Sistema Federato Interregionale di Autenticazione: ORGANIZZAZIONE

Versione 1.0

INDICE

1. MODIFICHE DOCUMENTO

Descrizione Modifica	Edizione	Data
Revisione iniziale	1.0	12/01/2007

2. TERMINI ED ACRONIMI

Accordo di cooperazione: Insieme di accordi di servizio di un dominio di cooperazione

Accordo di servizio: Definizione delle funzionalità, interfacce, requisiti di sicurezza e di qualità di servizio di un servizio

ACoop: Accordo di cooperazione

Architettura ICAR: Architettura generale del Sistema di Cooperazione

AS: Accordo di servizio

Asserzione d'attributo:E' un documento firmato digitalmente che asserisce gli attributi di un Utente

Asserzione d'autorizzazione:E un documento firmato digitalmente che asserisce l'abilitazione di un Utente ad accedere in un determinato Contesto d'erogazione ad un determinato Servizio (risorsa)

Asserzione d'identità:E' un documento firmato digitalmente che asserisce l'identità di un Utente.

Asserzione di Certificatore:E' un'Asserzione d'attributo rilasciata dal Coordinatore del Dominio di Cooperazione CDC al Certificatore che ne attesta:

- la partecipazione al Dominio di Cooperazione secondo le regole stabilite dalla comunità sotto la supervisione dello stesso Garante;
- l'autorità d'attribuzione (elenco di attributi che è autorizzato a certificare) per i Certificatori degli attributi

Asserzione di Dominio:E' un'Asserzione d' attributo rilasciata dal Garante al Dominio che ne attesta la partecipazione al Dominio di Cooperazione secondo le regole stabilite dalla comunità e sotto la supervisione dello stesso responsabile

Autoasserzione Di Identità: Asserzione di identità sottoscritta dal soggetto stesso con un dispositivo di firma.

Autorizzazione: Individua la procedura che stabilisce se un Utente autenticato presso un Dominio e che sta richiedendo la fruizione di uno specifico servizio erogato dal Dominio, ha diritto o meno alla fruizione. L'autorizzazione viene attribuita verificando l'esistenza di un accreditamento dell'Utente che sia compatibile con le Politiche d'accesso al servizio. Ad esempio in base all'esistenza di una qualifica o ruolo, associata all'utente e al Dominio, appartenente all'insieme delle qualifiche/ruoli abilitate all'accesso al servizio.

Certificatore degli attributi:E' l'entità ("interna a" o "coincidente con" un dominio) che si fa garante dell'associazione di determinati attributi ad una data identità attraverso l'emissione di un'Asserzione di attributo

Certificatore dell'identità:E' l'entità ("interna a" o "coincidente con" un dominio) che accerta l'identità di un utente e se ne fa garante rispetto ai terzi attraverso l'emissione di un'Asserzione di identità

Certificatore delle politiche di autorizzazione:E' l'entità ("interna a" o "coincidente con" un dominio) che si fa responsabile di valutare le Politiche d' accesso ad un servizio sulla base delle asserzioni presentate dal Dominio richiedente attraverso l'emissione di un'Asserzione di.autorizzazione

CNIPA: Centro nazionale per l'informatica nella Pubblica Amministrazione

Comunità ICAR: Insieme dei soggetti ICAR

Contesto applicativo: Il contesto applicativo rappresenta l'ambito applicativo nel quale si sviluppa il processo di cooperazione. Vi possono essere Contesti applicativi dove partecipano più domini così

come domini dove partecipano più contesti applicativi. Nell'ambito di uno stesso Contesto applicativo i processi d'autenticazione dei rispettivi domini devono condividere semantica e formalismo delle informazioni scambiate

Contesto d'erogazione:E' il contesto entro il quale il servizio viene erogato. Il contesto viene definito attraverso molteplici fattori: l'orario, il carico dei sistemi, la ricorrenza delle richieste, la modalità di erogazione ecc

Coordinatore del Dominio di Cooperazione: Rappresenta chi garantisce il circuito ai partecipanti del Dominio di Cooperazione. E' il detentore della credenziale unica di validazione del circuito

DC: Dominio di cooperazione

Delega:E' un particolare tipo di Asserzione d'attributo che mette in relazione delegante, delegato e la funzione delegata. L'Asserzione di delega dovrà avere come Certificatore degli attributi

Dominio: Insieme dei sistemi di cui un soggetto è titolare

Dominio dei servizi applicativi: Insieme dei servizi di cui un soggetto è erogatore

Dominio di Cooperazione: Insieme di Amministrazioni che cooperano per l'automazione di un insieme di procedimenti amministrativi

Dominio erogante: Rappresenta il dominio con la responsabilità dell'erogazione del servizio

Dominio richiedente:E' il dominio dal quale parte la richiesta. Questo dominio si assume la responsabilità di legare la richiesta all'utente.

DSA: Dominio dei Servizi Applicativi

PD: Porta di dominio

PDD: Porta di dominio delegata

Politica d'accesso:E' una regola stabilita che deve essere rispettata per poter erogare un determinato servizio. Le Politiche d'accesso si basano sulle informazioni relative all'Utente, al Servizio, Dominio richiedente ed al Contesto di erogazione.

Portafoglio delle asserzioni: Entità legata alla richiesta di servizio che integra e raccoglie tutte le Asserzioni prodotte nel processo di autorizzazione

PPAA: Pubbliche amministrazioni

Profilo del servizio:elencha gli attributi necessari ad accedere al servizio

Profilo dell'utente:è gestito direttamente e liberamente dall'Utente e reca l'indicazione degli Attributi posseduti con il riferimento ai rispettivi Certificatori d'Attributo

R.U.P.A.: Rete Unitaria della Pubblica Amministrazione

Registro SICA: Servizi SICA di registrazione e ricerca. (nel documento si ipotizza l'uso del registro IPA)

SA: Servizi applicativi

SICA: Servizi infrastrutturali di interoperabilità, cooperazione e accesso

Soggetto della comunità: Soggetto emanante di una amministrazione, un'impresa o una associazione qualificata registrato sull'indice dei soggetti del Registro SICA nazionale

SPC: Sistema Pubblico di Connettività e Cooperazione

SPConn: Sistema Pubblico di Connettività

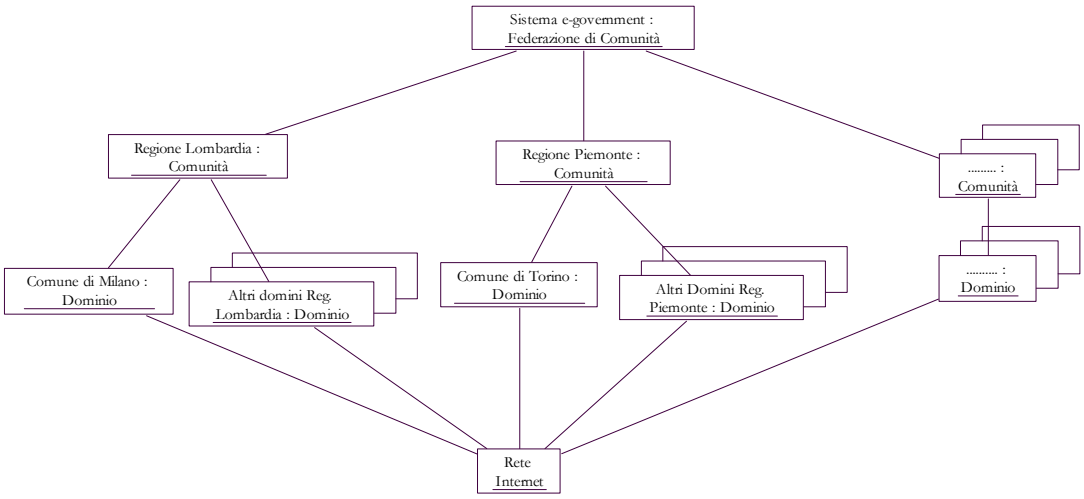
SPCoop: Sistema Pubblico di Cooperazione

3. MODELLO DI FUNZIONAMENTO ORGANIZZATIVO DEL SISTEMA FEDERATO DI AUTENTICAZIONE

Il Sistema Federato di Autenticazione (SFA) non può prescindere da un Modello di Funzionamento organizzativo chiaro e condiviso da tutta il Dominio di Cooperazione. Il presente documento fa riferimento pressoché integrale al Modello di Funzionamento Organizzativo del Sistema Pubblico di Cooperazione (SPCoop) definito dal CNIPA nell'ambito del SPC ["Sistema Pubblico di Cooperazione: ORGANIZZAZIONE" CNIPA : - v1.0: 25 novembre 2004].

La parte che segue vuole essere la contestualizzazione del succitato modello rispetto al sistema federato di autenticazione così come definito dal Modello di Riferimento.

Dal modello di riferimento si intuisce come la collettività dei soggetti che operano nell'ambito del Dominio di Cooperazione vanno a costituire una Comunità di soggetti con specifici ruoli e responsabilità. La comunità si struttura in domini di responsabilità che coincidono di fatto con Enti ed Amministrazioni All'interno di questi domini è possibile distinguere diverse attività e processi che richiedono un modello organizzativo di riferimento. L'accreditamento di un utente, di un dominio, di un Certificatore sono i processi che richiedono una precisa regolamentazione.



Il presupposto di questo modello organizzativo è che l'utente non sia noto al dominio erogatore del servizio, questi valuterà le proprie politiche d'accesso sulla base delle attestazioni di identità e di attributo fornite dall'utente. Le attestazioni in oggetto avranno la validità conferitagli dal loro sottoscrittore. Tutto il circe of trust si sostiene sul certificato del Coordinatore del Dominio di Cooperazione (CDC). Ciò che è sottoscritto con questo certificato ha per tutti gli aderenti alla comunità validità certa. Al pari del CDC possono essere considerate le Certification Authority (CA) qualificate ma, al momento, solo per le asserzioni di identità

La partecipazione alla comunità (come dominio erogatore o fruitore) così come la qualifica di dominio Certificatore, con la tipologia di attributi asseribili, può essere attestata esclusivamente dal CDC. Per altro un dominio può partecipare a più comunità contemporaneamente riconoscendo i rispettivi CDC.

Di fatto il Modello Organizzativo del Sistema Federato di Autenticazione copre molti degli aspetti trattati da SPCoop e definisce specifici soggetti, ruoli, servizi, processi e funzioni per i quali deve essere trovata una corretta collocazione.

Riprendendo i principi generali da SPCoop:

- il modello di cooperazione applicativa supporta una modalità di erogazione del servizio organizzata per adempimenti e procedimenti che derivano da dettati normativi o da compiti istituzionali;
- il modello di cooperazione applicativa è paritetico fra tutti i soggetti cooperanti;
- il modello di cooperazione è indipendente dagli assetti organizzativi dei soggetti cooperanti;
- ciascun soggetto cooperante ha la responsabilità dei servizi erogati e dei dati forniti ;
- ciascun soggetto è autonomo nella gestione dei propri sistemi e nella definizione ed attuazione delle politiche di sicurezza del proprio sistema informativo;
- ciascuna soggetto è responsabile delle autorizzazioni per l'accesso ai propri dati e/o servizi.;
- ciascun soggetto risponde della mancata applicazione degli accordi di servizio stipulati;

Il modello di funzionamento organizzativo del SFA ha per oggetto gli stessi concetti del SPCoop ed in particolare:

- I servizi
- I soggetti
- I processi

3.1. I servizi

L'interazione tra i soggetti della comunità avviene tramite servizi. Nel concetto di servizio assimileremo anche quello di evento in quanto caso particolare. Gli eventi vengono infatti notificati attraverso servizi che non prevedono un riscontro.

L'erogazione di un qualsiasi servizio da parte del Dominio dei Servizi Applicativi (DSA) non può prescindere dalla definizione di una relativa politica d'accesso. Una politica d'accesso definisce le condizioni necessarie e sufficienti per concedere l'erogazione del servizio. Essendo questo un aspetto organizzativo interno all'amministrazione non vi sono vincoli imposti a livello di Dominio di Cooperazione. Il vincolo riguarda la produzione di un atto informatico che attesti la concessione dell'abilitazione (Asserzione di autorizzazione) al servizio e la produzione degli elementi (sempre sottoforma di atto informatico) a partire dai quali questo atto può essere prodotto in base alle politiche di accesso.

Le politiche di accesso, di norma, dovrebbero essere condizionate dagli accordi di servizio stipulati tra le amministrazioni. Formalmente, è possibile che una policy differisca da un accordo di servizio, ma non in termini restrittivi rispetto all'accordo di servizio stesso.

3.1.1. Servizi applicativi e accordi di servizio

Con il termine "*sistema applicativo*" si intende genericamente l'automazione di un processo o di una funzione di cui è responsabile un soggetto sulla base della normativa vigente e dei propri compiti.

Con il termine "*servizio applicativo*" si intende un insieme di funzionalità applicative, erogate da un sistema applicativo, presentate e rese accessibili ai sistemi fruitori attraverso SPCoop.

Nell'ambito di SPCoop i sistemi applicativi possono interagire solo mediante la erogazione/richiesta di servizi (applicativi o infrastrutturali), dove la sola ed esclusiva modalità d'interazione tra il sistema erogatore e il sistema fruitore di un servizio è lo scambio di messaggi.

Per assicurare l'interoperabilità tra sistemi di servizi applicativi (o infrastrutturali) realizzati con architetture e tecniche d'implementazione eterogenee è necessario l'accordo su:

- i protocolli applicativi di scambio dei messaggi (protocolli di conversazione),
- il contenuto applicativo dei messaggi,
- i formati dei messaggi,
- i protocolli di connessione tra i punti di accesso,
- i protocolli di trasporto dei messaggi.

L'accordo sui protocolli di conversazione e il contenuto applicativo dei messaggi è stabilito a livello applicativo. Ciascun sistema componente dell'architettura di servizi, implementa, in piena autonomia e indipendenza, i componenti di gestione di detti formati e protocolli.

In SPCoop un servizio applicativo è costituito da una implementazione e da un *accordo di servizio*.

L'accordo di servizio è composto da un accordo generale di servizio, che comprende:

- la descrizione delle funzionalità,
- la descrizione delle interfacce di scambio di messaggi,
- la descrizione delle politiche e dei requisiti di sicurezza,
- la descrizione dei requisiti di qualità di servizio.

3.2.Soggetti

Di seguito sono schematizzate le principali tipologie di soggetti che potranno partecipare al dominio di cooperazione così come previsto in ambito SPC.

Soggetti	
Pubbliche Amministrazioni	"1. *al SPC partecipano tutte le amministrazioni di cui al d.gls 30 marzo 2001, n.165.* *2. il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n. 165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali nazionali ed europee*"[4] Tali soggetti possono essere erogatori o fruitori di servizi applicativi, erogatori di servizi SICA, responsabili di domini di cooperazione[5]. " *Le pubbliche amministrazioni nell'ambito della loro autonomia funzionale e gestionale adottano nella progettazione e gestione dei propri sistemi informativi, ivi inclusi gli aspetti organizzativi, soluzioni tecniche compatibili con la cooperazione applicativa con le altre pubbliche amministrazioni, secondo le regole tecniche di cui all'articolo 16."*[6]
Imprese singole o in forma associata (consorzi, raggruppamenti..)	a) Fornitori di cui le PPAA si avvalgono per realizzare/erogare propri servizi applicativi o servizi SICA b) Soggetti qualificati come ***Erogatori SICA***
Soggetti privati	a) soggetti che operano per finalità pubbliche, esercenti di pubblici servizi Sono assimilati alle pubbliche amministrazioni per le funzioni svolte per finalità di pubblico interesse. Partecipano analogamente alle amministrazioni pubbliche al progetto ICAR Es. Poste, Banche tesoriere, Enel, ANAS … b) soggetti abilitati a cooperare con le PPAA Sono soggetti privati che hanno una sistematica necessità di interagire con le pubbliche amministrazioni e per questo possono essere (di solito attraverso le loro associazioni) abilitati ad utilizzare servizi applicativi di ICAR. (es. notai e geometri con Agenzia del Territorio, trasportatori con Ag. Dogane, Banche, …)

Le amministrazioni possono aderire a tali servizi restando comunque responsabili dell'erogazione dei servizi applicativi che rendono disponibili.

[4] art.4 schema di decreto istitutivo SPC

[5] Eventuali soggetti di natura pubblica e privata che intendano assumere ruoli sussidiari svolgendo attività di intermediazione (a livello di infrastrutture tecniche) e di integrazione devono rispettare le regole del SPCoop. Le amministrazioni possono aderire a tali servizi tenendo conto che restano comunque responsabili dell'erogazione dei servizi applicativi che rendono disponibili.

[6] art.7 comma 1 schema di decreto istitutivo SPC

3.3. Processi

Di seguito sono schematizzati i processi organizzativi fondamentali che riguardano il funzionamento complessivo del Sistema Federato di Autenticazione così come previsto in ambito ICAR.

MacroProcesso	Processo
Monitoraggio e controllo	▪ Controllo del rispetto delle regole, inclusa la verifica dei livelli di servizio ▪ Gestione reclami e controversie
Gestione Dominio Servizi Applicativi	▪ Definizione e predisposizione componenti di base del DSA ▪ Registrazione /aggiornamento/chiusura del DSA (comprende la qualificazione dei soggetti)
Gestione Dominio di Cooperazione	▪ Costituzione del DC (definizione dell'accordo istitutivo, della tipologia di amministrazioni che possono/devono partecipare al domino e dei procedimenti coinvolti) ▪ Definizione dell'accordo di cooperazione (inclusa la scelta del fornitore dei servizi o in alternativa predisposizione dei servizi per il Dominio di Cooperazione) ▪ Registrazione del DC e dei servizi erogati ▪ Adesione al DC
Erogazione dei servizi applicativi	▪ Erogazione dei servizi applicativi ▪ Gestione delle autorizzazioni individuali e delle politiche di accesso ai servizi ▪ Verifica Autorizzazione all'erogazione di servizi applicativi
Fruizione dei servizi applicativi	▪ Fruizione dei servizi
Certificazione dell'identità	▪ Gestione degli utenti ▪ Gestione credenziali ▪ Riconoscimento dell'utente ▪ Rilascio asserzione d'identità per l'utente
Certificazione degli attributi	▪ Gestione degli utenti ▪ Gestione attributi dell'utente ▪ Identificazione del richiedente ▪ Rilascio asserzioni di attributo per l'utente
Autorizzazione	▪ Registrazione dei servizi ▪ Gestione delle politiche di accesso ▪ Identificazione del richiedente ▪ Rilascio asserzioni di autorizzazione

3.3.1. *Monitoraggio e controllo*

Di seguito viene riportata una descrizione sintetica dei processi relativi al macro processo di monitoraggio e controllo.

Monitoraggio e Controllo		
Processo	**Attori**	**Ruolo**
• **Controllo del rispetto delle regole, inclusa la verifica dei livelli di servizio**	Coordinatore del Dominio di Cooperazione	Il CDC manterrà attivo un osservatorio con il compito di monitorare in via continuativa il corretto svolgimento di tutte le attività all'interno dello specifico DC. Per la verifica dei livelli di servizio il CDC predisporrà dei piani di test che verranno eseguiti periodicamente o su esplicita richiesta degli Enti.
• **Gestione reclami e controversie**		Il Coordinatore provvederà ad istituire un servizio di gestione dei reclami e delle controversie. Tale servizio dovrà essere opportunamente regolamentato e gestito..

3.3.2. *Gestione del Dominio dei Servizi Applicativi*

Di seguito viene riportata una descrizione sintetica dei processi relativi alla formazione ed alla gestione del Dominio di Servizi applicativi (DSA), compresa la relativa Porta di Dominio

Gestione DSA		
Processo	**Attori**	**Ruolo**
• **Definizione e predisposizione delle componenti di base del DSA** ✓ Attivazione della Porta di Dominio Comprende tutte le attività "di base" necessarie per predisporre le infrastrutture e l'organizzazione ICT per erogare e/o per fruire di servizi applicativi	Soggetto della comunità	Definisce l'organizzazione del DSA, in termini di responsabilità, funzionamento e modalità operative di esercizio. E' responsabile della realizzazione e gestione delle componenti di base (servizi applicativi del DSA e Porta di Dominio), anche se affidate a terzi. Predispone il piano di sviluppo del DSA in termini di offerta e di fabbisogno di servizi applicativi su ICAR.
• **Registrazione/aggiornamento/ chiusura del DSA** ✓ Verifica funzionalità della Porta di Dominio ✓ Richiesta di qualificazione del soggetto e di registrazione del DSA ✓ Registrazione del responsabili del DSA e delle figure delegate alla gestione della sicurezza. ✓ Aggiornamento caratteristiche DSA/ Porta di Dominio ✓ Richiesta di chiusura del DSA	Soggetto della comunità	Verifica/collauda le funzionalità standardizzate della Porta di Dominio in conformità alle regole di ICAR. Fornisce le informazioni necessarie per l'istruttoria di qualificazione del soggetto e la registrazione del DSA; allega il certificato di collaudo (o il verbale di verifica) per l'accettazione della Porta di Dominio. Il responsabile del DSA potrà individuare altre figure cui delegare la gestione parziale o totale della sicurezza del sistema. Presenta la richiesta di chiusura del DSA.; l'evento, considerato eccezionale, va comunicato con congruo anticipo.
	Coordinatore del Dominio di Cooperazione	Provvede alla registrazione/cancellazion del responsabile del DSA sul registro SICA secondario. Provvede alla registrazione/cancellazione del DSA sul registro SICA secondario

3.3.3. Gestione del Dominio di Cooperazione

Di seguito è descritto il processo di costituzione e di partecipazione ad un Dominio di Cooperazione. Il processo di gestione di ciascun servizio applicativo richiesto/erogato nell'ambito del Dominio di Cooperazione rientra in via generale nei processi descritti nei due successivi paragrafi, salvo quanto espressamente indicato di seguito.

Gestione Dominio di Cooperazione(DC)		
Processo	**Attori**	**Ruolo**
	Coordinatore del Dominio di Cooperazione	Promuove e provvede alla emanazione della normativa, alla stipula di eventuali protocolli di intesa e degli accordi necessari. Propone e concorda con i soggetti aventi diritto le finalità, i servizi applicativi, le responsabilità e quanto altro necessario al corretto adempimento dei procedimenti indirizzati.

Gestione Dominio di Cooperazione(DC)		
Processo	**Attori**	**Ruolo**
	Soggetto promotore	Collabora con il soggetto responsabile nella definizione degli accordi e della normativa.
▪ **Definizione dell'Accordo di cooperazione**	Coordinatore del Dominio di Cooperazione	Presiede la Commissione di Coordinamento del DC Propone e concorda con i soggetti aventi diritto: - l'accordo di cooperazione, - gli accordi di servizio per i servizi applicativi organici al Dominio di Cooperazione. Individua e specifica i SICA, di base, accessori ed opzionali, necessari al Dominio di Cooperazione coerenti con il piano delle esigenze dei procedimenti coinvolti dalla cooperazione.
▪ **Registrazione del Dominio di Cooperazione e dei servizi erogati**	Coordinatore del Dominio di Cooperazione	Registra l'accordo di cooperazione nel Registro SICA del DC ed in quello nazionale. E' responsabile della gestione del ciclo di vita dell'accordo di cooperazione e della coerenza degli accordi di servizio per i servizi organici al DC Aggiorna l'accordo di cooperazione. Notifica la chiusura dell'accordo.
• **Adesione al Dominio di Cooperazione**	Soggetto della Comunità	Definisce il piano dei servizi che eroga/fruisce nell'ambito del DC; Dichiara se i propri servizi sono messi a disposizione anche di altre amministrazioni (attraverso altri DC) Richiede di partecipare al DC; sottoscrive gli accordi. Concorda se i propri servizi possono essere interfacciati in modo trasparente dall'esterno del DC, attraverso la Porta di Dominio del soggetto responsabile del DC.
	Coordinatore del Dominio di Cooperazione	Esamina le richieste di adesione/revoca Registra/cancella i soggetti nel DC. Pubblica periodicamente le amministrazioni registrate/ cancellate ed emette le relative asserzioni.

3.3.4. Erogazione dei servizi applicativi

Come precisato in precedenza. I servizi applicativi devono essere gestiti per versioni dell'accordo di servizio. Ogni versione segue un ciclo di vita autonomo, che è definito dal soggetto responsabile dell'accordo di servizio.

Erogazione servizi applicativi		
Processo	**Attori**	**Ruolo**

Erogazione servizi applicativi		
Processo	**Attori**	**Ruolo**
• **Erogazione dei servizi applicativi** ✓ Comprende tutte le attività necessarie per gestire i singoli servizi applicativi erogati dal DSA ✓ registrazione ed erogazione del servizio sul DC ✓ monitoraggio e controllo dei servizi applicativi erogati	Soggetto della comunità	Definisce gli accordi di servizio per ciascun servizio /tipologia di fruitore Provvede a registrare i servizi erogati dal DSA sul registro SICA del DC Attiva i sistemi necessari all'erogazione del servizio Effettua il monitoraggio e controllo relativi all'erogazione dei servizi sulla base degli accordi di servizio predefiniti.
• **Gestione delle autorizzazioni individuali e delle politiche di accesso ai servizi** ✓ Gestione delle autorizzazioni ✓ Definizione della Politica di accesso	Soggetto della comunità	Gestisce, per ogni servizio erogato, le autorizzazioni individuali concesse ad utenti interni o esterni al DSA. Gestisce, per ogni servizio erogato, le politiche d'accesso che devono essere osservate per concedere l'accesso al servizio stesso. • L'associazione di una politica d'accesso ad un servizio deve essere sempre legata ad un soggetto fisico delegato dal responsabile della sicurezza per l'Amministrazione. • L'associazione di una politica d'accesso ad un servizio deve essere sempre tracciata e storicizzata con le date di attivazione e disattivazione dell'associazione.
• **Verifica delle autorizzazioni individuali e delle politiche di accesso**	Soggetto della comunità	Attiva i sistemi necessari alla verifica delle autorizzazioni e delle politiche di accesso.

3.3.5. *Fruizione servizi applicativi*

Di seguito viene riportata una descrizione sintetica dei processi relativi alla Fruizione dei servizi applicativi.

Fruizione servizi applicativi		
Processo	**Attori**	**Ruolo**
• **Fruizione dei servizi applicativi** ✓ Comprende tutte le attività necessarie per la fruizione dei singoli servizi applicativi da parte del DSA	Soggetto della comunità	Recepisce gli accordi di servizio per ciascun servizio che intende utilizzare Attiva i sistemi necessari alla fruizione del servizio Effettua il monitoraggio e controllo relativi all'erogazione dei servizi sulla base degli accordi di servizio predefiniti.

3.3.6. *Certificazione dell'identità*

Certificazione dell'identità		
Processo	**Attori**	**Ruolo**
• **Gestione degli utenti**	Soggetto Certificatore d'identità	Compito del Certificatore di identità è la gestione diretta o indiretta dei dati necessari all'accreditamento dell'utente. Nel caso della gestione diretta il Certificatore di identità è anche CA e gestirà in proprio sia la registrazione che le credenziali dell'utente. Nel caso della gestione indiretta il Certificatore di Identità si appoggerà ad una CA esterna verso la quale potrà fungere da registration authority. Esiste anche la possibilità di gestione mista dove il Certificatore si appoggerà alla CA per la gestione delle credenziali mentre si assumerà in proprio la gestione delle informazioni necessarie all'autenticazione debole (login e password).
• **Gestione delle credenziali**		La gestione delle credenziali è in carico al Certificatore di identità solo se si assume la gestione diretta dei dati di accreditamento. Sarà comunque responsabilità del Certificatore verificare la validità delle credenziali utilizzate dall'utente al momento dell'identificazione.
• **Riconoscimento dell'utente** ✓ identificazione		L'identificazione dell'utente potrà essere effettuata secondo diverse modalità. Login e password, sulla base delle informazioni di autenticazione possedute dal Certificatore. Autentica, sulla base di una negoziazione avvenuta con dispositivo di autentica (smartcard). Ogni altra modalità potrà essere ammessa purché inequivocabilmente evidenziata sulla asserzione di identità
• **Rilascio asserzioni d'identità**		Il Certificatore di identità rilascerà un'asserzione di identità firmata digitalmente con firma attribuita ad un "Certificatore di identità". L'asserzione dovrà recare l'identificativo univoco dell'utente rappresentato dal Codice Fiscale, una validità temporale e la modalità di autenticazione. L'asserzione di identità potrà essere rilasciata solo ai domini appartenenti ad uno dei Circle of Trust riconosciuto dal Certificatore. Con l'asserzione di identità dovrà essere rilasciata dal Certificatore l'asserzione che lo qualifica quale Certificatore di uno specifico Dominio di Cooperazione, sottoscritta dal Coordinatore del Dominio di Cooperazione. L'asserzione di identità viene considerata "valida" solo nell'ambito della sua validità temporale (expiration time).

3.3.7. *Certificazione degli attributi*

Certificazione degli attributi		
Processo	**Attori**	**Ruolo**
• **Gestione degli utenti**	Soggetto Certificatore d'attributo	Compito del Certificatore di attributo è la gestione e manutenzione delle informazioni legate alla qualifica degli utenti nello specifico ambito di pertinenza del Certificatore stesso. Il Certificatore di attributo si assumerà dunque l'onere di gestire l'iscrizione dell'utente, l'associazione degli attributi per i quali gli viene riconosciuta autorità e le relative condizioni di validità (es.:periodo di validità).
• **Gestione degli attributi**		Il Certificatore d'attributo si assume l'onere di mantenere costantemente aggiornate le condizioni e lo stato di validità dei singoli attributi gestiti per un dato utente.
• **Identificazione del richiedente**		Il Certificatore d'attributo può rilasciare asserzioni di attributo solo sulla base di asserzioni di identità "valide" e sottoscritte da un Certificatore di identità appartenente ad uno dei Circle of Trust riconosciuti dal Certificatore d'attributo stesso.
• **Rilascio asserzioni d'attributo**		Il Certificatore d'attributo rilascerà un'asserzione di identità firmata digitalmente con firma attribuita ad un "Certificatore di attributo". L'asserzione dovrà recare l'identificativo univoco dell'utente rappresentato dal Codice Fiscale, gli attributi certificati con il relativo valore ed una validità temporale. L'asserzione di attributo potrà essere rilasciata solo ai domini appartenenti ad uno dei Circle of Trust riconosciuto dal Certificatore. Con l'asserzione di identità dovrà essere rilasciata dal Certificatore l'asserzione che lo qualifica quale Certificatore di uno specifico Dominio di Cooperazione, sottoscritta dal Coordinatore del Dominio di Cooperazione. L'asserzione di attributo viene considerata "valida" solo nell'ambito della sua validità temporale (expiration time).

3.3.8. *Autorizzazione*

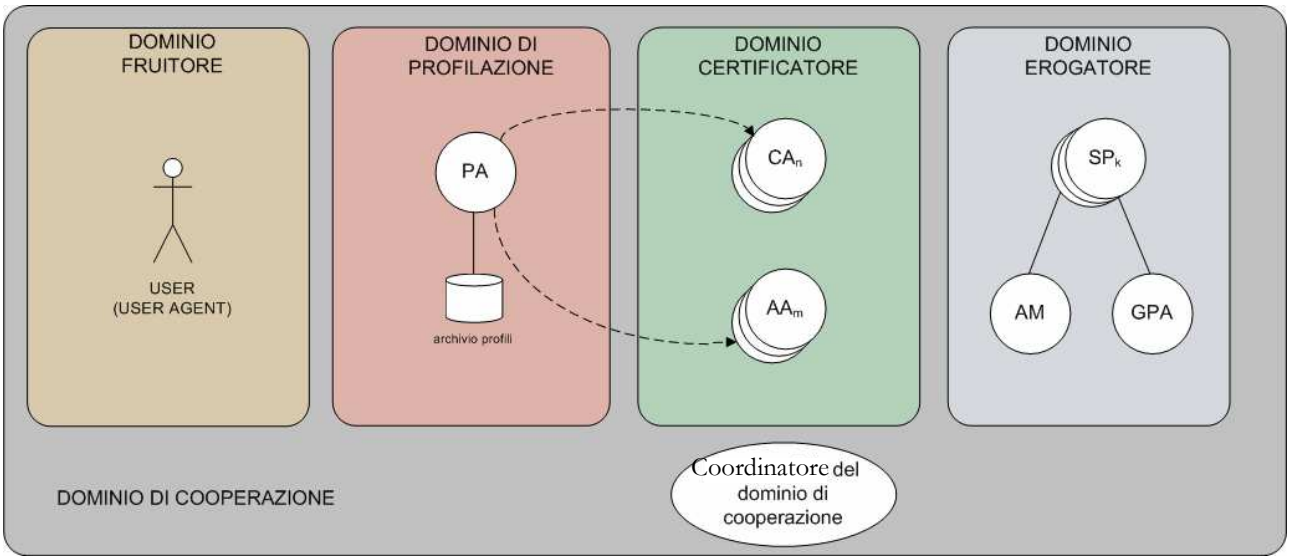
Autorizzazione		
Processo	**Attori**	**Ruolo**

Autorizzazione		
Processo	**Attori**	**Ruolo**
• **Registro dei servizi**	Soggetto Certificatore d'autorizzazione	Compito del Certificatore di atorizzazione è la gestione e manutenzione delle politiche di accesso ai vari servizi di un determinato dominio. Il Certificatore di autorizzazione si assumerà dunque l'onere di gestire la registrazione dei servizi, l'associazione delle politiche di accesso e relative condizioni di validità ricavate sulla base degli accordi di servizio.
• **Gestione delle politiche d'accesso**		Le politiche di accesso saranno gestite sulla base degli accordi di servizio presi tra le amministrazioni che partecipano al Dominio di Cooperazione. Ciò nonostante il Certificatore di autorizzazione sarà libero di applicare, su sua esclusiva responsabilità, politiche di autorizzazione diverse. La politica d'accesso sarà sempre relativa ad una risorsa (servizio) preventivamente definita e registrata.
• **Identificazione del richiedente**		Il Certificatore d'autorizzazione può rilasciare asserzioni di autorizzazione solo sulla base di asserzioni "valide" e sottoscritte da certificatori appartenenti ad uno dei Circle of Trust riconosciuti dal Certificatore d'autorizzazione stesso.
• **Rilascio asserzioni d'autorizzazione**		Il Certificatore d'autorizzazione rilascerà un'asserzione di identità firmata digitalmente con firma attribuita ad un "Certificatore di autorizzazione". L'asserzione di attributo potrà essere rilasciata solo ai domini appartenenti ad uno dei Circle of Trust riconosciuto dal Certificatore. Con l'asserzione di identità dovrà essere rilasciata dal Certificatore l'asserzione che lo qualifica quale Certificatore di uno specifico Dominio di Cooperazione, sottoscritta dal Coordinatore del Dominio di Cooperazione. L'asserzione di attributo viene considerata "valida" solo nell'ambito della sua validità temporale (expiration time).

4. SICUREZZA E PRIVACY

4.1. Gli attori

Nel modello concettuale si fa riferimento ai domini informatici (chiamati semplicemente "domini") e le entità o soggetti certificatori (chiamati anche authority). Questi sono i ruoli che, nel modello organizzativo, dovranno essere assunti dai vari soggetti coinvolti.



4.1.1. Il Coordinatore del Dominio di Cooperazione

Il Coordinatore del Dominio di Cooperazione (CDC), relativamente alla sicurezza, svolge il compito di amministratore e gestore dei meccanismi primari. Quella del CDC è ad esempio l'unica credenziale che deve essere riconosciuta da tutti i sistemi. Sarà del CDC la firma sull'asserzione di porta che abilità il soggetto ad interfacciarsi al resto della comunità. Sempre del CDC sarà la firma delle asserzioni dei certificatori che abilita i certificatori al rilascio delle rispettive asserzioni.

Il responsabile del DC deciderà la validità temporale di queste asserzioni e avrà il compito di generare via via le nuove in tempo utile per la sostituzione. La diffusione di queste asserzioni dovrà essere garantita attraverso un Directory Server pubblicamente accessibile.

4.1.2. I fruitori

Il sistema così come è stato concepito consente la massima apertura e coinvolgimento di soggetti specialmente in qualità di semplici fruitori. Qui è però necessario un distinguo tra il Dominio fruitore ed il fruitore inteso come singolo individuo. Mentre il soggetto Dominio fruitore deve poter acclarare il suo diritto a partecipare al Dominio di Cooperazione, il singolo individuo deve semplicemente essere in grado di acclarare la sua identità attraverso le credenziali rilasciate da un Certificatore riconosciuto valido all'interno del Dominio di cooperazione stesso.

4.1.3. *Il dominio di profilazione*

Per profilo dell'utente viene intesa quell'informazione che consente di associare agli attributi dichiarati come propri dall'utente medesimo i domini di certificazione che a questi attributi sono in grado di dare validità. In quest'ottica la Profile Authority(PA) ha la sola responsabilità di gestire il profilo utente consentendone allo stesso la modifica, ogni qual volta questi decida di farlo, e la pubblicazione dello stesso profilo.

4.1.4. *I certificatori*

Detto Certificatore il responsabile dell'omonimo dominio, il Certificatore è il soggetto centrale del sistema di sicurezza. Solo soggetti di conclamata affidabilità sia per ruolo istituzionale che per elevato livello qualitativo dei processi interni possono far parte dei Certificatori. Vi sono tre tipi di Certificatori:

- Certificatori di identità;
- Certificatori di attributo;
- Certificatori di autorizzazione.

4.1.4.1. Certificatore di identità

Il Certificatore di identità deve essere in grado di identificare l'utente, e come tale deve gestire un database degli utenti e riconoscere le informazioni necessarie alla loro autenticazione. E' possibile che un soggetto funga da Certificatore di identità per gli utenti che ha in carico. Molto più spesso il Certificatore di identità è un entità specifica indipendente che possiamo vedere associata ad una CA. Un caso particolare è l'autoasserzione di identità, in questo caso l'utente è Certificatore di se stesso.

4.1.4.2. Certificatore di attributo

La definizione di Certificatore di attributo è estremamente flessibile. Un Certificatore di attributo associa delle informazioni, attributi per l'appunto, ad un'identità. Un Certificatore di attributo è abilitato a certificare solo gli attributi previsti dall'asserzione di Certificatore rilasciata dal CDC.

4.1.4.3. Certificatore di autorizzazione

Di massima il Certificatore di autorizzazione è interno al DSA. Questo perché la gestione dei diritti d'acceso ai servizi è di norma un aspetto interno. Può però sussistere il caso che il Certificatore di autorizzazione sia esterno al DSA nel qual caso varranno per lui le stesse indicazioni previste per il Certificatore di attributo.

4.1.5. *Gli erogatori.*

Il responsabile di un Dominio di Erogazione risponderà del servizio offerto dal suo dominio. In questo rientra il rispetto degli accordi di servizio e la responsabilità dei processi interni al dominio alla base dell'errogazione dei singoli servizi. La responsabilità dello specifico servizio può invece essere assunta da un soggetto diverso (ad esempio il responsabile di uno specifico settore amministrativo) attraverso meccanismi che sono però propri del livello applicativo.

4.2.Autenticazione dei messaggi

4.2.1. *Firma di provenienza*

Ogni soggetto della Comunità può usare una qualsiasi firma qualificata come firma di provenienza, essendo questa utilizzata attraverso una procedura automatica di sottoscrizione, secondo la normativa [linee guida CNS 18-5-2004 cap. 10.2], non può essere utilizzata per altre operazioni di firma. Perché la Firma di provenienza venga riconosciuta come firma di un Dominio abilitato al Dominio di Cooperazione deve essere accompagnata da un'Asserzione di Dominio in corso di validità rilasciata dal Coordinatore del Dominio di Cooperazione.

4.2.2. *Asserzione di Dominio*

L'asserzione di dominio abilita il Dominio a far parte del Dominio di Cooperazione. Questa Asserzione viene rilasciata dal CDC al termine dell'iter di accettazione e verifica della richiesta di adesione.

Il CDC fissa la validità temporale di queste asserzioni e provvede alla loro riemissione in tempo utile per la loro distribuzione. La distribuzione avviene attraverso pubblicazione su un directory server accessibile a tutti i soggetti della comunità.

4.3.Autenticazione delle asserzioni

Normativamente le Asserzioni sono documenti elettronici rilasciati da un soggetto associato al Dominio di Cooperazione detto Certificatore.

Le asserzioni hanno la validità che gli viene conferita dalla firma digitale apposta sulla base della normativa vigente dall'articolo 15 della L. 59/97 al Decreto legislativo 7 marzo 2005, n. 82.

Tutte la asserzioni hanno una data di emissione ed una data di scadenza.

Alcune asserzioni devono essere messe a disposizione di tutta la comunità e per questo dovranno essere pubblicate su un directory server gestito dal CDC.

4.3.1. *Asserzione di Certificatore*

Questo è un particolare tipo di asserzione d'attributo. Ad ogni soggetto Certificatore abilitato il CDC rilascia un' Asserzione firmata con un range temporale di validità. Questa Asserzione, attraverso il certificato di firma, legittima il Certifcatore nei confronti degli altri soggetti per il rilascio di Asserzioni. Ogni Asserzione di Certificatore deve contenere anche la tipologia di Certificatore. Uno stesso soggetto può assumere più ruoli di Certificatore.

L'Asserzione di Certificatore rilasciata ai Certificatori di Attributo reca anche l'elenco degli attributi "asseribili". Questa Asserzione viene rilasciata dal CDC al termine dell'iter di accettazione e verifica della richiesta di adesione.

Il CDC fissa la validità temporale di queste asserzioni e provvede alla loro riemissione in tempo utile per la loro distribuzione. La distribuzione avviene attraverso pubblicazione su un directory server accessibile a tutti i soggetti della comunità.

4.3.2. Asserzioni di identità

L'asserzione di identità può essere rilasciata dal Certificatore d'identità, questi deve essere in grado di identificare l'utente in modo da certificarne il codice identificativo personale (CF) e la modalità di autenticazione utilizzata. Queste informazioni costituiscono il contenuto del Certificato di identità sottoscritto dal Certificatore. Questa Asserzione viene rilasciata dal CDC al termine dell'iter di accettazione e verifica della richiesta di adesione.

L'asserzione di identità è l'asserzione senza dubbio più importante. A partire infatti dall'asserzione di identità vengono poi rilasciate le asserzioni di attributo e soprattutto viene identificato univocamente il richiedente. Mentre per le altre asserzioni la validità è un concetto molto semplice e legato alla validità del contenuto stesso dell'asserzione, per l'asserzione di identità non è proprio così. L'asserzione di identità testimonia che in un dato momento il richiedente è stato riconosciuto, informazione questa spendibile solo se legata ad un'altra: la richiesta. Dunque l'asserzione di identità ha senso solo se legata in modo indissolubile, attraverso una firma digitale di porta, ad una richiesta di servizio.

4.3.2.1. Autoasserzione di identità

L'Autoasserzione di identità è un'asserzione generata sul dominio richiedente e sottoscritta dall'utente stesso con un dispositivo di firma (CNS, CIE). Questo tipo di asserzione, come nel caso dell'autocertificazione, rimette all'utente la responsabilità dell'identificazione. Ovviamente il valore dell'autoasserzione dipende esclusivamente dal tipo di certificato utilizzato per la sottoscrizione. Se il certificato è qualificato l'autoasserzione di identità fornita dall'utente ha il valore di un'autenticazione forte. Se invece il certificato è rilasciato da una CA non registrata o comunque non nota, l'autoasserzione ha valore praticamente nullo ai fini dell'autenticazione.

4.3.3. Asserzione di attributo

L'asserzione di attributo può essere rilasciata dal Certificatore d'attributo, questi deve essere in grado di associare all'identificazione dell'utente (Asserzione di identità) una serie di attributi di sua pertinenza. Queste informazioni costituiscono il contenuto del Certificato di attributo sottoscritto dal Certificatore. Saranno considerati validi i soli attributi dell'Asserzione (di attributo) che compaiono anche nell' Asserzione di Certificatore. Questa Asserzione viene rilasciata dal CDC al termine dell'iter di accettazione e verifica della richiesta di adesione.

La scadenza di una asserzione di attributo può variare, per motivi di sicurezza è bene che non superi le 24 o 48 ore, a meno che non debba venir utilizzata in procedimenti che hanno una vita temporale maggiore. Il Certificatore stabilirà nei vari casi il limite massimo di validità temporale

4.3.4. Asserzione di autorizzazione

L'asserzione di autorizzazione viene rilasciata a fronte di una richiesta d'accesso ad un servizio. Viene rilasciata dal Certificatore di Autorizzazione dopo aver verificato le politiche di accesso al servizio nei confronti di tutte le Asserzioni presenti nel Portafoglio delle Asserzioni al momento della richiesta.

Questa Asserzione viene rilasciata dal CDC al termine dell'iter di accettazione e verifica della richiesta di adesione.

I vincoli di validità temporale per un'asserzione di autorizzazione non sono in genere critici. Una stessa autorizzazione può essere riutilizzata anche più volte se i parametri d'accesso al servizio lo consentono.

5. PROCEDURE

5.1. Procedura di qualificazione dei soggetti erogatori/fruitori di servizi applicativi:

Soggetto della Comunità e DSA sono equivalenti, nel senso che esiste una corrispondenza biunivoca tra i due. Nel caso dei soggetti erogatori è implicito che questi possano operare anche come erogatori.

I soggetti, per registrarsi presentano la documentazione relativa al proprio DSA, tra cui:

- **Identificazione** del soggetto
  - la Denominazione
  - il Codice Identificativo. Per le Pubbliche Amministrazioni il codice identificativo dovrà corrispondere al codice assegnato per l'iscrizione al registro SICA secondario. Questo al fine di garantire l'univocità del codice assegnato.
- l'**Organizzazione** del DSA
  - la funzione e il responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni, in particolare per l'accreditamento ed autenticazione degli utenti;
  - le funzioni ed i responsabili del DSA, sotto il profilo giuridico dei servizi applicativi erogati da un determinato settore o area (Popolazione, tributi, contabilità, personale, ecc.) del DSA, nonché della registrazione degli utenti in carico al medesimo settore o area, compresa l'attribuzione del ruolo;
  - la funzione responsabile dell'informativa, nonché dell'assistenza e della risoluzione di eventuali malfunzionamenti (laddove a fattor comune per l'intero DSA)
- le **Regole Operative** del DSA
  - le modalità di segnalazione problemi/richieste di informazioni sull'intero DSA
  - gli indirizzi della Porta di Dominio del DSA
  - l'indirizzo del Registro su cui sono pubblicate le informazioni sui servizi applicativi erogati
  - le specifiche di Sicurezza del DSA

5.1.1.Procedura di qualificazione/revoca dei soggetti pubblici

Di norma sono registrate le amministrazioni con un DSA ed una Porta di Dominio (a livello funzionale) per ciascuna.

La procedura si attiva inviando al CDC una richiesta di accreditamento. Il documento, cartaceo o elettronico dovrà essere sottoscritto dal responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni.

5.1.2. Procedura di qualificazione/revoca dei soggetti privati

La procedura si attiva inviando al CDC una richiesta di accreditamento/revoca. Il documento, cartaceo o elettronico dovrà essere sottoscritto dal responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni.

Il CDC verificherà l'ammissibilità della richiesta, valutando se il soggetto opera per finalità pubblica o ha interazioni sistematiche e rilevanti con le PA.

5.1.3. Verifica e qualificazione del Dominio

Per la qualificazione del Dominio di un DSA è necessario fornire al CDC un **Certificato X509** con le seguenti caratteristiche:

- il certificato deve essere qualificato ed in corso di validità
- il certificato deve essere associato al responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni, in particolare per l'accreditamento ed autenticazione degli utenti;
- essendo il certificato utilizzato da una procedura automatica di sottoscrizione, secondo la normativa [linee guida CNS 18-5-2004 cap. 10.2], non può essere utilizzato per altre operazioni di firma.
- Per la firma è consentito l'uso dei dispositivi di firma denominati HSM (Hardware Security Module)

5.2. Procedura di qualificazione dei soggetti fruitori di servizi applicativi che operano attraverso il DSA di un altro soggetto.

Ribadito che soggetto e DSA sono equivalenti, nel senso che esiste una corrispondenza biunivoca tra i due, i soggetti solo fruitori che non hanno un proprio DSA sono quelli che operano attraverso il DSA di un altro soggetto (es.: un Front-End applicativo).

I soggetti per registrarsi presentano la documentazione relativa al proprio DSA, tra cui:

- **Identificazione** del soggetto
  - la Denominazione
  - il Codice Identificativo. Per le Pubbliche Amministrazioni il codice identificativo dovrà corrispondere al codice assegnato per l'iscrizione al registro SICA. Questo al fine di garantire l'univocità del codice assegnato.
- l'**Organizzazione** del DSA

- la funzione e il responsabile del DSA, sotto il profilo giuridico dei livelli di qualità e sicurezza garantiti nei processi interni, in particolare per l'accreditamento ed autenticazione degli utenti;
- le funzioni ed i responsabili del DSA, sotto il profilo giuridico della registrazione degli utenti in carico al medesimo settore o area, compresa l'attribuzione del ruolo;
- la funzione responsabile dell'informativa, nonché dell'assistenza e della risoluzione di eventuali malfunzionamenti (laddove a fattor comune per l'intero DSA)

5.2.1. *Procedura di qualificazione/revoca dei soggetti pubblici*

La procedura si attiva inviando al CDC una richiesta di accreditamento/revoca. Il documento, cartaceo o elettronico dovrà essere sottoscritto dal responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni.

5.2.2. *Procedura di qualificazione/revoca dei soggetti privati*

La procedura si attiva inviando al CDC una richiesta di accreditamento/revoca. Il documento, cartaceo o elettronico dovrà essere sottoscritto dal responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni.

Il CDC verificherà l'ammissibilità della richiesta di accreditamento, valutando se il soggetto opera per finalità pubblica o ha interazioni sistematiche e rilevanti con le PA.

5.3. Procedura di qualificazione dei soggetti certificatori

Il Certificatore è un particolare tipo di soggetto al quale non deve necessariamente corrispondere un DSA.

I soggetti, per registrarsi, presentano la documentazione relativa al proprio DSA, tra cui:

- **Identificazione** del soggetto
  - la Denominazione
  - il Codice Identificativo. Per le Pubbliche Amministrazioni il codice identificativo dovrà corrispondere al codice assegnato per l'iscrizione al registro SICA. Questo al fine di garantire l'univocità del codice assegnato.
- l'**Organizzazione** del Certificatore
  - la funzione e il responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni;
  - la funzione responsabile dell'informativa, nonché dell'assistenza e della risoluzione di eventuali malfunzionamenti
- le **Regole Operative** del Certificatore
  - le modalità di segnalazione problemi/richieste di informazioni sul Certificatore

- il provider dei servizi SICA utilizzati
- gli indirizzi dei Sistemi di :
  - Certificazione dell'Identità;
  - Certificazione degli attributi;
  - Certificazione delle politiche di accesso;
- le specifiche di Sicurezza del Certificatore

5.3.1. *Procedura di qualificazione/revoca dei soggetti certificatori*

La procedura può essere attivata dallo stesso CDC.

5.3.2. *Verifica e qualificazione dei sistemi di certificazione*

Per la qualificazione dei sistemi di certificazione è necessario rendere disponibili al CDC un **Certificato X509** con le seguenti caratteristiche:

- il certificato deve essere qualificato ed in corso di validità
- il certificato deve essere associato al responsabile del DSA, sotto il profilo giuridico dei servizi applicativi complessivamente erogati e dei livelli di qualità e sicurezza garantiti nei processi interni;
- essendo il certificato utilizzato da una procedura automatica di sottoscrizione, secondo la normativa [linee guida CNS 18-5-2004 cap. 10.2], non può essere utilizzato per altre operazioni di firma.
- Per la firma è consentito l'uso dei dispositivi di firma denominati HSM (Hardware Security Module)