La Consultazione Certificata è uno strumento che consente la consultazione dei partecipanti ad un processo partecipativo in merito ad uno o più quesiti proposti nel rispetto di alcuni requisiti volti ad aumentare il grado di attendibilità delle risposte fornite.



Una consultazione può essere composta da un numero variabile di quesiti (anche uno solo), senza alcun limite prefissato, appartenenti alle seguenti tipologie, in relazione alle modalità con cui è possibile esprimere la risposta.

- **Selezione singola**: i partecipanti possono scegliere una sola delle alternative proposte;
- **Selezione multipla**: i partecipanti possono scegliere un numero di alternative compreso tra un minimo e un massimo;
- **Cumulativo**: ogni partecipante ha a disposizione un numero determinato di "punti" che può distribuire a sua discrezione tra le alternative proposte;
- **Ordinamento**: il partecipante ordina le N alternative secondo un proprio criterio di preferenza. Sulla base di questo ordinamento le alternative ottengono un punteggio pari a N punti per la prima, N-1 per la seconda, e così via;
- **Testo libero**: il partecipante può inserire un testo a piacere di lunghezza massima prefissata.

E' possibile definire per ciascuno di essi se richiedere obbligatoriamente una risposta o lasciare la possibilità di non rispondere.
La possibiltà di impostare una data di inizio e fine determina l'intervallo di tempo in cui lasciare aperta la consultazione. Al di fuori di questo intervallo di date è possibile comunque visualizzare i quesiti, ma non inviare le risposte.

I requisiti volti ad aumentare il grado di attendibilità della consultazione sono i seguenti:

- **anonimato**: sulla base delle risposte fornite non è possibile risalire all'identità dell'autore;
- **univocità** delle risposte inviate: è possibile rispondere solo una volta ai quesiti proposti nella consultazione;
- **non alterabilità** delle risposte inviate: le risposte inviate non possono essere modificate;
- **non falsificabilità** della consultazione: non è possibile aggiungere risposte per conto di potenziali partecipanti.

Il sistema di gestione dei permessi openDCN assicura inoltre che possano partecipare alla consultazione esclusivamente gli utenti in possesso del relativo permesso.

Dati questi particolari requisiti da soddisfare, tale strumento è stato implementato tramite moduli

esterni in grado di dialogare con il sistema principale. In particolare sono stati realizzati:

- un Client dedicato alla visualizzazione dei quesiti e all'invio delle relative risposte, realizzato tramite un'applet Java;
- una terna di server denominati **Registrar**, **Forwarder** e **Collector**, anch'essi realizzati in Java, dedicati alla gestione dei dati della consultazione (autenticazione, memorizzazione, cifratura, raccolta e conteggio dei risultati). Tali server possono risiedere su macchine differenti.

Questa architettura, implementata con l'obiettivo di soddisfare i requisiti suddetti, presenta alcune criticità di cui occorre esser consapevoli al momento dell'utilizzo dello strumento.
In particolare occorre tener conto che:

- Registrar può generare coppie quasi-valide simulando le credenziali private di un Client conosciuto. Questa eventualità può essere scoperta da un conflitto al momento della consegna delle risposte al Forwarder.
- Registrar e Collector possono mettere insieme le informazioni e ricostruire le risposte dei Client.

E' importante sottolineare come quest'ultimo punto non costituisca una criticità dal punto di vista tecnico, ma solo dal punto di vista organizzativo, quindi di cui deve farsi carico l'ente che organizza la consultazione. Il fatto che Registrar e Collector possano mettere insieme le informazioni è subordinato ad un accordo tra i responsabili della gestione di tali server. Un primo passo per ostacolare questo accordo è quindi quello di sfruttare la potenzialità del sistema e far risiedere i due server su due macchine diverse sotto la responsabilità di due entità organizzative diverse. In questo modo l'accordo volto a ricostruire le risposte non si ridurrebbe a mettere insieme le informazioni controllate dai due server, Registrar e Collector, ma dovrebbe coinvolgere le due organizzazioni responsabili della loro gestione, aumentando notevolmente le garanzie nei confronti dei partecipanti.