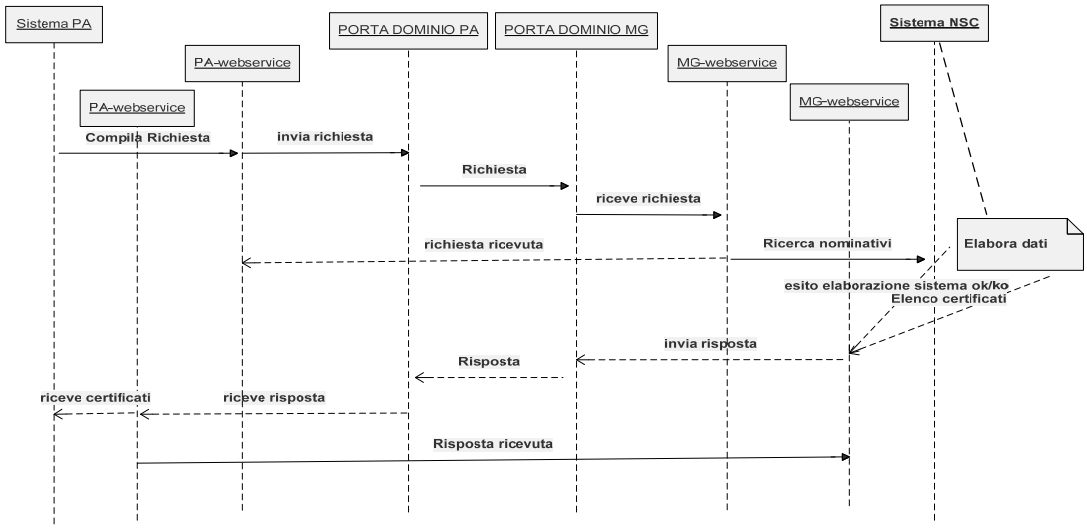


Diagramma di sequenza della richiesta effettuata dalla PA con produzione certificati (esito ok), senza certificati (esito ko – errore in elaborazione)

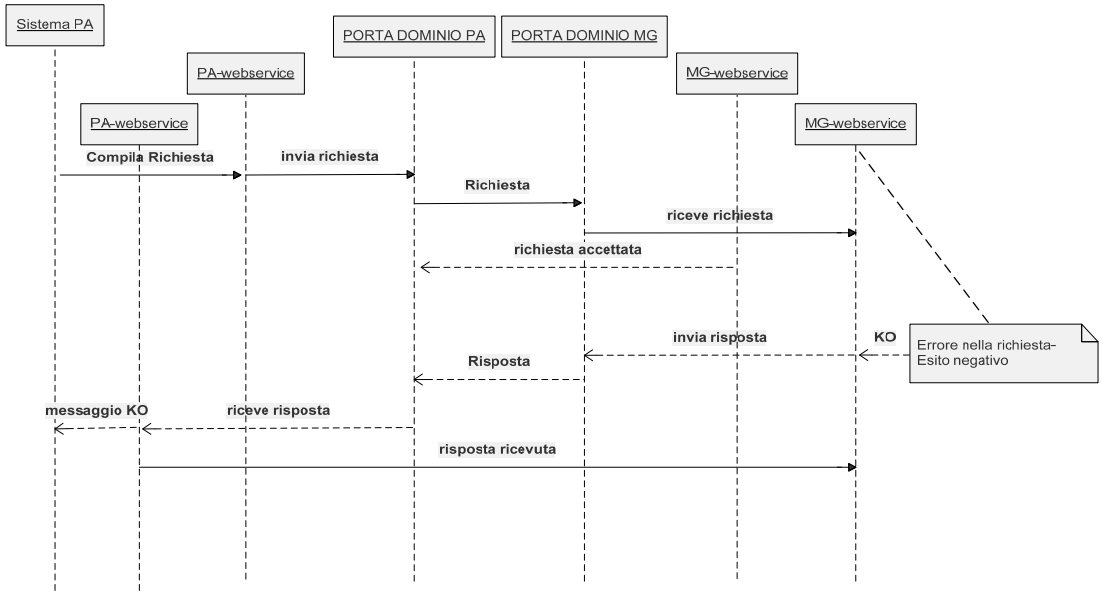


Diagramma di sequenza della richiesta effettuata dalla PA con esito negativo (errore nella richiesta, non dà luogo ad elaborazioni).

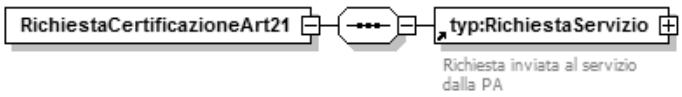
6 Struttura dati web-service

Di seguito è analizzato lo schema xml utilizzato nei web service descritti nel capitolo precedente, illustrando ogni singolo elemento. La struttura dati è la stessa sia per i servizi di certificazione relativi al Casellario Giudiziale, sia per quelli relativi all'Anagrafe delle Sanzioni Amministrative, ad eccezione del solo elemento DatiNominativo.

6.1 Documento xsd: schema e definizione elementi

6.1.1 RichiestaCertificazioneArt21

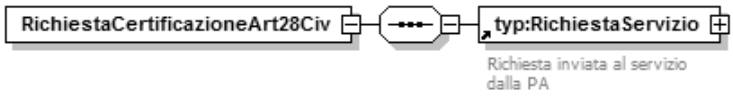
E' l'elemento contenitore di una richiesta di certificazione per ex art. 21 T.U. in relazione all'art. 38 D.lgs. 163/2006. Incapsula una richiesta servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt21	Contenitore della richiesta per Art. 21 inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.2 RichiestaCertificazioneArt28Civ

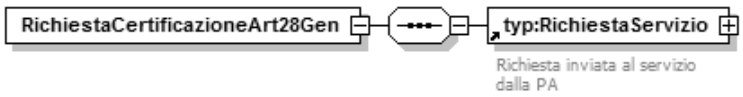
E' l'elemento contenitore di una richiesta di certificazione per Art. 28 Civile. Incapsula una richiesta servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt28Civ	Contenitore della richiesta per Art. 28 Civile inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.3 RichiestaCertificazioneArt28Gen

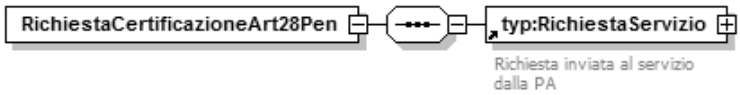
E' l'elemento contenitore di una richiesta di certificazione per Art. 28 Generale. Incapsula una richiesta servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt28Gen	Contenitore della richiesta per Art. 28 Generale inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.4 RichiestaCertificazioneArt28Pen

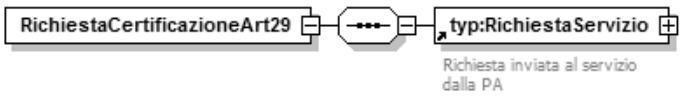
E' l'elemento contenitore di una richiesta di certificazione per Art. 28 Penale. Incapsula una richiesta servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt28Pen	Contenitore della richiesta per Art. 28 Penale inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.5 RichiestaCertificazioneArt29

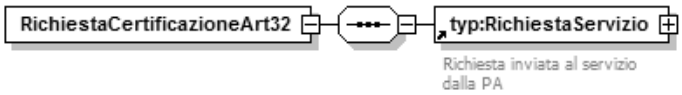
E' l'elemento contenitore di una richiesta di certificazione per Art. 29. Incapsula una richiesta servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt29	Contenitore della richiesta per Art. 29 inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.6 RichiestaCertificazioneArt32 (Anagrafe delle Sanzioni Amministrative)

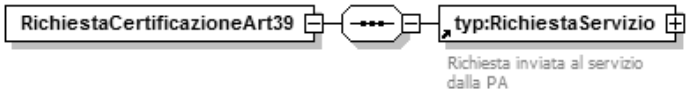
E' l'elemento contenitore di una richiesta di certificazione per Art. 32. Incapsula una richiesta servizio. E' presente solo per le richieste relative all'area Sanzioni Amministrative.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt32	Contenitore della richiesta per Art. 32 inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.7 RichiestaCertificazioneArt39

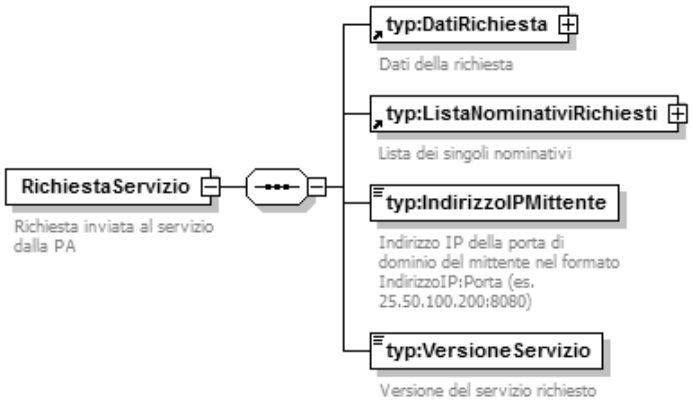
E' l'elemento contenitore di una richiesta di certificazione per Art. 39. Incapsula una richiesta servizio. Questo oggetto esiste anche per l'area Sanzioni Amministrative.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaCertificazioneArt39	Contenitore della richiesta per Art. 39 inviata dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--

6.1.8 RichiestaServizio

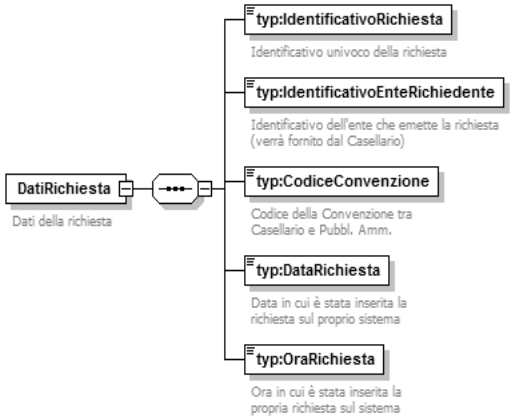
E' l'elemento contenitore di tutti i dati necessari alla richiesta del servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RichiestaServizio	Richiesta inviata al servizio dalla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
VersioneServizio	Versione del servizio esposto	String	--
DatiRichiesta	Dati della richiesta	Tipo complesso	--
ListaNominativiRichiesti	Lista dei singoli nominativi	Tipo complesso	--
IndirizzoIPMittente	Indirizzo IP della porta di dominio del mittente	String	15

6.1.9 DatiRichiesta

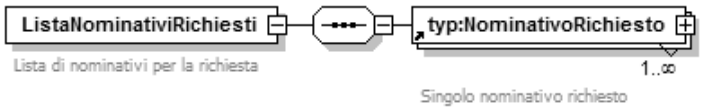
È l'elemento contenitore dei dati identificanti comuni a tutta la richiesta.



Nome Elemento	Descrizione	Tipo	Lunghezza
DatiRichiesta	Dati della richiesta	Tipo complesso	--
Composto dalle seguenti proprietà:			
IdentificativoRichiesta	Identificativo univoco della richiesta	string	15
IdentificativoEnteRichiedente	Identificativo dell'ente che emette la richiesta (verrà fornito dal Casellario)	string	3
CodiceConvenzione	Codice della Convenzione tra Casellario e Pubblica Amministrazione	string	9
DataRichiesta	Data in cui è stata inserita la richiesta sul proprio sistema	date	--
OraRichiesta	Ora in cui è stata inserita la propria richiesta sul sistema	time	--

6.1.10 ListaNominativiRichiesti

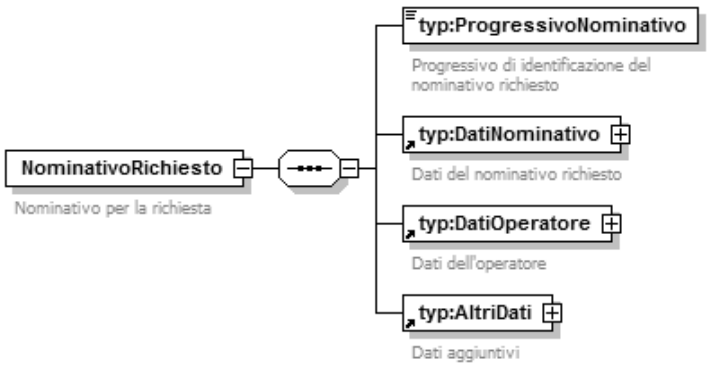
È una lista di oggetti di tipo NominativoRichiesto; deve essere costituita da almeno un nominativo.



Nome Elemento	Descrizione	Tipo	Lunghezza
ListaNominativiRichiesti	Lista di nominativi per la richiesta	Tipo complesso	--
Composto dalle seguenti proprietà:			
NominativoRichiesto	Singolo nominativo richiesto	Tipo complesso	--

6.1.11 NominativoRichiesto

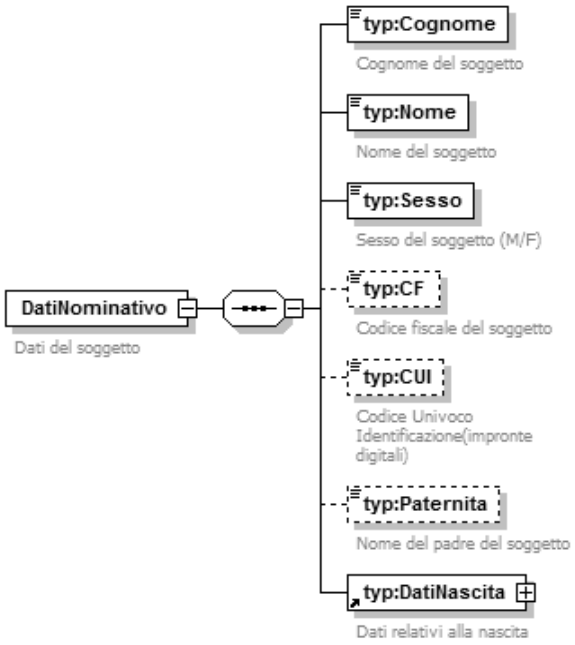
Questo elemento contiene le informazioni relative al singolo nominativo, all'operatore che effettua la richiesta, e ad altri dati relativi al certificato.



Nome Elemento	Descrizione	Tipo	Lunghezza
NominativoRichiesto	Nominativo per la richiesta	Tipo complesso	--
Composto dalle seguenti proprietà:			
ProgressivoNominativo	Progressivo di identificazione del nominativo richiesto	string	15
DatiNominativo	Dati del nominativo richiesto	Tipo complesso	--
DatiOperatore	Dati dell'operatore	Tipo complesso	--
AltriDati	Dati aggiuntivi	Tipo complesso	--

6.1.12 DatiNominativo (Casellario Giudiziale)

Contiene i dati anagrafici di un soggetto.

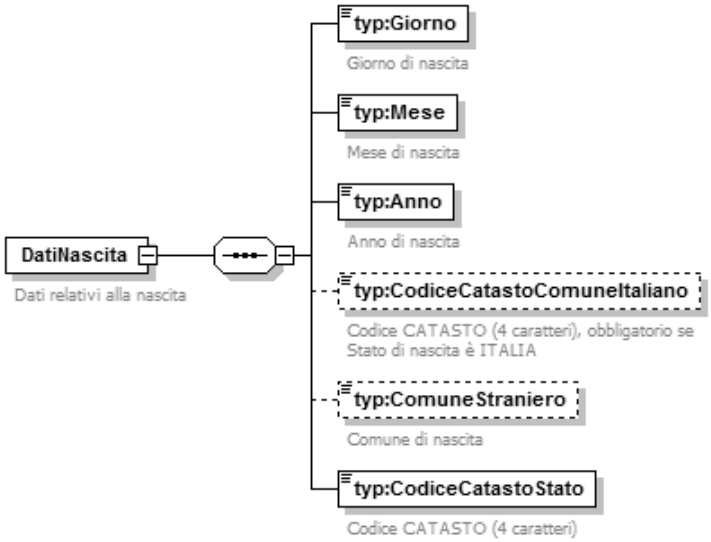


Nome Elemento	Descrizione	Tipo	Lunghezza
DatiNominativo	Dati del soggetto	Tipo complesso	--
Composto dalle seguenti proprietà:			
Cognome	Cognome del soggetto	string72	72
Nome	Nome del soggetto	string72	72
Sesso	Sesso del soggetto (M/F)	string	1
CF	Codice fiscale del soggetto (obbligatorio per gli italiani)	string	16
CUI	Codice Univoco Identificazione (impronte digitali)	string	7
Paternita	Nome del padre del soggetto	string72	72
DatiNascita	Dati relativi alla nascita	Tipo complesso	--

Le proprietà Cognome, Nome e Paternità, oltre le 26 lettere dell'alfabeto latino, possono contenere soltanto lo spazio, l'apostrofo ed i caratteri diacritici definiti nell'omonima tabella presente sul sito CERPA-WEB. Nessun altro carattere è consentito.

6.1.13 DatiNascita (Casellario Giudiziale)

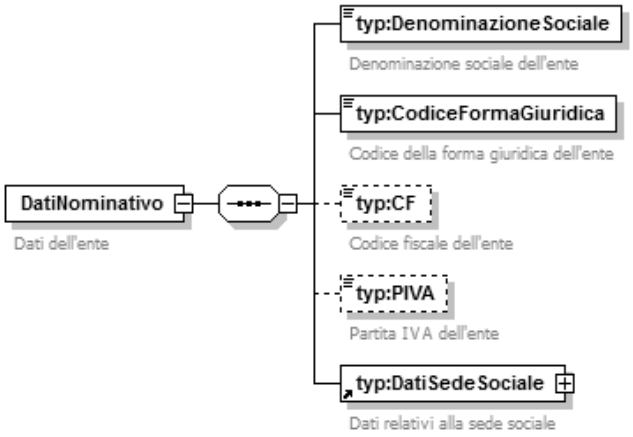
È l'elemento contenitore dei dati di nascita di un soggetto.



Nome Elemento	Descrizione	Tipo	Lunghezza
DatiNascita	Dati relativi alla nascita	Tipo complesso	--
Composto dalle seguenti proprietà:			
Giorno	Giorno di nascita	string	2
Mese	Mese di nascita	string	2
Anno	Anno di nascita	string	4
CodiceCatastoComuneItaliano	Codice CATASTO (4 caratteri), obbligatorio se Stato di nascita è ITALIA	string	4
ComuneStraniero	Comune di nascita	string	60
CodiceCatastoStato	Codice CATASTO (4 caratteri)	string	4

6.1.14 DatiNominativo (Anagrafe delle Sanzioni Amministrative)

Contiene i dati anagrafici di un ente.

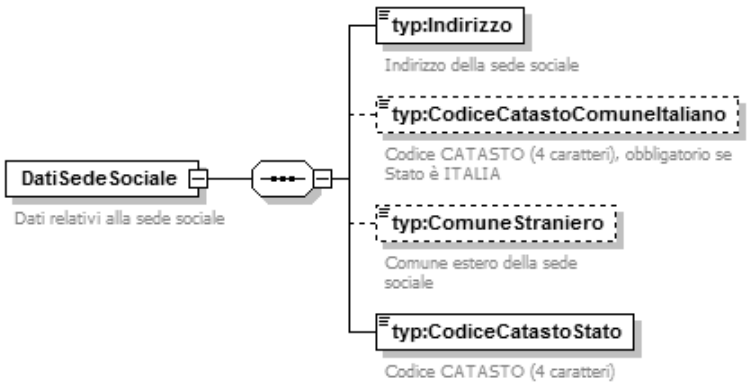


Nome Elemento	Descrizione	Tipo	Lunghezza
DatiNominativo	Dati dell'ente	Tipo complesso	--
Composto dalle seguenti proprietà:			
DenominazioneSociale	Denominazione sociale dell'ente	string	150
CodiceFormaGiuridica	Codice della forma giuridica dell'ente	string	3
CF	Codice fiscale dell'ente	string	16
PIVA	Partita IVA dell'ente	string	11
DatiSedeSociale	Dati relativi alla sede sociale	Tipo complesso	--

L'elemento CodiceFormaGiuridica trasporta la forma giuridica del soggetto. La tabella contenente i valori di tale campo sarà fornita dall'Amministrazione del Casellario in formato xls o csv.

6.1.15 DatiSedeSociale (Anagrafe delle Sanzioni Amministrative)

È l'elemento contenitore dei dati relativi alla sede sociale di un ente.

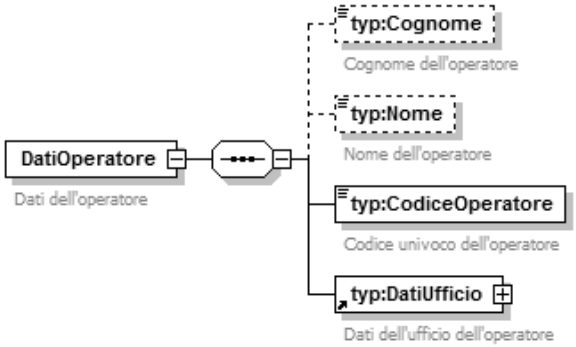


Nome Elemento	Descrizione	Tipo	Lunghezza
DatiSedeSociale	Dati relativi alla sede sociale	Tipo complesso	--
Composto dalle seguenti proprietà:			
Indirizzo	Indirizzo della sede sociale	string	100
CodiceCatastoComuneItaliano	Codice CATASTO (4 caratteri), obbligatorio se Stato è ITALIA	string	4
ComuneStraniero	Comune estero della sede sociale	string	60
CodiceCatastoStato	Codice CATASTO (4 caratteri)	string	4

L'elemento Indirizzo corrisponde all'indirizzo della sede legale della persona giuridica. È un campo di testo libero che non concorre alla ricerca del soggetto, ma che sarà stampato sul certificato tra i dati anagrafici.

6.1.16 DatiOperatore

È l'elemento contenitore dei dati dell'operatore che richiede il certificato.

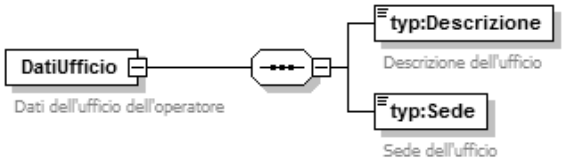


Nome Elemento	Descrizione	Tipo	Lunghezza
DatiOperatore	Dati dell'operatore	Tipo complesso	--
Composto dalle seguenti proprietà:			
Cognome	Cognome dell'operatore	string72	72
Nome	Nome dell'operatore	string72	72
CodiceOperatore	Codice univoco dell'operatore	String	40
DatiUfficio	Dati dell'ufficio dell'operatore	Tipo complesso	--

Le proprietà Cognome e Nome, oltre le 26 lettere dell'alfabeto latino, possono contenere soltanto lo spazio, l'apostrofo ed i caratteri diacritici definiti nell'omonima tabella presente sul sito CERPA-WEB. Nessun altro carattere è consentito.

6.1.17 DatiUfficio

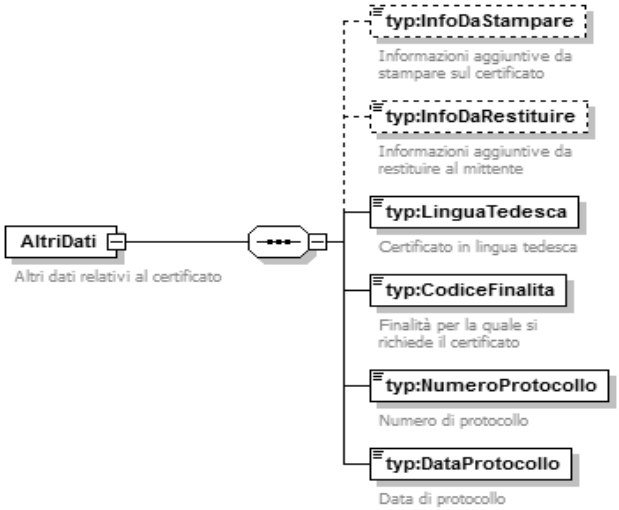
È l'elemento contenitore dei dati relativi all'ufficio di appartenenza dell'operatore che effettua la richiesta.



Nome Elemento	Descrizione	Tipo	Lunghezza
DatiUfficio	Dati dell'ufficio dell'operatore	Tipo complesso	--
Composto dalle seguenti proprietà:			
Descrizione	Descrizione dell'ufficio	string	300
Sede	Sede dell'ufficio	string	60

6.1.18 AltriDati

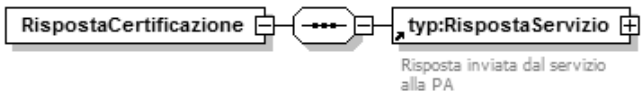
È l'elemento contenitore di dati aggiuntivi, relativi al certificato richiesto per un nominativo.



Nome Elemento	Descrizione	Tipo	Lunghezza
AltriDati	Altri dati relativi al certificato	Tipo complesso	--
Composto dalle seguenti proprietà:			
InfoDaStampare	Informazioni aggiuntive da stampare sul certificato	string	100
InfoDaRestituire	Informazioni aggiuntive da restituire al mittente	string	100
LinguaTedesca	Certificato in lingua tedesca	boolean	N.D.
CodiceFinalita	Finalità per la quale si richiede il certificato	string	3
NumeroProtocollo	Numero di protocollo	integer	6
DataProtocollo	Data protocollo	date	--

6.1.19 RispostaCertificazione

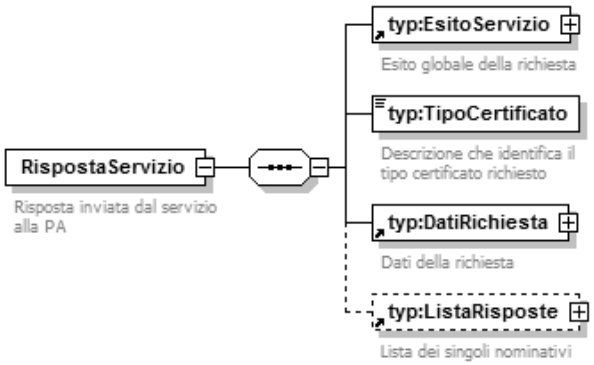
È il wrapper della risposta emessa dal servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RispostaCertificazione	Wrapper della risposta inviata dal servizio alla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
RispostaServizio	Risposta inviata dal servizio alla PA	Tipo complesso	--

6.1.20 RispostaServizio

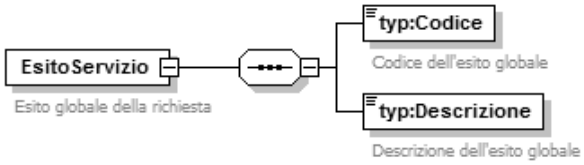
È il contenitore delle informazioni relative alla risposta emessa dal servizio.



Nome Elemento	Descrizione	Tipo	Lunghezza
RispostaServizio	Risposta inviata dal servizio alla PA	Tipo complesso	--
Composto dalle seguenti proprietà:			
EsitoServizio	Esito globale della richiesta	Tipo complesso	--
TipoCertificato	Descrizione che identifica il tipo certificato richiesto	string	--
DatiRichiesta	Dati della richiesta	Tipo complesso	--
ListaRisposte	Lista dei singoli nominativi	Tipo complesso	--

6.1.21 EsitoServizio

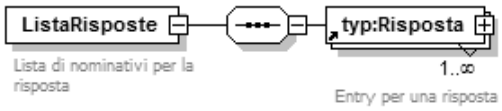
È l'esito globale della richiesta.



Nome Elemento	Descrizione	Tipo	Lunghezza
EsitoServizio	Esito globale della richiesta	Tipo complesso	--
Composto dalle seguenti proprietà:			
Codice	Codice dell'esito globale	integer	3
Descrizione	Descrizione dell'esito globale	string	200

6.1.22 ListaRisposte

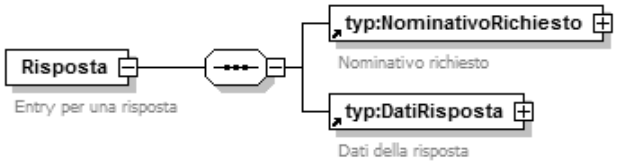
È una lista di oggetti Risposta, uno per ogni NominativoRichiesto presente sulla richiesta.



Nome Elemento	Descrizione	Tipo	Lunghezza
ListaRisposte	Lista di nominativi per la risposta	Tipo complesso	--
Composto dalle seguenti proprietà:			
Risposta	Entry per una risposta	Tipo complesso	--

6.1.23 Risposta

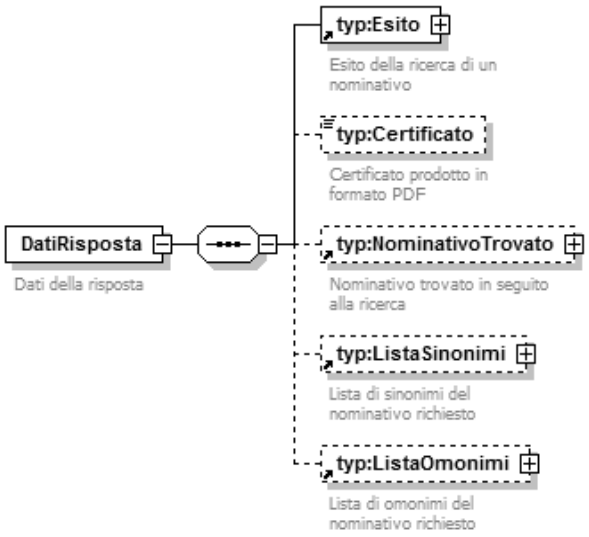
È l'elemento contenitore della risposta per ogni nominativo richiesto.



Nome Elemento	Descrizione	Tipo	Lunghezza
Risposta	Entry per una risposta	Tipo complesso	--
Composto dalle seguenti proprietà:			
NominativoRichiesto	Nominativo richiesto	Tipo complesso	--
DatiRisposta	Dati della risposta	Tipo complesso	--

6.1.24 DatiRisposta

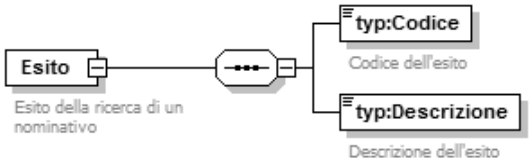
È l'elemento contenitore dei dati dettagliati della risposta, fornisce un esito, il certificato prodotto, l'eventuale nominativo trovato, o le eventuali liste di sinonimi ed omonimi.



Nome Elemento	Descrizione	Tipo	Lunghezza
DatiRisposta	Dati della risposta	Tipo complesso	--
Composto dalle seguenti proprietà:			
Esito	Esito della ricerca di un nominativo	Tipo complesso	--
Certificato	Certificato prodotto in formato PDF	base64Binary	N.D.
NominativoTrovato	Nominativo trovato in seguito alla ricerca	Tipo complesso	--
ListaSinonimi	Lista di sinonimi del nominativo richiesto	Tipo complesso	--
ListaOmonimi	Lista di omonimi del nominativo richiesto	Tipo complesso	--

6.1.25 Esito

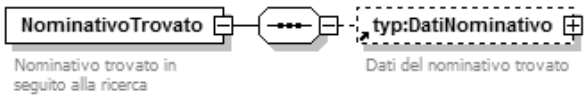
Indica l'esito dell'elaborazione della richiesta per un singolo nominativo.



Nome Elemento	Descrizione	Tipo	Lunghezza
Esito	Esito della ricerca di un nominativo	Tipo complesso	--
Composto dalle seguenti proprietà:			
Codice	Codice dell'esito	integer	3
Descrizione	Descrizione dell'esito	string	200

6.1.26 NominativoTrovato

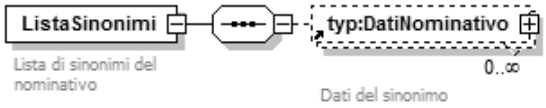
È l'elemento contenitore dei dati dell'eventuale nominativo trovato.



Nome Elemento	Descrizione	Tipo	Lunghezza
NominativoTrovato	Nominativo trovato in seguito alla ricerca	Tipo complesso	--
Composto dalle seguenti proprietà:			
DatiNominativo	Dati del nominativo trovato	Tipo complesso	--

6.1.27 ListaSinonimi

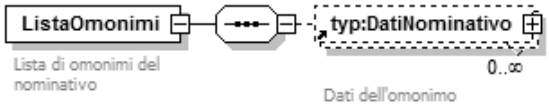
È una lista di oggetti DatiNominativo, ognuno dei quali rappresenta un sinonimo del nominativo richiesto.



Nome Elemento	Descrizione	Tipo	Lunghezza
ListaSinonimi	Lista di sinonimi del nominativo	Tipo complesso	--
Composto dalle seguenti proprietà:			
DatiNominativo	Dati del sinonimo	Tipo complesso	--

6.1.28 ListaOmonimi

È una lista di oggetti DatiNominativo, ognuno dei quali rappresenta un sinonimo del nominativo richiesto.



Nome Elemento	Descrizione	Tipo	Lunghezza
ListaOmonimi	Lista di omonimi del nominativo	Tipo complesso	--
Composto dalle seguenti proprietà:			
DatiNominativo	Dati dell'omonimo	Tipo complesso	--

6.2 Documento xsd: Definizione tipi

6.2.1 String72

È un tipo semplice di tipo String con lunghezza massima 72 caratteri.

Nome Tipo	Descrizione	Tipo	Lunghezza
string72	Tipo semplice per la definizione di nomi lunghi massimo 72 caratteri	string	72

7 Gestione esiti ed errori

Il sistema CERPA prevede due strutture dati dedicate alla gestione degli esiti dell'elaborazione delle richieste di certificazione:

1. EsitoServizio, contenitore per l'esito globale dell'elaborazione della richiesta;
2. Esito, specifico per un singolo nominativo.

Entrambe le strutture hanno un comportamento polivalente, in quanto sono usati sia per restituire un errore, sia per restituire l'esito. La loro struttura è descritta in dettaglio nel capitolo 4, mentre di seguito sono esposti i valori dei codici di errore con le relative descrizioni.

Nel caso in cui la struttura dati EsitoServizio, riferita quindi alla richiesta, presenti uno dei seguenti codici:

- 101 – Errore interno generico
- 102 – Errore applicativo generico
- 110 – Certificato digitale scaduto

oppure la struttura dati Esito, riferita al singolo nominativo, presenti uno dei seguenti codici:

- 007 – Il certificato non è stato prodotto poiché il soggetto non è sincronizzato.
- 104 - Errore nell'invocazione della Ricerca Soggetto/Ente

oppure nessuna risposta sia pervenuta

la PA interessata dovrà contattare il servizio di assistenza istituito presso l'Ufficio del Casellario Centrale, al numero reperibile all'interno del sito CERPA-WEB, al fine di sapere quando inviare nuovamente la richiesta.

7.1 Errori ed esiti a livello di richiesta - EsitoServizio

7.1.1 Errori

Codici di errore relativi all'intera richiesta:

Codice	Descrizione
000	Nessun errore riscontrato in fase di validazione.
101	Errore interno generico.
102	Errore applicativo generico.
110	Il certificato digitale è scaduto

Codici di errore relativi ai dati contenuti nell'oggetto Richiesta Certificazione

Codice	Descrizione
150	Manca richiesta servizio.

Codici di errore relativi ai dati contenuti nell'oggetto Richiesta Servizio

Codice	Descrizione
200	Mancano i dati richiesta.
201	Manca la lista dei nominativi
202	Manca l'indirizzo IP del mittente
203	Manca la versione del XSD
210	Indirizzo IP del mittente non valido
211	Versione XSD non valida
220	Lista nominativi vuota

Codici di errore relativi ai dati contenuti nell'oggetto Dati Richiesta

Codice	Descrizione
250	ID richiesta obbligatorio
251	L'identificativo dell'ente richiedente è obbligatorio.
252	La data della richiesta è obbligatoria.
253	L'ora della richiesta è obbligatoria.
254	Il codice convenzione è obbligatorio.
260	ID richiesta non valido
261	Identificativo dell'ente richiedente non valido.
262	Data della richiesta non valida.
263	Ora della richiesta non valida.
264	Il codice convenzione non è valido.
271	Il valore dell'ID richiesta eccede la lunghezza massima.
280	Tipo di certificato richiesto non autorizzato
281	ID della richiesta non univoco.
282	La convenzione è scaduta.

Il codice e la descrizione definiti in questa tabella ed in quella successiva, rappresentano le omonime proprietà che caratterizzano la struttura EsitoServizio.
Per ogni chiamata è sempre possibile conoscere la buona riuscita o meno della funzionalità andando ad indagare sui valori restituiti da questa struttura.

7.1.2 Esiti

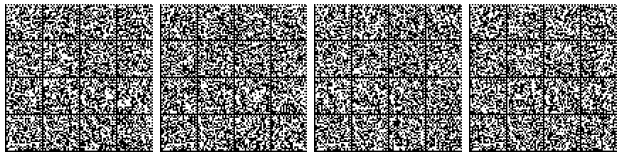
Di seguito è riportata una tabella con i codici esito relativi all'intera richiesta:

Codice	Descrizione
100	Richiesta elaborata correttamente

Il codice 100 indica che la richiesta ricevuta è stata elaborata correttamente, tuttavia questo non esclude la possibilità che uno o più nominativi abbiano generato un errore locale, a livello di singolo nominativo, riportato nell'oggetto Esito.

7.2 Errori ed esiti a livello di nominativo - Esito

Per ogni nominativo richiesto, è sempre fornita una risposta, all'interno della quale è presente l'oggetto Esito. Come per EsitoServizio (oggetto addetto al trasporto delle informazioni sugli errori e sugli esiti a livello di richiesta), l'oggetto Esito trasporta il codice e la descrizione di un errore o di un esito relativo al singolo nominativo.



7.2.1 Errori

Codici di errore applicativi relativi al singolo nominativo:

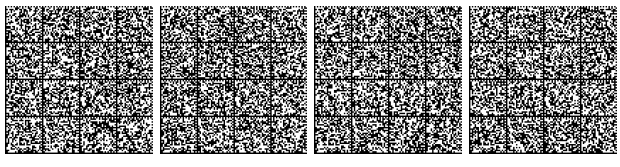
Codice	Descrizione
104	Errore nell'invocazione della Ricerca Soggetto/Ente

Codici di errore relativi ai dati contenuti nell'oggetto NominativoRichiesto:

Codice	Descrizione
300	Progressivo nominativo obbligatorio
301	Dati nominativo obbligatori
302	Dati operatore obbligatori
303	Altri dati obbligatori

Codici di errore relativi ai dati contenuti nell'oggetto DatiNominativo CASELLARIO GIUDIZIALE:

Codice	Descrizione
310	Cognome obbligatorio
311	Nome obbligatorio
312	Sesso obbligatorio
313	Codice fiscale soggetto obbligatorio
314	Dati nascita obbligatori
320	Cognome non valido
321	Nome non valido
322	Sesso non valido
323	Codice fiscale non valido
324	Codice CUI non valido
325	Paternità non valida
330	Campo cognome eccede la lunghezza massima
331	Campo nome eccede la lunghezza massima
332	Campo paternità eccede la lunghezza massima
333	Campo codice fiscale eccede la lunghezza massima
334	Campo CUI eccede la lunghezza massima

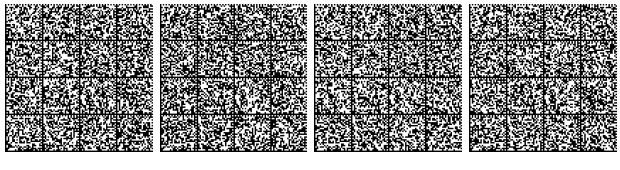


Codici di errore relativi ai dati contenuti nell'oggetto DatiNascita:

Codice	**Descrizione**
350	Giorno nascita obbligatorio
351	Mese nascita obbligatorio
352	Anno nascita obbligatorio
353	Codice Catasto luogo di nascita obbligatorio
354	Codice Catasto nazione di nascita obbligatorio
355	Se campo codice Catasto stato di nascita diverso da italia (00000), il campo codice Catasto luogo di nascita non deve essere impostato
360	Data di nascita non valida
361	Giorno di nascita non valido
362	Mese di nascita non valido
363	Anno di nascita non valido
364	Codice Catasto luogo di nascita non valido
365	Codice Catasto nazione di nascita non valido
370	Campo Codice Catasto luogo di nascita eccede lunghezza massima
371	Campo Comune straniero di nascita eccede la lunghezza massima
372	Campo Codice Catasto stato di nascita eccede lunghezza massima
373	Campo giorno di nascita eccede la lunghezza massima
374	Campo mese di nascita eccede la lunghezza massima
375	Campo anno di nascita eccede la lunghezza massima

Codici di errore relativi ai dati contenuti nell'oggetto DatiNominativo SANZIONI AMMINISTRATIVE:

Codice	**Descrizione**
410	Denominazione sociale obbligatoria
411	Forma giuridica obbligatoria
412	Dati sede sociale obbligatori
420	Forma giuridica non valida
421	Partita IVA non valida
423	Codice fiscale ente non valido
430	Campo denominazione sociale eccede la lunghezza massima
431	Campo forma giuridica eccede la lunghezza massima
433	Campo codice fiscale eccede la lunghezza massima
434	Campo partita IVA eccede la lunghezza massima



Codici di errore relativi ai dati contenuti nell'oggetto DatiSedeSociale:

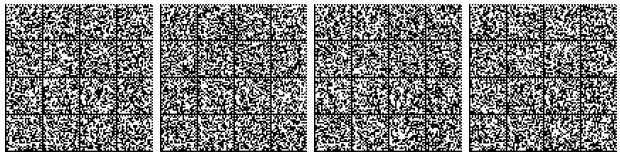
Codice	Descrizione
450	Indirizzo obbligatorio
451	Codice Catasto stato sede obbligatorio
452	Codice Catasto sede obbligatorio
453	Se campo codice Catasto stato della sede diverso da italia (00000), il campo codice Catasto comune della sede non deve essere impostato
461	Codice Catasto sede non valido
462	Codice Catasto stato sede non valido
470	Campo indirizzo eccede la lunghezza massima
471	Campo codice Catasto sede sociale eccede la lunghezza massima
472	Campo comune straniero sede sociale eccede la lunghezza massima
473	Campo codice Catasto stato sede sociale eccede la lunghezza massima

Codici di errore relativi ai dati contenuti nell'oggetto DatiOperatore:

Codice	Descrizione
500	Codice operatore obbligatorio
501	Dati ufficio obbligatori
510	Cognome operatore non valido
511	Nome operatore non valido
520	Campo codice operatore eccede la lunghezza massima
521	Campo cognome operatore eccede la lunghezza massima
522	Campo nome operatore eccede la lunghezza massima

Codici di errore relativi ai dati contenuti nell'oggetto DatiUfficio:

Codice	Descrizione
550	Sede ufficio obbligatoria
551	Descrizione ufficio obbligatoria
560	Sede ufficio non valida
561	Descrizione ufficio non valida
570	Campo sede ufficio eccede la lunghezza massima
571	Campo descrizione ufficio eccede la lunghezza massima



Codici di errore relativi ai dati contenuti nell'oggetto AltriDati:

Codice	Descrizione
600	Codice finalità obbligatorio
601	Numero protocollo obbligatorio
602	Data protocollo obbligatoria
611	Codice finalità non valido
612	Numero protocollo non valido
613	Data protocollo non valida
614	Codice finalità non autorizzata
615	Alla data odierna la finalità richiesta non è valida
616	Alla data odierna la finalità richiesta è sospesa
621	Campo info da stampare eccede la lunghezza massima
622	Campo info da restituire eccede la lunghezza massima
623	Campo codice finalità eccede la lunghezza massima
624	Campo numero protocollo da stampare eccede la lunghezza massima

7.2.2 Esiti

Di seguito la tabella dettagliata con i codici esito relativi al singolo nominativo:

Codice	Descrizione
001	Per il nominativo richiesto il certificato prodotto risulta positivo.
002	Per il nominativo richiesto il certificato prodotto risulta positivo ma sono stati trovati dei sinonimi. Verificare la lista degli sinonimi.
003	Per il nominativo richiesto il certificato prodotto risulta nullo.
004	Per il nominativo richiesto il certificato prodotto risulta nullo ma sono stati trovati dei sinonimi. Verificare la lista dei sinonimi.
005	Per il nominativo richiesto sono stati trovati degli omonimi. Il certificato non è stato prodotto. Verificare la lista degli omonimi.
006	Il certificato non è stato prodotto poiché il soggetto risulta deceduto.
007	Il certificato non è stato prodotto poiché il soggetto non è sincronizzato.
008	Il certificato non è stato prodotto poiché il soggetto è in lavorazione.
009	Il certificato non è stato prodotto poiché il soggetto è con errori.
010	Il certificato non è stato prodotto poiché il soggetto è minorenne.

8 Informazioni in merito all'acquisizione del certificato di firma elettronica di cui all'articolo 7, comma 8, del decreto dirigenziale

8.1 Soggetto fornitore - Certification Authority (CA)

Ministero della Giustizia – Dipartimento dell'Organizzazione Giudiziaria, del personale e dei servizi - Direzione Generale per i Sistemi Informativi Automatizzati – Ufficio sistemi di rete e innovazioni tecnologiche (DGSIA).

Sede - Via Crescenzio – 17/C - 00193 Roma

Sito web - http://www.giustizia.it

8.2 Oggetto

E' la certificazione della chiave pubblica appartenente alla coppia di chiavi asimmetriche (chiave privata e chiave pubblica) generata autonomamente dalla PA.

Tale certificazione permette di instaurare una comunicazione sicura garantendo alle parti l'identità comunicante e la riservatezza dei dati trasmessi.

La procedura di richiesta e rilascio del certificato sono gestite dalla CA, previa comunicazione alla stessa dell'indicazione delle PA ammesse all'accesso diretto del SIC da parte dell'Ufficio Centrale del Casellario.

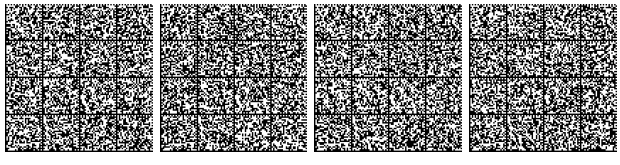
8.3 Procedure operative

La procedura per la certificazione si compone delle seguenti fasi:

- richiesta del certificato
- emissione del certificato

8.3.1 Richiesta del certificato

La richiesta, corredata dal file CSR, sarà inoltrata dalla PA alla CA tramite Posta Elettronica Certificata al seguente indirizzo di PEC: dgsia.dog@giustiziacert.it.



8.3.2 Il file CSR (Certificate Signing Request)

Il file CSR, contenente la richiesta di certificazione, conterrà la firma generata con la chiave privata corrispondente alla chiave pubblica che si desidera sia certificata, in modo da fornire prova di possesso della medesima chiave privata.

Nel file CSR dovranno essere inserite almeno le seguenti informazioni:

- il nome del referente da certificare (Common Name) = <nome PA>CERPA ;
- la denominazione dell'Amministrazione pubblica/Ente richiedente (Organization);
- l'ente responsabile dell'applicazione (Organizational Unit);
- la codifica fissa "IT" per il codice identificante il paese dell'ente proprietario del dominio (Country);

8.3.3 Caratteristiche della chiave pubblica da certificare

La lunghezza della chiave pubblica di cui si richiede la certificazione (e della corrispondente chiave privata) non deve essere inferiore ai 2048 bit allo scopo di fornire adeguate garanzie di sicurezza.

L'algoritmo di crittografia asimmetrica (hashing) da utilizzare è sha1.

Key usage: Digital signature.

Henhanced key usage: vuoto.

8.3.4 Emissione del certificato

La CA, verificata la provenienza, l'integrità e le autorizzazioni del mittente della busta crittografica, e verificata presso il Casellario Centrale la sussistenza delle condizioni per l'accesso diretto al SIC, metterà a disposizione il certificato richiesto trasmettendolo via PEC alla PA richiedente che, a sua volta, invierà la chiave pubblica al Casellario all'indirizzo di PEC uff3.dgpenale.dag@giustiziacert.it.

Analogamente il Casellario risponderà all'Amministrazione interessata inviando la chiave pubblica del proprio certificato.

La CA non darà corso all'emissione del certificato qualora i dati comunicati non risultino corretti o completi in base ai riscontri derivanti dalle verifiche poste in essere.

8.3.5 Formato del certificato e sua validità

Il certificato emesso è conforme al formato standard X.509 v3, codificato in base64, per quanto riguarda gli attributi in esso presenti e il relativo utilizzo.

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (validity) con gli attributi "valido dal" (not before) e "valido fino al" (not after).

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

La durata del certificato è stabilita in anni 3.

8.4 Revoca, sospensione e rinnovo del certificato

La revoca o la sospensione di un certificato ne tolgono la validità e rendono non validi gli utilizzi della corrispondente chiave privata effettuati successivamente al momento di revoca o sospensione.

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore e pubblicata con periodicità prestabilita nel registro dei certificati.

La revoca e la sospensione di un certificato hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso e degli utilizzi della corrispondente chiave privata effettuati successivamente a tale momento.

8.4.1 Revoca

Il Certificatore può eseguire la revoca del certificato su propria iniziativa o su richiesta del titolare. La revoca va chiesta nel caso si verifichino le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia venuta meno la segretezza della medesima, ovvero si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata stessa;
- il titolare non riesce più ad utilizzare il certificato in suo possesso;
- si verifica un cambiamento dei dati presenti nel certificato;
- termina il rapporto tra il titolare e il Certificatore.

8.4.2 Sospensione

Il Certificatore può eseguire la sospensione del certificato su propria iniziativa o su richiesta del titolare. La sospensione va richiesta nel caso in cui si verifichino le seguenti condizioni:

- è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il titolare o il Certificatore acquisiscono elementi di dubbio sulla validità del certificato;
- si presenta la necessità di un'interruzione della validità del certificato.

8.4.3 Rinnovo

Allo scadere del proprio certificato, l'Amministrazione interessata dovrà provvedere al suo rinnovo inoltrando la richiesta alla CA competente. Analogamente dovrà fare il Casellario.

Le chiavi pubbliche scambiate precedentemente non dovranno essere aggiornate.