RegioneLombardia

LA GIUNTA

DELIBERAZIONE N° X / 6788 Seduta del 30/06/2017

Presidente **ROBERTO MARONI**

Assessori regionali FABRIZIO SALA *Vice Presidente*
VALENTINA APREA
VIVIANA BECCALOSSI
SIMONA BORDONALI
FRANCESCA BRIANZA
CRISTINA CAPPELLINI
LUCA DEL GOBBO
GIOVANNI FAVA
GIULIO GALLERA
MASSIMO GARAVAGLIA
MAURO PAROLINI
ANTONIO ROSSI
ALESSANDRO SORTE
CLAUDIA TERZI

Con l'assistenza del Segretario Fabrizio De Vecchi

Su proposta dell'Assessore Massimo Garavaglia

Oggetto

SUPPORTO AGLI ENTI LOCALI DELLA LOMBARDIA PER L'ADESIONE AL SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE (SPID)

Il Segretario Generale Antonello Turturiello

Si esprime parere di regolarità amministrativa ai sensi dell'art.4, comma 1, l.r. n.17/2014:

Il Dirigente Oscar Alessandro Sovani

Il Direttore Vicario Ugo Palaoro

Il Direttore Centrale Manuela Giaretta

L'atto si compone di 20 pagine

di cui 15 pagine di allegati

parte integrante

PRESO ATTO:

- che Regione Lombardia, per il tramite della sua società Lombardia Informatica SpA, ha realizzato nel 2007 al fine di dare attuazione all'art. 64 del DLgs n. 82/2005 (Codice dell'Amministrazione Digitale, di seguito "CAD") il servizio per la gestione dell'Identità Digitale denominato Identity Provider del Cittadino (di seguito IdPC) e da allora è stato utilizzato per l'identificazione informatica ai servizi online della Regione e del SIREG e messo gratuitamente a disposizione degli Enti Locali della Lombardia;

- che con la DGR X/5668 del 11/10/2016 "ADESIONE AL SISTEMA PUBBLICO PER L'IDENTITA' DIGITALE (SPID). APPROVAZIONE SCHEMA DI CONVENZIONE TRA REGIONE LOMBARDIA E AGENZIA PER L'ITALIA DIGITALE" si dà atto che l'infrastruttura IdPC è stata adeguata alle nuove disposizioni di legge inerenti l'adozione di SPID in tema di autenticazione e accesso sicuro ai servizi digitali;

VISTI:

- le modifiche introdotte con decreto-legge 21 giugno 2013 all'art. 64 del CAD che prevede "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (di seguito "SPID");
- l'articolo 64, comma 2-quater, del CAD che recita "il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con un decreto del Presidente del Consiglio dei Ministri";
- il DPCM 24 ottobre 2014, recante "Definizione delle caratteristiche del sistema SPID, nonché dei tempi e delle modalità di adozione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) da parte delle pubbliche amministrazioni e delle imprese", pubblicato sulla Gazzetta Ufficiale n. 285 del 9/12/2014;
- l'art. 14, comma 1, del DPCM 24 ottobre 2014 ai sensi del quale le pubbliche amministrazioni che erogano in rete servizi qualificati, direttamente o tramite altro fornitore di servizi, consentono l'identificazione informatica degli utenti attraverso l'uso di SPID;

CONSIDERATO che il Piano Triennale per l'Informatica nella Pubblica

Amministrazione 2017-2019, approvato in data 31 maggio 2017 dal Presidente del Consiglio dei Ministri, stabilisce che tutte Le Pubbliche amministrazioni devono implementare SPID per tutti i servizi digitali che richiedono autenticazione, sia quelli già esistenti che quelli di nuova attivazione, entro marzo 2018;

DATO ATTO che, ai sensi dell'art. 64 comma 1 del CAD, la Carta Nazionale dei Servizi (CNS) costituisce uno degli strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica e che il servizio IdPC di Regione Lombardia continua a svolgere la funzione di accesso con CNS;

RICHIAMATA l'Agenda Digitale Lombarda 2014-2018, approvata con DGR n. X/1887 del 30-5-2014, che prevede nell'area d'intervento "Reti e servizi digitali interoperabili" l'obiettivo 2.2 "Digitalizzazione dei processi amministrativi e diffusione di servizi digitali della PA interoperabili";

RICHIAMATA l'Agenda Lombardia Semplice, approvata con DGR n. X/2557 del 31/10/2014, che prevede tra gli "INTERVENTI di semplificazione per CITTADINI e TERZO SETTORE" la "estensione del sistema di identità regionale (successivamente integrabile con le iniziative nazionali) per l'accesso unificato ai servizi di Regione Lombardia e delle P.A. locali che vogliono erogare servizi in ottica federata";

RITENUTO OPPORTUNO confermare l'infrastruttura IdPC come piattaforma di riferimento per l'autenticazione e l'accesso sicuro ai servizi digitali ai sensi dell'art. 64 del CAD e come strumento per facilitare l'adesione e l'utilizzo di SPID;

VISTO il Protocollo D'intesa tra Regione Lombardia, ANCI e ANCI Lombardia per l'attuazione di iniziative di innovazione e digitalizzazione dei Comuni lombardi, approvato con la DGR n. X/3039 del 23/01/2015;

VISTA La Legge Regionale n. 20 del 8 luglio 2015, che all'art. 6 ha apportato modifiche alla L.R. 7 del 2012, ed in particolare ha introdotto l'art. 52 ter (Interventi per la crescita digitale) che recita: "La Regione fornisce agli enti locali supporto tecnico specialistico per la progettazione e lo sviluppo di interventi di digitalizzazione e per l'attuazione del codice dell'amministrazione digitale"

DATO ATTO che Regione, in continuità con quanto già fatto a partire dal 2007, mette a disposizione del territorio, ed in particolare degli enti locali, la propria piattaforma tecnologica IdPC per l'accesso ai servizi pubblici online e che questa

semplifica e velocizza il processo di adesione a SPID e la conseguente conformità al CAD da parte degli enti locali;

VISTA la D.G.R. n. 6101 del 29.12.2016 che ha approvato il programma pluriennale delle attività di Lombardia informatica, tra le quali è prevista quella relativa ad iniziative per adeguamento al CAD da parte degli enti locali;

VISTO il documento "SPID - Linee Guida per gli Enti Locali" (Allegato A) che indica agli enti locali lombardi le modalità per avvalersi del supporto di Regione Lombardia per l'autenticazione e l'accesso sicuro ai servizi digitali ai sensi dell'art. 64 del CAD e per l'adesione a SPID;

PRECISATO che non ci sono oneri a carico di Regione Lombardia in relazione alla presente delibera;

RICHIAMATA la l.r. 7 luglio 2008, n. 20 "Testo unico delle leggi regionali in materia di organizzazione e personale", nonché i provvedimenti organizzativi della X Legislatura;

A VOTI UNANIMI espressi nelle forme di legge;

DELIBERA

1. di approvare il documento "SPID - Linee Guida per gli Enti Locali" (Allegato A), parte integrante e sostanziale del presente atto;
2. di dare mandato al dirigente della Struttura Semplificazione e Digitalizzazione della Direzione Centrale Programmazione, Finanza e Controllo di gestione, di promuovere e facilitare l'adesione e l'utilizzo di SPID da parte degli Enti Locali e di adottare tutti gli atti connessi e consequenziali al presente provvedimento;
3. di mantenere attivo il servizio per la gestione dell'Identità Digitale, denominato Identity Provider del Cittadino (IdPC), a disposizione degli enti locali lombardi;

4. di pubblicare il presente atto sul Bollettino Ufficiale della Regione Lombardia (BURL).

IL SEGRETARIO

FABRIZIO DE VECCHI

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

ALLEGATO A

AGENDA DIGITALE LOMBARDA

SPID - Linee guida per EELL

Sommario

1 Introduzione

1.1 Scopo e campo di applicazione

Questo documento ha lo scopo di illustrare il supporto offerto da Regione Lombardia e Lombardia Informatica alla migrazione verso il Sistema Pubblico per l'Identità Digitale (di seguito SPID), sia per gli EELL della Regione Lombardia che già utilizzano il servizio IdPC (Identity Provider Cittadini) che per tutti gli altri enti locali che intendono avvalersene.

1.2 Acronimi e definizioni

Le definizioni e gli acronimi utilizzati nel resto del documento sono:

AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
CNS	Carta Nazionale dei Servizi
CRS	Carta Regionale dei Servizi
EELL	Enti Locali
HTTP	Hyper Text Transfer Protocol
IdP	Identity Provider
IdPC	Identity Provider del Cittadino
LISPA	Lombardia Informatica SpA
OTP	One Time Password
RL	Regione Lombardia
SAML	Security Assertion Markup Language
Shibboleth	OpenSource Shibboleth-ServiceProvider (https://shibboleth.net/)
SP	Service Provider
SPID	Sistema Pubblico per l'Identità Digitale
TS-CNS	Tessera Sanitaria – Carta Nazionale dei Servizi
XML	Extensible Markup Language

2 Contesto

Regione Lombardia, dopo aver completato la distribuzione a tutti i cittadini della CRS (conforme allo standard nazionale CNS – Carta Nazionale dei Servizi), nel corso del 2007 ha sviluppato e reso disponibile a tutti gli EELL della regione un servizio per la gestione dell'identificazione informatica denominato IdPC – Identity Provider del Cittadino.

L'IdPC, basato sullo standard più diffuso e aperto (SAML), permette alle pubbliche amministrazioni di adempiere alle norme nazionali (art. 64 del Codice dell'Amministrazione Digitale) nella gestione dell'accesso sicuro da parte dei cittadini a servizi qualificati che hanno la necessità di assicurarsi dell'identità dell'utente, tramite l'uso della CNS.

L'IdPC è stato utilizzato, a partire dal 2009, come unico servizio per identificare cittadini e imprese che accedono ai servizi di Regione Lombardia, affiancando alla modalità di autenticazione "forte" con la CNS una modalità di accesso "basic" (username e password) ed una "intermedia" (usr/pwd e OTP).

I servizi di Regione Lombardia che si avvalgono di IdPC sono oltre 100, mentre gli EELL che utilizzano IdPC direttamente o tramite portali "aggregati" sono oltre 500.

L'utilizzo di IdPC è cresciuto nel tempo a causa dell'aumento dei servizi integrati e per l'aumento dell'utilizzo dei servizi online da parte degli utenti, arrivando a superare 1.300.000 accessi al mese.

L'architettura di IdPC è ridondata e scalabile (3 FrontEnd, 3 BackEnd, 4 LDAP server) ed è stata misurata, tramite test di carico, la capacità di reggere fino a 100.000 transazioni/ora, ovvero quattordici volte l'attuale picco di 7.000 transazioni/ora, senza aumentare le risorse hardware.

È attiva un'istanza di Disaster Recovery presso il secondo DataCenter di Lombardia Informatica ed è in programma la realizzazione di una soluzione di Business Continuity.

Nel corso del 2015 IdPC ha garantito una disponibilità del 99,996%, ovvero un solo blocco di 20 minuti, mentre nel 2016 IdPC ha garantito una disponibilità del 99,982%, ovvero un solo blocco di 90 minuti.

3 L'introduzione di SPID

Nella normativa italiana è stato introdotto un sistema, denominato **SPID** – **S**istema **P**ubblico di **I**dentità **D**igitale che si pone l'obiettivo di rendere possibile l'accesso a tutti i servizi online della PA e dei privati con un'unica identità digitale. SPID rappresenta quindi un pilastro fondamentale della strategia digitale nazionale. L'art. 64 del CAD è stato quindi così modificato:

Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. La **carta d'identità elettronica** e la **carta nazionale dei servizi** costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, Le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi **solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID**. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

2-ter Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, 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, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.

2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

Il sistema SPID definisce i seguenti attori:

- il Service Provider (nel seguito SP), che espone online servizi applicativi ;

- l'Identity Provider (nel seguito IdP), che rilascia credenziali SPID e governa il processo di autenticazione ;
- il cittadino, che accede ai servizi online esposti dai SP utilizzando una credenziale rilasciata da un IdP.

Il primo provvedimento di attuazione previsto dall'articolo 64, comma 2-sexies del D.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) è il decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014.

Il 28 luglio 2015, con la Determinazione n. 44/2015, sono stati emanati i quattro regolamenti previsti dall'articolo 4, commi 2, 3 e 4, del suddetto DPCM 24 ottobre 2014:

- Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2)
- Regolamento recante le regole tecniche (articolo 4, comma 2)
- Regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale (articolo 1, comma 1, lettera l)
- Regolamento recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale (articolo 4, comma 4)

Il 19 dicembre 2015 AgID, con un comunicato stampa, ha annunciato di aver accreditato i primi tre Identity Provider SPID: Infocert S.p.A., Telecom Italia Trust Technologies srl, Poste Italiane S.p.A.

Con la DETERMINAZIONE N. 32/2016 del 16 febbraio 2016 del Direttore Generale di AgID è stato emanato lo schema di convenzione per l'adesione al Sistema Pubblico per la gestione dell'Identità digitale (SPID) dei Gestori accreditati ai sensi dell'art.4 del DPCM 24 ottobre 2014.

Con la DETERMINAZIONE N. 40/2016 del 23 febbraio 2016 del Direttore Generale di AgID è stato emanato lo schema di convenzione tra l'Agenzia per l'Italia Digitale e le pubbliche amministrazioni in qualità di fornitori di servizi in materia di Sistema Pubblico per la gestione dell'identità digitale di cittadini e imprese

Il 15 marzo 2016 i primi tre Identity Provider hanno iniziato ad operare ed a rilasciare le credenziali SPID e sono stati resi fruibili online i primi due SP (INPS e alcuni servizi di Regione Toscana). Il 14-9-2016 la società Sielte SpA ha firmato la convenzione ed ha cominciato ad operare come IdP. Il 18-1-2017 la società Aruba Pec S.p.A. ha firmato la convenzione ed ha iniziato ad operare.

Nel "Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019" approvato dal Presidente del Consiglio dei Ministri il 31.05.2017, è stabilito che tutte le Pubbliche amministrazioni devono implementare SPID in tutti i servizi digitali che richiedono autenticazione, sia quelli già esistenti che quelli di nuova attivazione, entro marzo 2018.

È previsto che gli IdP possano rilasciare credenziali di tre differenti livelli:

- **Livello L1** – permette l'autenticazione con username e password
- **Livello L2** – permette l'autenticazione con username, password e la generazione di un codice temporaneo inviato all'utente
- **Livello L3** – permette l'autenticazione attraverso l'utilizzo di un "dispositivo sicuro"

Ad oggi, gli IdP accreditati rilasciano credenziali di livello L1 ed L2.

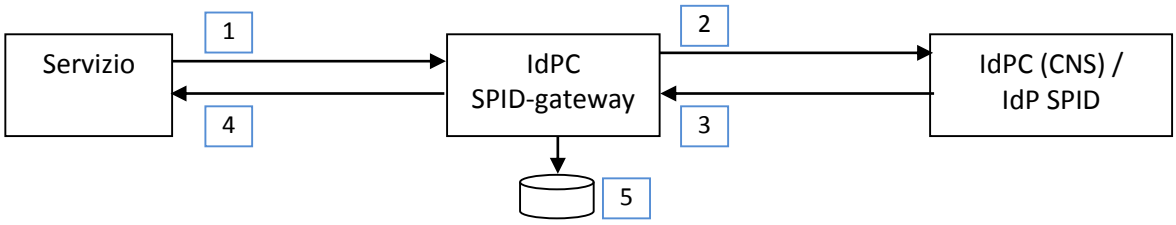
4 Gli adeguamenti a SPID di Regione Lombardia

Lombardia Informatica, a partire dall'emanazione delle Regole Tecniche, ha provveduto a sviluppare e testare l'integrazione con gli Identity Provider SPID.

Allo scopo di facilitare l'integrazione a SPID dei numerosi SP di RL ed EELL, LISPA ha realizzato un componente "**SPID gateway**", collocato logicamente nel perimetro di IdPC, con le seguenti caratteristiche:

- lato SP, viene integrato come l'unico Identity Provider della federazione, quindi accetta richieste di autenticazione e rilascia asserzioni di identità, con protocollo SAML 2.0 e rispettando le interfacce odierne (documentate in SIAU#76) ;
- consente all'utente la selezione della modalità di autenticazione preferita: CNS oppure SPID, in questo caso presentando in modo paritetico i diversi IdP disponibili, in conformità al Regolamento sulle modalità attuative di SPID;
- verso gli IdP si presenta come un SP, quindi invia richieste di autenticazione e consuma asserzioni di identità in accordo alle Regole Tecniche definite da AgID.

La soluzione adottata è descritta sinteticamente di seguito:



Funzionamento di IdPC "SPID gateway"-:

1. Il servizio chiede l'autenticazione a IdPC
2. IdPC "SPID gateway"produce la richiesta d'autenticazione per l'IdP SPID presentandosi come SP
3. l'IdP SPID risponde con l'asserzione di identità SPID
4. IdPC "SPID gateway", ottenuta l'asserzione, la "converte" nella forma RL/LI e la firma come propria trasferendola poi al servizio
5. l'onere di legge del logging formale da parte del SP viene assolto da IdPC, memorizzando tutti e quattro i messaggi

Il componente IdPC "SPID gateway" è stato incluso nella release 9.1 di IdPC in produzione dal 21-12-2015.

IdPC continua ad erogare in totale autonomia l'autenticazione CNS, basic (usr/pwd) e OTP (gli ultimi due solo per i servizi di Regione Lombardia).

Il componente SPID-gateway è conforme alle nuove regole introdotte con l'Avviso 5 e l'Avviso 6.

Nota Bene: I meccanismi di SSO e Single Logout definiti nell'Avviso 3 non sono implementati, in quanto applicabili unicamente a servizi che si avvalgono i credenziali di Livello L1, al momento non in programma da parte di regione Lombardia.

Per una definizione omogenea dei Livelli di sicurezza si faccia riferimento all'Avviso 4.

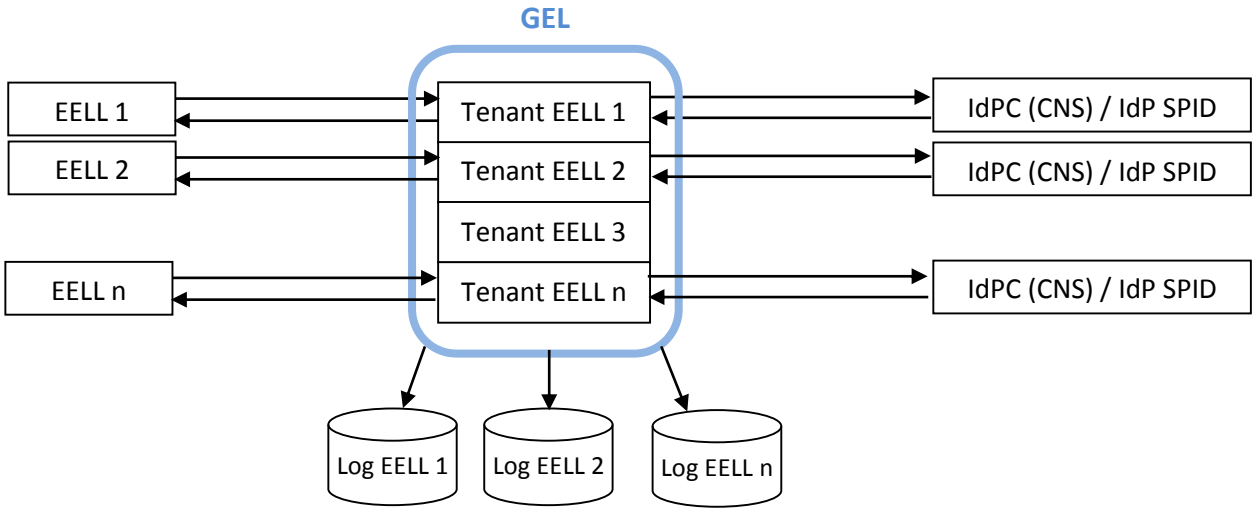
5 Il servizio GEL (Gateway Enti Locali)

Al fine di supportare l'adesione a SPID degli EELL della Regione Lombardia è stato realizzato un servizio, denominato GEL (Gateway Enti Locali), che è messo a disposizione gratuitamente in modalità SaaS (Software as a Service) presso il Datacenter di Regione Lombardia sito in via Taramelli 26 a Milano.

Il servizio GEL è progettato in architettura "multi-tenant" ovvero in modo che sia possibile creare istanze separate per ogni singolo Ente Locale.

Ogni Ente Locale che intenda avvalersi del servizio GEL sarà quindi autonomo nella possibilità di configurare la propria istanza avvalendosi comunque delle componenti di base comune a tutte le istanze e potendo contare sull'impegno di Regione Lombardia e Lombardia informatica ad adeguare il servizio GEL ad ogni modifica delle regole tecniche emanate da AgID.

La soluzione adottata è descritta sinteticamente di seguito:



Il servizio GEL metterà a disposizione degli enti aderenti una console di gestione con la quale potranno essere svolte tutte le attività di configurazione necessarie. Tramite la stessa console ogni ente potrà prelevare il proprio LOG, previsto dal regolamento attuativo di SPID, per conservarlo attraverso i propri processi di conservazione.

Il servizio GEL è utilizzabile sia dagli enti che hanno già integrato il servizio IdPC, sia da chi non l'ha mai utilizzato ed intende utilizzarlo da ora per adeguarsi alla necessità di identificazione informatica con CNS e SPID prevista dal CAD.

Gli enti che hanno già integrato IdPC tramite il componente Shibboleth, come descritto nel documento "SIAU#97 – Integrazione a IdPC tramite Shibboleth" (rif. #SIAU97), potranno integrare il servizio GEL con pochissimi interventi, essenzialmente di tipo sistemistico.

Gli altri enti dovranno adeguare i servizi introducendo l'integrazione tramite Shibboleth con le configurazioni dettagliate nei documenti di specifiche tecniche.

5.1 Livelli di servizio

Regione Lombardia e Lombardia informatica si impegnano a garantire l'operatività del servizio h24x365gg, con un livello di **disponibilità del 99,8%**, escluse le finestre di manutenzione.

La manutenzione ordinaria, necessaria ad esempio alla installazione di patch di sicurezza o di nuove release è svolta di norma in orario serale (tra le 19 e le 22) e non comporta fermi del servizio superiori ai 5 minuti.

In caso di manutenzione straordinaria che richieda un fermo significativo del servizio questa verrà svolta nel fine settimana e sarà annunciata con almeno 10 giorni di anticipo.

5.2 Assistenza

Sarà disponibile un servizio di assistenza per gli Enti che utilizzeranno il servizio GEL, previsto su 6gg lavorativi, nelle fasce orarie 8:00-18:00 da lunedì a venerdì e nelle fasce orarie 8:00-13:00 il sabato.

5.3 Referente tecnico dell'Ente

L'Ente aderente dovrà comunicare a Lombardia Informatica il nominativo del referente tecnico, con le informazioni di contatto (email, telefono cellulare), nonché l'elenco delle software house che realizzeranno l'integrazione con il GEL ed i loro referenti tecnici.

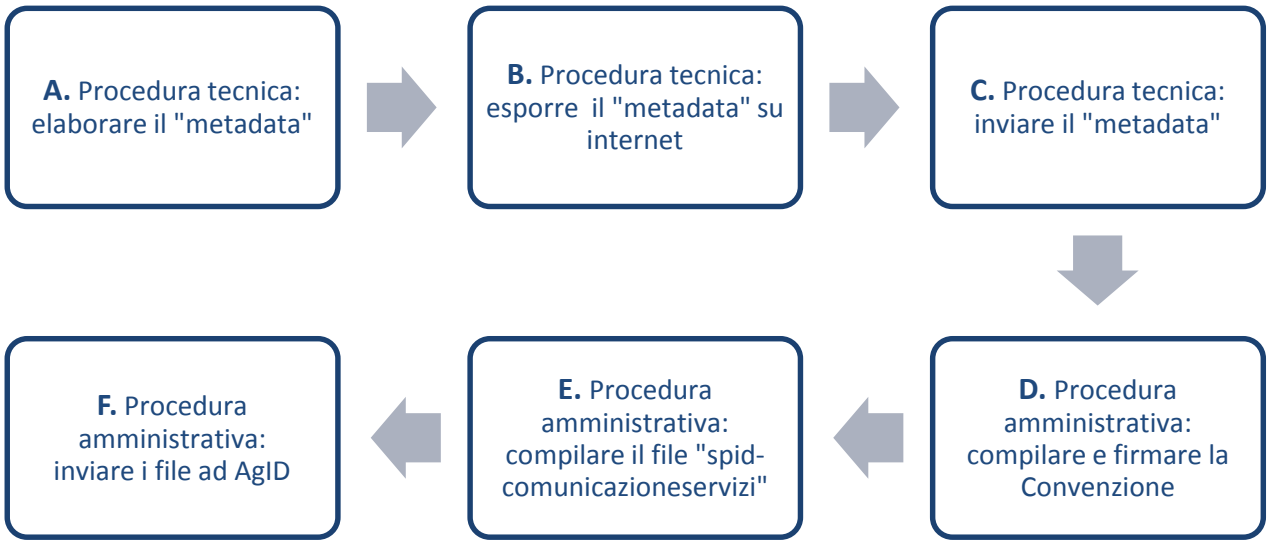
6 Il percorso di adesione a SPID

Di seguito è descritto il percorso di adesione a SPID per chi sceglie di utilizzare il servizio GEL. Il processo di adesione previsto da AgID verrà esploso in seguito.

1. Il primo passo consigliato è la presa visione da parte dell'Ente e/o delle proprie software house delle presenti Linee Guida e della documentazione tecnica riguardante l'integrazione dei servizi dell'Ente con il GEL, al fine di valutare compiutamente il servizio offerto e le implicazioni tecniche;
2. Il secondo passo è l'espressione dell'adesione dell'Ente al servizio GEL, tramite l'invio dell'atto di adesione di cui è fornito uno schema tipo in allegato alle presenti Linee Guida;
3. Il terzo passo è rappresentato dalle attività di sviluppo e/o configurazione necessarie alla integrazione dei servizi dell'Ente con il GEL, secondo le indicazioni contenute nei documenti di integrazione al GEL;
4. congiuntamente agli sviluppi sarà possibile eseguire i test, con una istanza del GEL specificatamente dedicata alle attività di test e che è configurata per interfacciarsi con le piattaforme di test messe a disposizione dagli IdP SPID;
5. configurazione del proprio tenant del GEL;
6. Procedura di adesione prevista da AgiD, vedi paragrafo successivo;
7. Ottenuta la conferma da AgID dell'avvenuta registrazione del proprio "metadata" da parte degli IdP, sarà possibile configurare i servizi in produzione ed iniziare ad utilizzare SPID.

6.1 Processo di adesione formale a SPID

Di seguito è descritto il percorso di adesione a SPID previsto da AgID e descritto sul sito www.spid.gov.it, in particolare nella sezione https://spid.gov.it/sei-una-pubblica-amministrazione



A. Il primo passo richiesto è l'elaborazione del file "metadata". Si tratta di una attività discretamente complessa e critica in quanto, se il file non è completo e corretto non passerebbe le verifiche di AgID. Per questa attività sarà dato supporto agli enti fornendo un file "metadata" standardizzato, una chiave di firma prodotta dalla Certification Autority di LIspa ma di esclusiva proprietà dell'ente e supportandoli nella firma XML dello stesso;

B. per poter permettere ad AgID di verificare il file "metadata" è necessario che lo stesso sia esposto su Internet. Allo scopo sarà messo a disposizione degli enti una funzione del pannello di gestione per caricare ed esporre il file "metadata";

C. una volta verificato che il file "metadata" sia scaricabile da Internet sarà necessario inviare una comunicazione ad AgID, utilizzando il sistema di supporto per le pubbliche amministrazioni (http://helpdesk.spid.gov.it/) selezionando la categoria "Comunicazione metadata";

D. Al fine di formalizzare l'adesione a SPID sarà necessario compilare la Convenzione, disponibile qui: http://www.agid.gov.it/sites/default/files/circolari/spid_schema_convenzione_sp_pa.doc, indicando in particolare: l'URL del sito dell'ente nel quale verranno elencati i servizi accessibili con SPID, il referente dell'ente per la Convenzione e l'indirizzo PEC.; una volta compilata andrà firmata digitalmente dal legale rappresentante dell'ente;

E. Compilare il file per la comunicazione dei servizi, disponibile qui http://www.spid.gov.it/assets/res/SPID-ComunicazioneServizi.ods ;

F. Inviare la Convenzione firmata ed il file dei servizi ad AgID, tramite PEC.

6.2 Principi generali sull'integrazione a SPID tramite GEL

Per fruire del servizio GEL è necessario che il SP si integri al GEL attraverso la componente Shibboleth, configurata per lavorare con SAML 2.0.

Per le informazioni generali in merito alla integrazione tramite Shibboleth, che permette l'integrazione di servizi applicativi realizzati con qualunque tecnologia (Java, .NET, PHP, Python, etc), si faccia riferimento al documento SIAU#97 – Integrazione a IdPC tramite Shibboleth (rif. SIAU#97).

La componente Shibboleth dovrà essere equipaggiata di un file (denominato *metadata*) necessario per indirizzare le richieste di autenticazione verso il corretto endpoint di GEL, e di chiavi crittografiche per la firma delle richieste di autenticazione. Le istruzioni su come configurare i metadata e le chiavi crittografiche vengono fornite da LISPA.

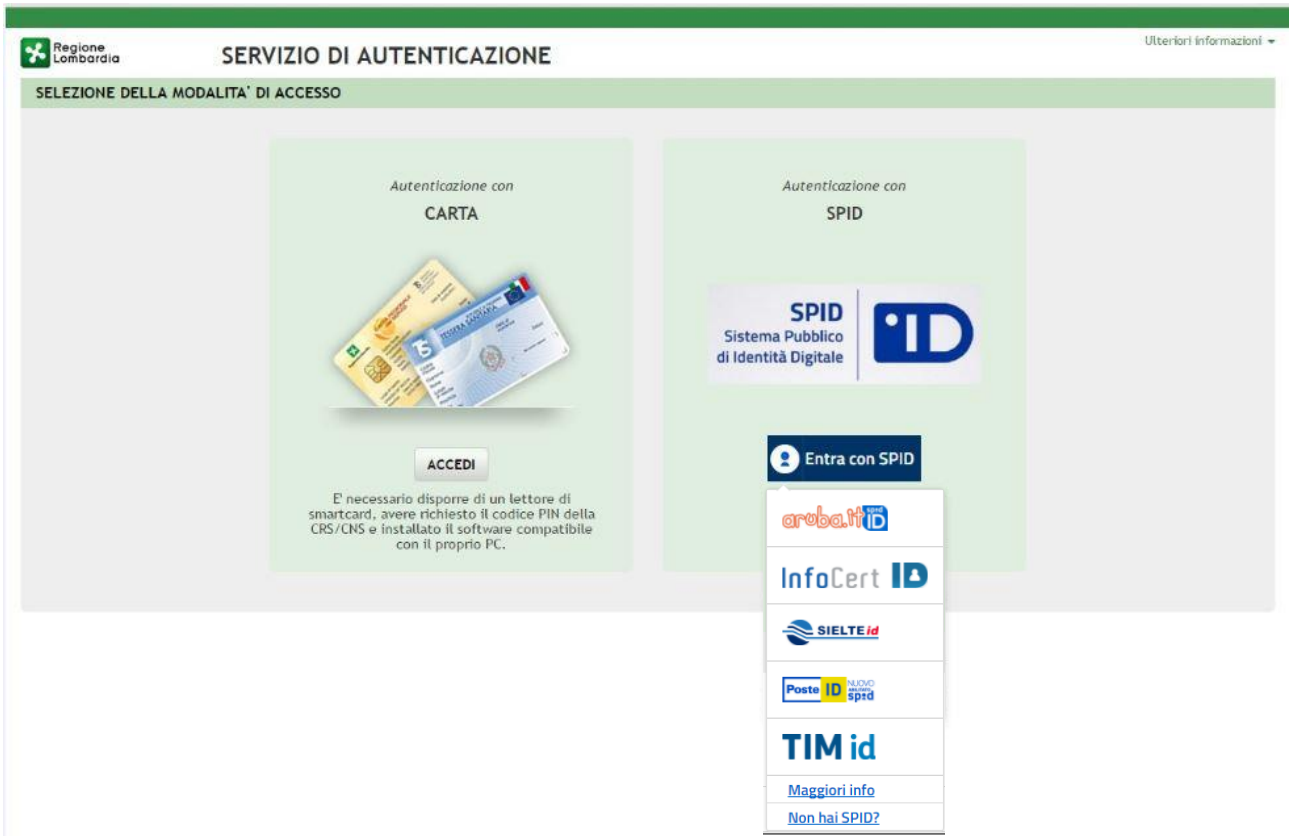
Il SP dovrà fornire un file di configurazione ("regola di accesso al servizio") che verrà censito nella base dati di GEL.

L'esperienza utente attesa è la seguente:

1. Il cittadino che, nell'ambito del SP, intende accedere ad un'area protetta da autenticazione, seleziona un tasto che inizia il processo di autenticazione ;
2. Il browser viene indirizzato ad una landing page esposta da GEL che illustra le varie modalità di accesso – queste modalità devono essere scelte dal SP in fase di integrazione, nell'esempio in figura viene mostrata la scelta tra CNS e SPID:

Se l'utente sceglie CARTA, viene re-indirizzato sul sistema IdPC così come avviene già oggi per i servizi che ne fanno uso, con le operazioni conseguenti (scelta del certificato, richiesta PIN, ecc.).

Se l'utente sceglie "SPID" il sistema propone una selezione tra i diversi IdP disponibili (come da indicazioni AgID, l'ordine di elencazione degli IdP è casuale e differente ad ogni sessione):



1. l'utente sceglie uno degli IdP SPID, il browser viene indirizzato sulle pagine dell'IdP (quindi al di fuori del perimetro RL-LISPA) dove il cittadino effettua l'autenticazione in accordo alle singole politiche adottate dall'IdP ;
2. tutta la comunicazione tra GEL e IdP SPID avviene in accordo alle specifiche AgID, sia durante la richiesta di autenticazione sia durante la ricezione della asserzione di identità;
3. l'asserzione ricevuta da SPID viene "tradotta" da GEL in modo da valorizzare gli stessi attributi oggi conosciuti dalle applicazioni e descritti nel documento SIAU#76;
4. il SP ha accesso alle informazioni di identità utente tramite Shibboleth e l'utente accede al servizio.

Si noti che:

- gli obblighi di logging formale delle autenticazioni in carico ai SP e definiti nei regolamenti di AgID sono assolti centralmente dal servizio GEL, ma è compito degli enti recuperare periodicamente i file di log e conservarli; il file di log sarà cifrato, come previsto dai regolamenti di AgID, e decifrabile unicamente dall'ente tramite una chiave privata;
- a fronte dell'accreditamento di nuovi IdP, LISPA adeguerà la configurazione del servizio GEL e gli utenti potranno immediatamente richiedere autenticazioni ai nuovi IdP, senza alcun impatto sui SP;
- le interfacce grafiche esposte dal servizio GEL sono *responsive*, quindi in grado di adeguarsi alle esigenze di visualizzazione dei dispositivi mobile. LISPA non ha alcuna possibilità di definire o modificare le interfacce grafiche esposte dagli IdP SPID.

7 Riferimenti

[1] Pagina Web contenente la documentazione su IdPC
http://www.crs.regione.lombardia.it/ds/Satellite?c=Page&childpagename=CRS%2FCRSLayout&cid=1213352757673&p=1213352757673&pagename=CRSWrapper

[2] SIAU#76 - Identity Provider Cittadini Regione Lombardia
http://www.crs.regione.lombardia.it/ds/ccurl/690/209/CRS-ISAU-SIAU_76.pdf

[3] SIAU#97 – Integrazione a IdPC tramite Shibboleth
http://www.crs.regione.lombardia.it/ds/ccurl/881/707/CRS-ISAU-SIAU_97.pdf

[4] Allegati a SIAU#97
http://www.crs.regione.lombardia.it/ds/ccurl/308/418/Esempi_Integrazione_IdPC_Shibboleth.zip
http://www.crs.regione.lombardia.it/ds/ccurl/916/702/componente_aggiuntivo_shibboleth.zip

[5] Pagina SPID su sito AgID
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

[6] Sito dedicato su SPID
http://www.spid.gov.it/

[7] CAD - Codice dell'Amministrazione Digitale
http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig=

[8] DPCM 24 ottobre 2014
http://www.gazzettaufficiale.it/eli/id/2014/12/09/14A09376/sg

[9] Regolamento SPID: modalità attuative (versione 2.0 del 22 luglio 2016)
http://www.agid.gov.it/sites/default/files/circolari/regolamento_modalita_attuative_spid_2.0.pdf

[10] Modello Convenzione SPID tra AgID e Pubbliche Amministrazioni
http://www.agid.gov.it/sites/default/files/circolari/spid_schema_convenzione_sp_pa.doc

Appendice: Atto di adesione

L'Ente che vuole utilizzare il servizio SPID GEL di Regione Lombardia deve approvare, con le modalità definite dall'Ente stesso (Delibera o determina), il seguente atto di adesione.

Oggetto: adesione al servizio SPID GEL (SPID Gateway Enti Locali) di Regione Lombardia

premesso che:

- le modifiche introdotte con decreto-legge 21 giugno 2013 all'art. 64 del CAD che prevede "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (di seguito "SPID");
- l'articolo 64, comma 2-quater, del CAD recita "il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con un decreto del Presidente del Consiglio dei Ministri";

visto:

- il DPCM 24 ottobre 2014, recante "Definizione delle caratteristiche del sistema SPID, nonché dei tempi e delle modalità di adozione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) da parte delle pubbliche amministrazioni e delle imprese", pubblicato sulla Gazzetta Ufficiale n. 285 del 9/12/2014;
- l'art. 14, comma 1, del DPCM 24 ottobre 2014 ai sensi del quale le pubbliche amministrazioni che erogano in rete servizi qualificati, direttamente o tramite altro fornitore di servizi, consentono l'identificazione informatica degli utenti attraverso l'uso di SPID
- il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019 adottato da Presidente del Consiglio dei Ministri in data 31 maggio 2017, che prevede che tutte Le Pubbliche amministrazioni devono implementare SPID in tutti i servizi digitali che richiedono autenticazione sia quelli già esistenti che quelli di nuova attivazione, entro marzo 2018;
- il Protocollo D'intesa tra Regione Lombardia, ANCI e ANCI Lombardia per l'attuazione di iniziative di innovazione e digitalizzazione dei Comuni lombardi, approvato con la DGR n. X/3039 del 23/01/2015;
- la Legge Regionale n.20 del 8 luglio 2015, che all'art. 6 ha apportato modifiche alla L.R. 7 del 2012, ed in particolare ha introdotto l'art. 52 ter (Interventi per la crescita digitale) che recita: "La Regione fornisce agli enti locali supporto tecnico specialistico per la progettazione e lo sviluppo di interventi di digitalizzazione e per l'attuazione del codice dell'amministrazione digitale";
- Visto l'allegato A della dgr. n…del… "SPID - Linee Guida per gli Enti Locali";
- Visto il documento "….." approvato con decreto regionale n…..del……..;

DELIBERA/DETERMINA

- di aderire al servizio SPID GEL (SPID Gateway Enti Locali) di Regione Lombardia ;
- di attenersi a quanto previsto al capitolo 6 delle Linee Guida SPID approvate con dgr…..