

Gestione delle credenziali del cittadino in ordine all'integrazione del sistema informatico aggiudicato con i servizi di autenticazione regionali attualmente in essere (Comunità Sistema Piemonte e Torino Facile) ed anche al servizio SPID di prossima attivazione.

Accesso al servizio CUP attraverso le credenziali Cittadini “Sistema Piemonte” e “TorinoFacile”

Per poter consentire l'accesso ai Cittadini che dispongono di credenziali della comunità di Sistema Piemonte e di quella di TorinoFacile, l'aggiudicatario dovrà installare e configurare un Service Provider (SP) compatibile con le specifiche SAML2 (protocollo standard utilizzato a livello nazionale e internazionale per la realizzazione di logiche di autenticazione e federazione di identità).

E' uno standard aperto di cui sul mercato esistono varie implementazioni sia proprietarie sia opensource sviluppate in differenti linguaggi di programmazione; il SP interagirà poi con l'Identity Provider CSI per la verifica effettiva delle credenziali utente.

Per poter consentire l'accesso ad entrambe le comunità sarà necessario che in fase di configurazione dell'SP si configurino i metadata in modo tale da dichiarare la validità reciproca delle credenziali (federazione basata su Trust).

L'architettura di integrazione che si intende realizzare tra i servizi dell'aggiudicatario e i sistemi di autenticazione del CSI Piemonte è la seguente:

- sui sistemi dell'aggiudicatario verrà installato e configurato un Service Provider SAML2 (a cura dell'aggiudicatario stesso)
- il Service Provider si relazionerà con l'Identity Provider di CSI Piemonte riferito alle comunità di utenti SistemaPiemonte e TorinoFacile
- le due componenti (Service ed Identity Provider) saranno configurate in modo da realizzare una federazione di identità
- il servizio erogato dall'aggiudicatario dovrà essere protetto ed esposto per mezzo del Service Provider realizzato
- l'autenticazione dell'utente finale avverrà sull'Identity Provider del CSI Piemonte e verrà restituita al Service Provider l'asserzione di autenticazione e di autorizzazione per consentire successivamente l'accesso protetto al servizio dell'aggiudicatario.

Riconoscimento di credenziali Imputabili

Le normative vigenti stabiliscono che per accedere ai servizi sanitari on line della Regione Piemonte è necessario che l'utilizzatore sia in possesso di credenziali “imputabili”, ovvero rilasciate al richiedente sulla base di riconoscimento certo (de visu) della sua identità da parte di un operatore di sportello.

L'attività di autenticazione, effettuata dall'IDP di CSI Piemonte, indicherà la natura “imputabile” delle credenziali tramite un attributo specifico.

L'aggiudicatario dovrà implementare un meccanismo di verifica di questo attributo al fine di consentire l'accesso alle procedure solo ed esclusivamente a cittadini in possesso di credenziali imputabili.

In fase di implementazione del servizio, l'aggiudicatario dovrà prendere contatti con il CSI Piemonte per i dettagli implementativi.

Single Sign-On (SSO)

I cittadini in possesso di credenziali della comunità di Sistema Piemonte o di TorinoFacile possono sfruttare il meccanismo di Single Sign-On, proprio del protocollo SAML2, per poter accedere ai vari applicativi esposti dal portale su cui verrà pubblicato il servizio (ex. "La mia Salute") inserendo una sola volta le proprie credenziali.

Il SSO, infatti, è garantito per tutti i servizi autenticati dall'Identity Provider del CSI Piemonte e non richiede alcuna configurazione specifica da parte dell'aggiudicatario.

Accesso al servizio CUP attraverso le credenziali della federazione SPID

Con l'istituzione del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese¹ (SPID) le pubbliche amministrazioni potranno consentire l'accesso in rete ai propri servizi, oltre che con lo stesso SPID, solo mediante la carta d'identità elettronica e la carta nazionale dei servizi. La possibilità di accesso con carta d'identità elettronica e carta nazionale dei servizi resta comunque consentito indipendentemente dalle modalità predisposte dalle singole amministrazioni.

Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni.

Le regole di integrazione con il Sistema Pubblico di Identità Digitale, alla data di stesura del presente documento, non sono ancora definitive, ma si baseranno fondamentalmente sullo stesso protocollo (SAML2) e sulle stesse logiche di integrazione descritte nel paragrafo precedente.

E' fatto obbligo all'aggiudicatario di predisporre quanto necessario per adeguare il sistema di accesso ai servizi erogati, come da norma, alle specifiche SPID, non appena queste saranno operative.

Collegamento del Data Center dell'aggiudicatario con il Data Center del CSI Piemonte

Il collegamento avverrà attraverso un «collegamento dedicato» approvvigionato dall'aggiudicatario attraverso un operatore di TLC. Dovrà avere degli SLA di servizio definiti (H24, intervento in 4 ore e ripristino in 8 ore solari) ed una capacità di trasporto e latenza tale da garantire la corretta fruizione del servizio da parte degli attori coinvolti. La stima di queste capacità è a carico dell'aggiudicatario. Per motivi di affidabilità del servizio si richiede che il collegamento (possibilmente in fibra ottica) sia ridondato (doppia via) con doppio apparato di terminazione (router) sia lato CSI che lato DC dell'aggiudicatario.

All'aggiudicatario sarà assegnato uno spazio di indirizzamento RUPAR per consentire l'allineamento dei propri sistemi con i servizi esposti dal CSI (es. Aura, etc..). L'aggiudicatario potrà esporre direttamente i

¹ http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_24_ottobre_2014a.pdf

servizi su questo spazio di indirizzamento fornito o effettuare un *Network Address Translation* (NAT) da propri indirizzi interni allo spazio di indirizzamento RUPAR fornito dal CSI. In quest'ultimo caso l'aggiudicatario dovrà garantire la compatibilità del NAT con il funzionamento delle varie componenti applicative che renderà disponibili.

Le attività di assistenza (diagnosi e troubleshooting sul collegamento e sull'infrastruttura) di primo livello saranno a carico dell'aggiudicatario.