Regione Lombardia

Supporto agli EELL

per la conformità al Codice Amministrazione Digitale

Adozione di spid

Milano, 6-2-2018

Alcune indicazioni

- **Registreremo la sessione**
  Audio + video e domande che farete
- **Alle domande risponderemo** anche sulla pagina web
- On line nei prossimi giorni: Documenti + filmato
- Tutto su www.agendadigitale.regione.lombardia.it

Agenda

- SPID: norme, obblighi e scadenze
- Supporto di Regione Lombardia all'adesione a SPID
- Il processo di adesione a GEL e SPID
- Le funzionalità per gli Enti Locali
- Domande e risposte

spid

Norme, obblighi e scadenze per le Pubbliche Amministrazioni

regole tecniche, avvisi concetti di identità federata e SAML2.0

L’introduzione di SPID

Nella normativa italiana (CAD art. 64) 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.

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.**

Il 28 luglio 2015, con la Determinazione n. 44/2015, sono stati emanati i quattro regolamenti previsti dal 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.

SPID nel Piano Triennale

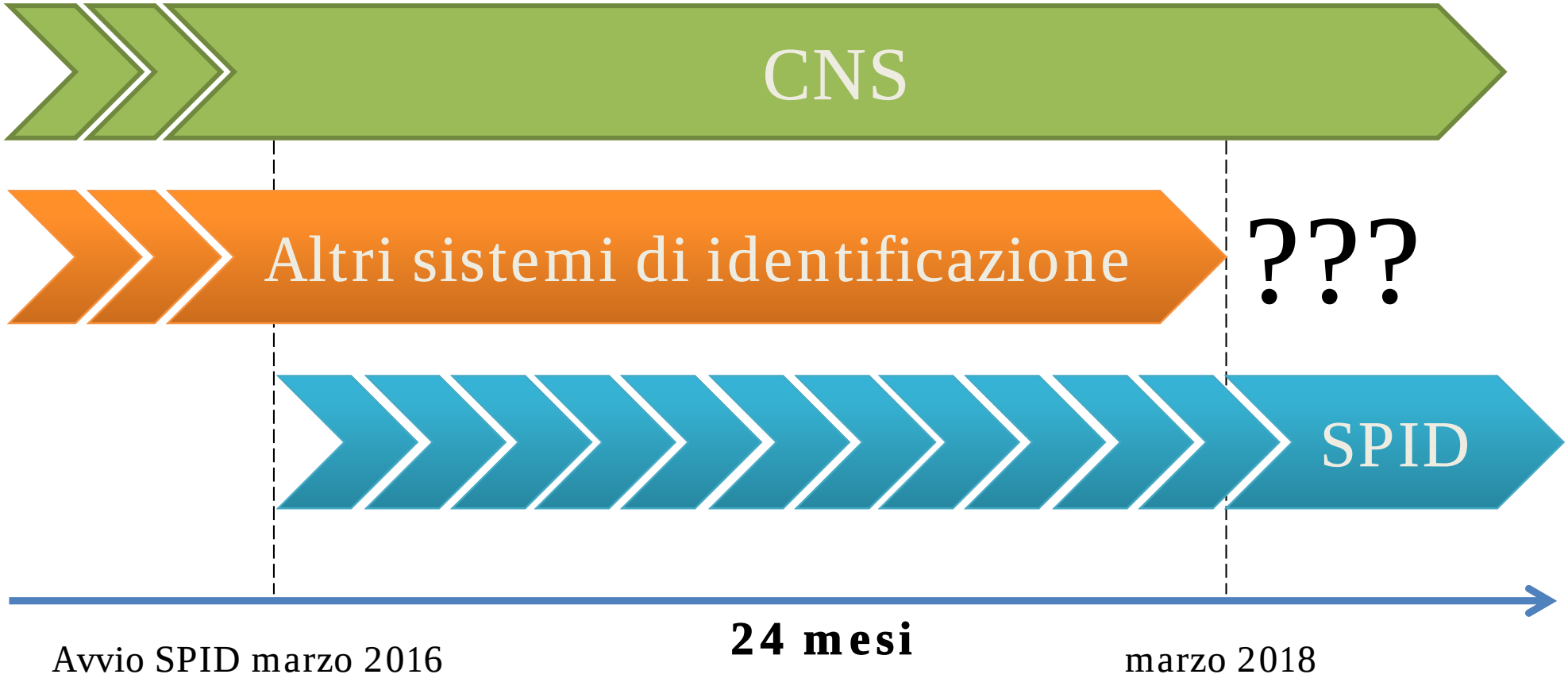
Oggetto	Integrazione con SPID
Tempi	Entro marzo 2018
Attori	AgID, PA
Descrizione	Le Pubbliche amministrazioni devono implementare SPID in tutti i servizi digitali che richiedono autenticazione sia quelli già esistenti che quelli di nuova attivazione, entro marzo 2018, ovvero entro 24 mesi dall'attivazione del primo *Identity Provider*, come definito dal D.P.C.M. 24 Ottobre 2014. L'implementazione si conclude con la controfirma, da parte di AgID, della convenzione SPID inviata dalla PA[61].
Risultato	Completamento dell'integrazione di SPID nei servizi on line della PA *(data di rilascio: marzo 2018)*

SPID nel Piano Triennale

Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione

Oggetto	Monitoraggio implementazione SPID da parte delle PA
Tempi	Entro marzo 2018
Attori	AgID , PA
Descrizione	AgID provvederà a stilare un piano di implementazione di SPID con le PA che non hanno ancora provveduto a farlo e ne monitorerà l'esecuzione.
Risultato	Effettiva adesione a SPID da parte delle PA (*data di rilascio: entro marzo 2018*)

SPID – I tempi della transizione



Entro al massimo marzo 2018 le P.A. adottano SPID
e abbandonano altri sistemi di identificazione (tranne la CNS)

Modifiche al CAD 1 di 3

Decreto Legislativo recante disposizioni integrative e correttive al Decreto Legislativo 26 agosto 2016, n. 179, recante modifiche e integrazioni al Codice dell'Amministrazione Digitale di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di razionalizzazione delle amministrazioni pubbliche

Art.61 (Disposizioni transitorie)
Il diritto di cui all'articolo 3-bis, comma 01,
è riconosciuto a decorrere dal 1° gennaio 2018.

Art. 3-*bis*. Identità e domicilio digitale

01. **Chiunque ha il diritto di accedere ai servizi online** offerti dai soggetti di cui all'articolo 2, comma 2, lettere a) e b), **tramite la propria identità digitale**.

u-quater) identità digitale: la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64;

Modifiche al CAD 2 di 3

Art. 64 Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni

1. e 2 ((COMMI ABROGATI DAL D.LGS. 26 AGOSTO 2016, N. 179)).

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'AgID, secondo modalità definite con il decreto di cui al comma 2-sexies, identificano gli utenti per consentire loro l'accesso ai servizi in rete.

2-quater. L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies. **Resta fermo quanto previsto dall'articolo 3-bis, comma 01**.

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 ……

Modifiche al CAD 3 di 3

QUINDI ?

Il cittadino ha diritto a poter accedere ai servizi online della pubblica amministrazione con SPID dal 1-1-2018.

La pubblica amministrazione, per riconoscere il diritto del cittadino, deve integrare i propri servizi con SPID entro l' 1-1-2018.

DOC UFFICIALE

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

Normativa

Circolari e deliberazioni

- Regolamento SPID: accreditamento gestori (versione 2.0 del 22 luglio 2016)
- Regolamento SPID: modalità attuative (versione 2.0 del 22 luglio 2016)
- Determinazione AGID N. 14/2018 Convenzione SPID tra AgID e Pubbliche Amministrazioni
- Determinazione AGID N. 32/2016 Modello Convenzione SPID tra AgID e Identity Provider
- Modello Convenzione SPID tra AgID e IdP - allegato Determina N.32/2016
- Regolamento SPID: utilizzo identità pregresse
- Regolamento SPID: regole tecniche
- Determinazione AGID pubblicazioni AVVISI SPID
- Determina DG 311 - Referente convenzioni SPID
- Certificato per cifrare la documentazione riservata da inviare all'Agenzia

Leggi decreti e direttive

- Decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014

Documenti

Regole tecniche

- Messaggi SPID
- Tabella attributi
- Note tecniche interfacce SPID
- Obblighi dei Gestori di identità e dei Titolari

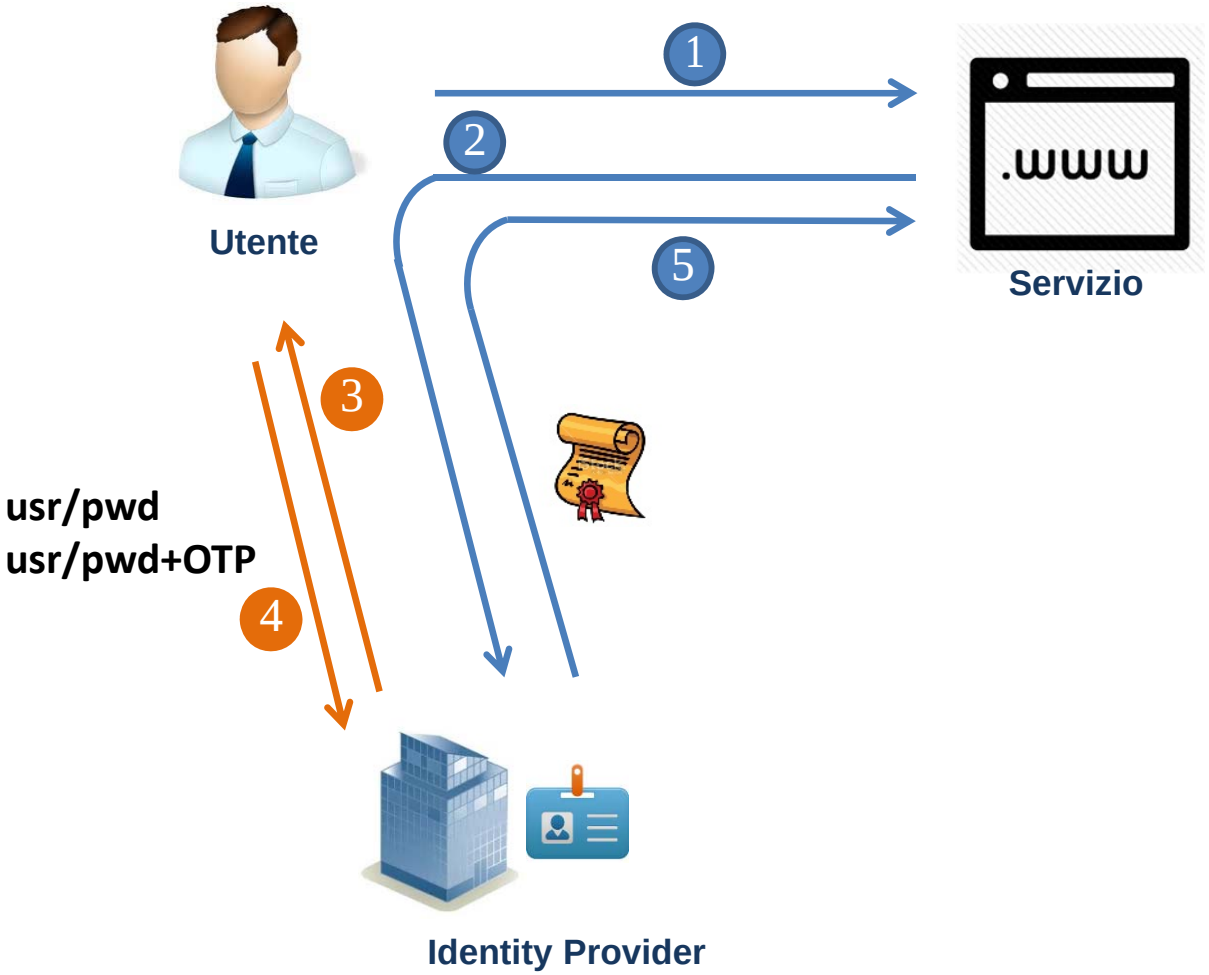
DOC UFFICIALE

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid/avvisi

Documentazione

- Determinazione AGID - pubblicazione AVVISI SPID
- Avviso n. 1 - Gestione della sicurezza del canale di trasmissione
- Avviso n. 2 - Collaborazione tra IDP e SP per problematiche di accesso a SPID
- Avviso n. 3 - Chiarimenti sulla gestione delle sessioni SSO e meccanismo di Single logout
- Avviso n. 4 - Livelli di servizio minimo per funzionalità omogenee
- Avviso n. 5 - Regolamento recante le Regole Tecniche - Errata Corrige
- Avviso n. 6 - Note sul dispiegamento di SPID presso i gestori dei servizi
- Avviso n. 7 – Rilascio Identità SPID agli italiani residenti all'estero

SPID – schema di funzionamento



1. Richiesta di servizio
2. Inoltro verso Identity provider
3. Richiesta credenziali
4. Verifica credenziali
5. Reindirizzamento verso il service provider con asserzione di autenticazione

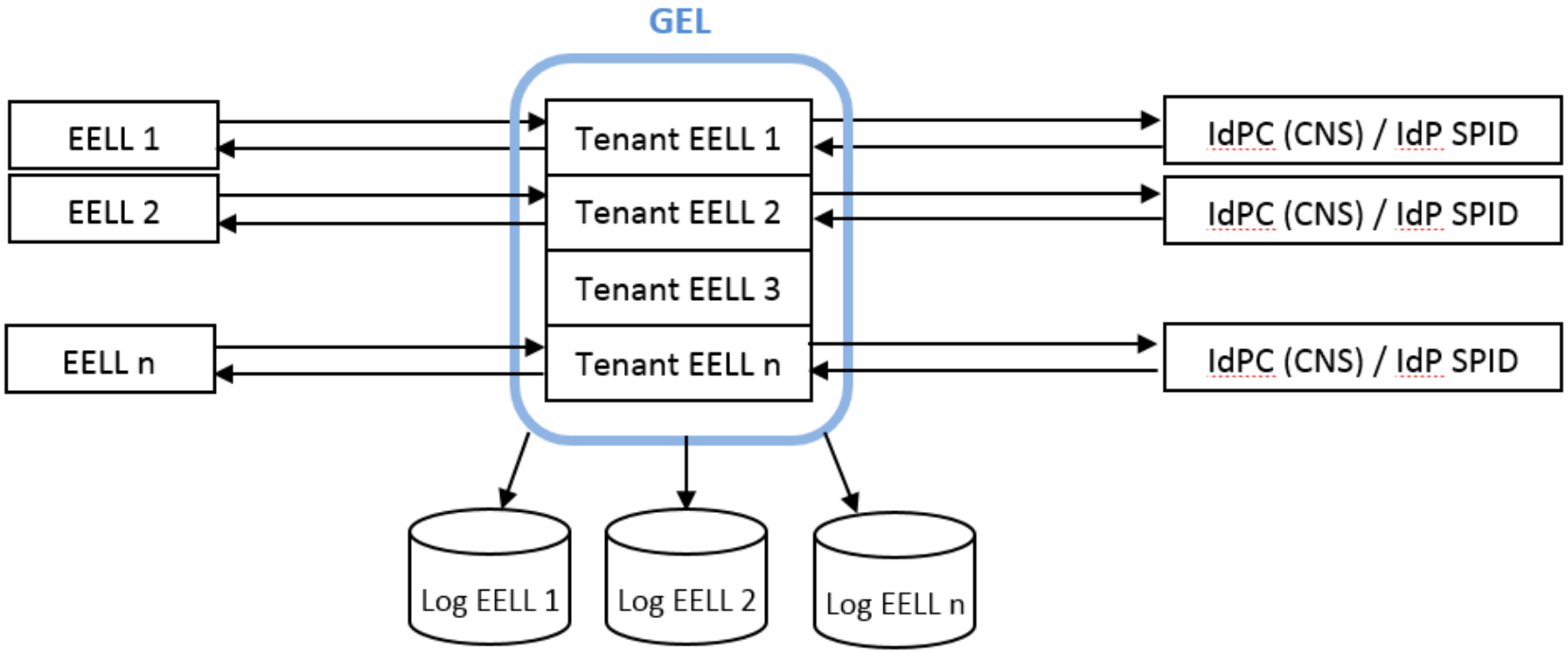
Regione Lombardia

Supporto di Regione Lombardia agli ELL per la migrazione a sp:d

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.

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.



SPID – Linee Guida per gli Enti Locali


RegioneLombardia

LOMBARDIA INFORMATICA

ALLEGATO A

AGENDA DIGITALE LOMBARDA

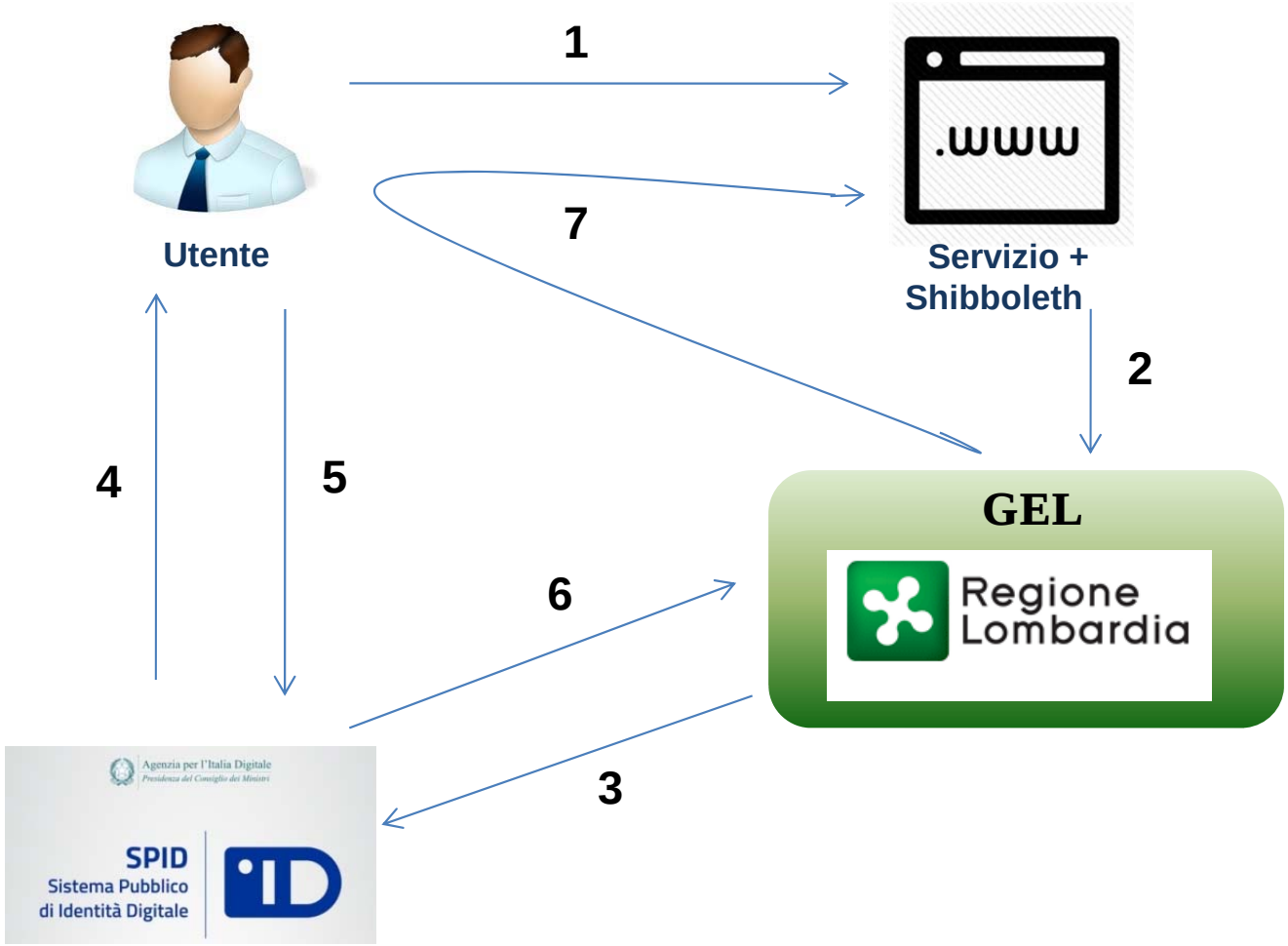
SPID - Linee guida per EELL

SPID - Linee guida per EELL - v. 1.0 1

Per responsabili S.I. e amministratori

Il documento descrive il servizio ed i processi che vanno seguiti per aderire al GEL e a SPID.

SPID tramite GEL



1. Richiesta di servizio
2. Inoltro verso servizio GEL, utente sceglie IdP
3. Richiesta aut.ne (protocollo SPID) verso IdP scelto da utente
4. Richiesta credenziali
5. Verifica credenziali
6. Interpretazione risposta (protocollo SPID)
7. Reindirizzamento verso il SP con dati utente

Accorgimenti sulla user experience

A carico del servizio GEL:

- interpretazione e visualizzazione in “linguaggio naturale” di eventuali errori occorsi durante lo scambio messaggi con sistema SPID, con indicazione del contact point IdP (call center, sito, …)
- test e configurazione di ogni nuovo IdP che viene accreditato da AgID ;
- “IdP chooser” secondo indicazioni AgID

A carico del Service Provider (EELL):

- indicazione dell’area riservata con bottone “Entra con SPID” in accordo a LLGG AgID (http://www.agid.gov.it/sites/default/files/regole_tecniche/spid-notetecnicheinterfacce.pdf sezione 3)
- solo implementazione del bottone, chooser in carico a GEL
- sito SP da proteggere in https (scelta protocolli/algoritmi ha impatti su browser supportati)

Nota - sia il servizio GEL che IdP offrono interfacce (GUI) responsive !

Aspetti di sicurezza

Le Regole Tecniche richiedono l'utilizzo del protocollo TLS 1.2 da parte dei Service Provider per la gestione della sicurezza del canale di trasmissione.

Con l'Avviso n. 1 pubblicato da AgID viene ammesso anche TLS 1.1
http://www.agid.gov.it/sites/default/files/documentazione/spid_-_avviso_n1_-_sicurezza_canale_trasmissione_0.pdf

Impatti:

1) Configurazioni sugli apparati che gestiscono l'SSL
2) Utenti con browser "obsoleti" non accedono ai servizi

Per gli impatti sui Browser utile il riferimento
https://en.wikipedia.org/wiki/Template:TLS/SSL_support_history_of_web_browsers

A nostro avviso il tema è molto più complesso e articolato !
Possibile ottenere ottime configurazioni anche con TLS 1.0

Aspetti di sicurezza

Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > idpcrl.crs.lombardia.it

SSL Report: idpcrl.crs.lombardia.it (82.149.35.24)

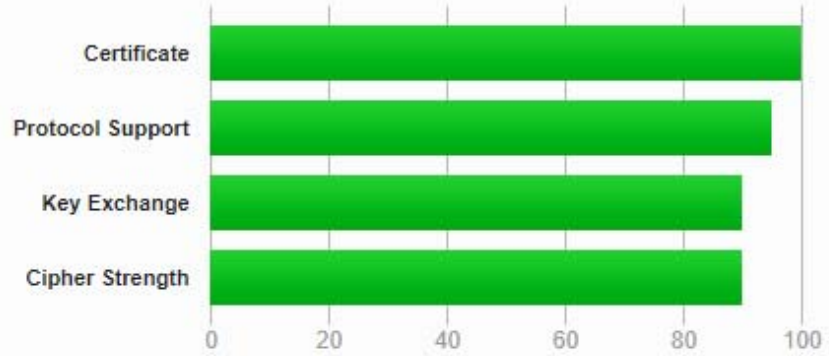
Assessed on: Mon, 05 Feb 2018 19:26:31 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

https://www.ssllabs.com/ssltest

Aspetti di sicurezza

Summary of idpcrl.crs.lombardia.it SSL/TLS Security Test

FINAL GRADE

A

INFO

DATE OF TEST
13:38 CET 25.01.2018

SERVER IP : PORT
82.149.35.24:443

TEST OPTIONS

REFRESH

PDF REPORT

HIGHLIGHTS

The server supports cipher suites that are not approved by PCI DSS requirements, NIST guidelines and HIPAA guidance.	Non-compliant with NIST, HIPAA and PCI DSS
NIST has recently released an **Update to Current Use and Deprecation of TDEA** to abrogate 3DES that was initially authorized in the guidelines.	Information
Test results are over one-week-old, click "Refresh" to update the results.	Information
The server prefers cipher suites supporting Perfect-Forward-Secrecy.	Good configuration
The server provides HTTP Strict Transport Security.	Good configuration

https://www.htbridge.com

Aspetti di sicurezza

Qualys. SSL Labs

Home Projects Qualys.com Contact

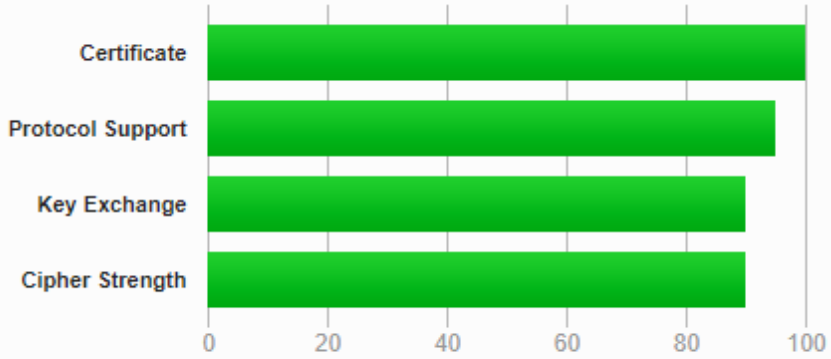
You are here: Home > Projects > SSL Server Test > www.comune.venezia.it > 94.247.8.202

SSL Report: www.comune.venezia.it (94.247.8.202)

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the DROWN attack. Grade set to F. MORE INFO »

This server's certificate will be distrusted by Google and Mozilla from March 2018. MORE INFO »

Aspetti di sicurezza

SSL Report: www.comune.roma.it (93.63.254.113)

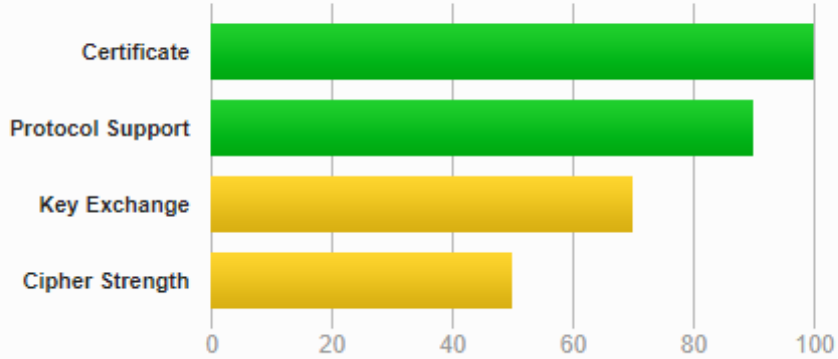
Assessed on: Mon, 05 Feb 2018 19:33:17 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

This server uses RC4 with modern protocols. Grade capped to C.

This server does not support Forward Secrecy with the reference browsers. Grade will be capped to B from March 2018. MORE INFO »

Aspetti di sicurezza

SSL Report: serviziweb2.inps.it (93.63.43.56)

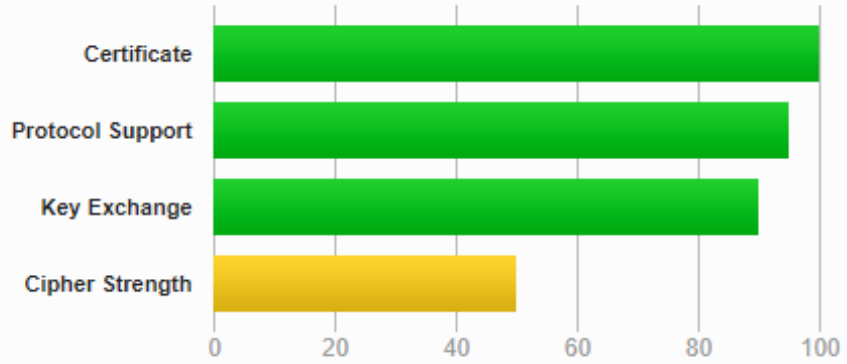
Assessed on: Mon, 05 Feb 2018 19:34:58 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server uses 64-bit block cipher (3DES / DES / RC2 / IDEA) with modern protocols. Grade capped to C. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade will be capped to B from March 2018. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade will be capped to B from March 2018. MORE INFO »

This server's certificate will be distrusted by Google and Mozilla from September 2018. MORE INFO »

Aspetti di sicurezza

Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > spid.sogei.it

SSL Report: spid.sogei.it (217.175.50.72)

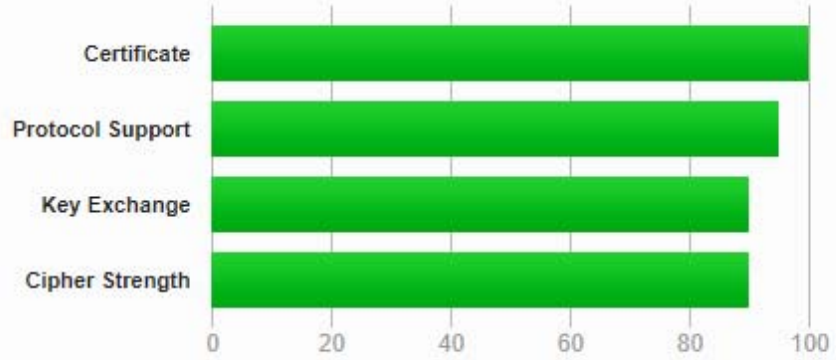
Assessed on: Mon, 05 Feb 2018 19:38:53 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

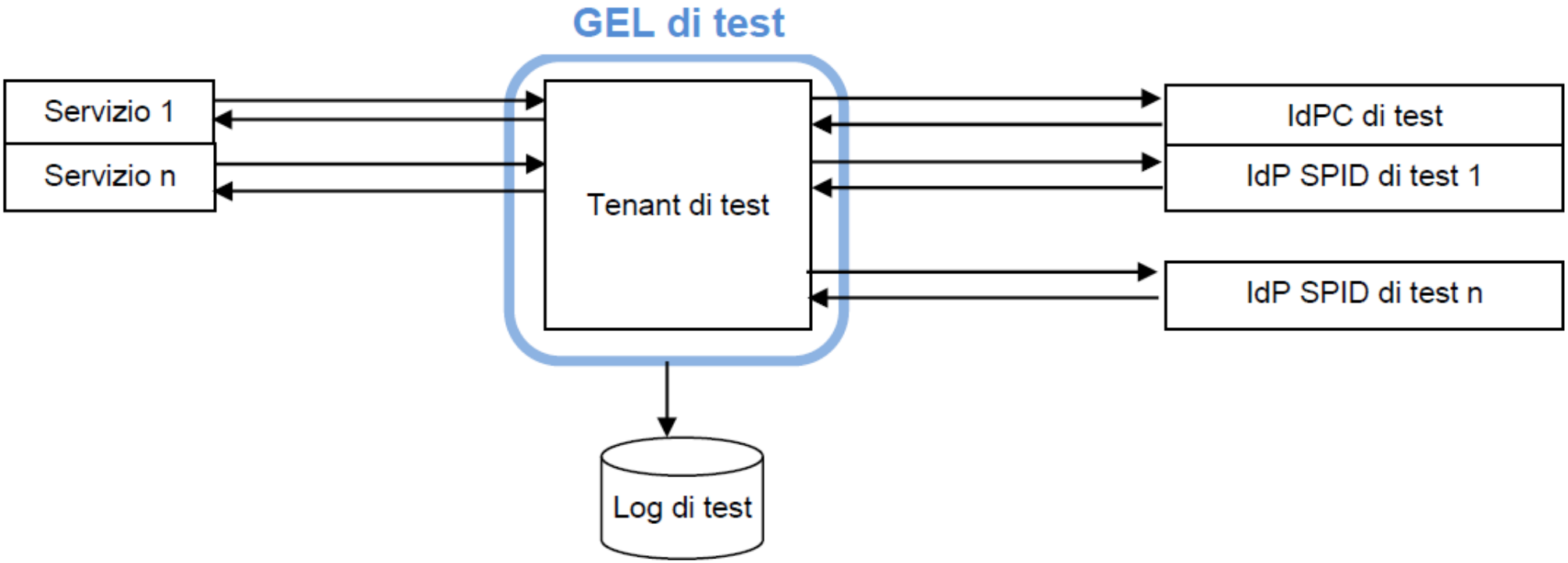
This server is vulnerable to the Return Of Bleichenbacher's Oracle Threat (ROBOT) vulnerability. Grade will be set to F from February 2018.

Demo utilizzo GEL

Il processo di sviluppo e test

Vista complessiva dei processi

Istanza di test



L'istanza di test, funzionalmente equivalente, permette di testare l'integrazione di uno o più servizi con l'istanza IdPC di test e con le istanze di test degli idP SPID che le hanno messe a disposizione.

È importante notare che, trattandosi di circuiti di test e non di circuiti reali, non è possibile utilizzare identità di cittadini reali, bensì nei circuiti di test è possibile unicamente utilizzare:

- Carte CRS/CNS di test (ovvero intestate a cittadini fittizi)
- Identità SPID di test fornite dagli IdP

Lombardia Informatica è in possesso di un certo numero di "credenziali SPID di test" che può distribuire agli Enti.

Processi: sviluppo, test

1. EELL e/o SH : Download «GEL Kit Integrazione»

2. EELL: Richiesta password del file .p12 contenente le chiavi crittografiche

3. SVILUPPO E TEST con istanza GEL di preIT esposta su Internet

4. Notifica di conclusione dei TEST

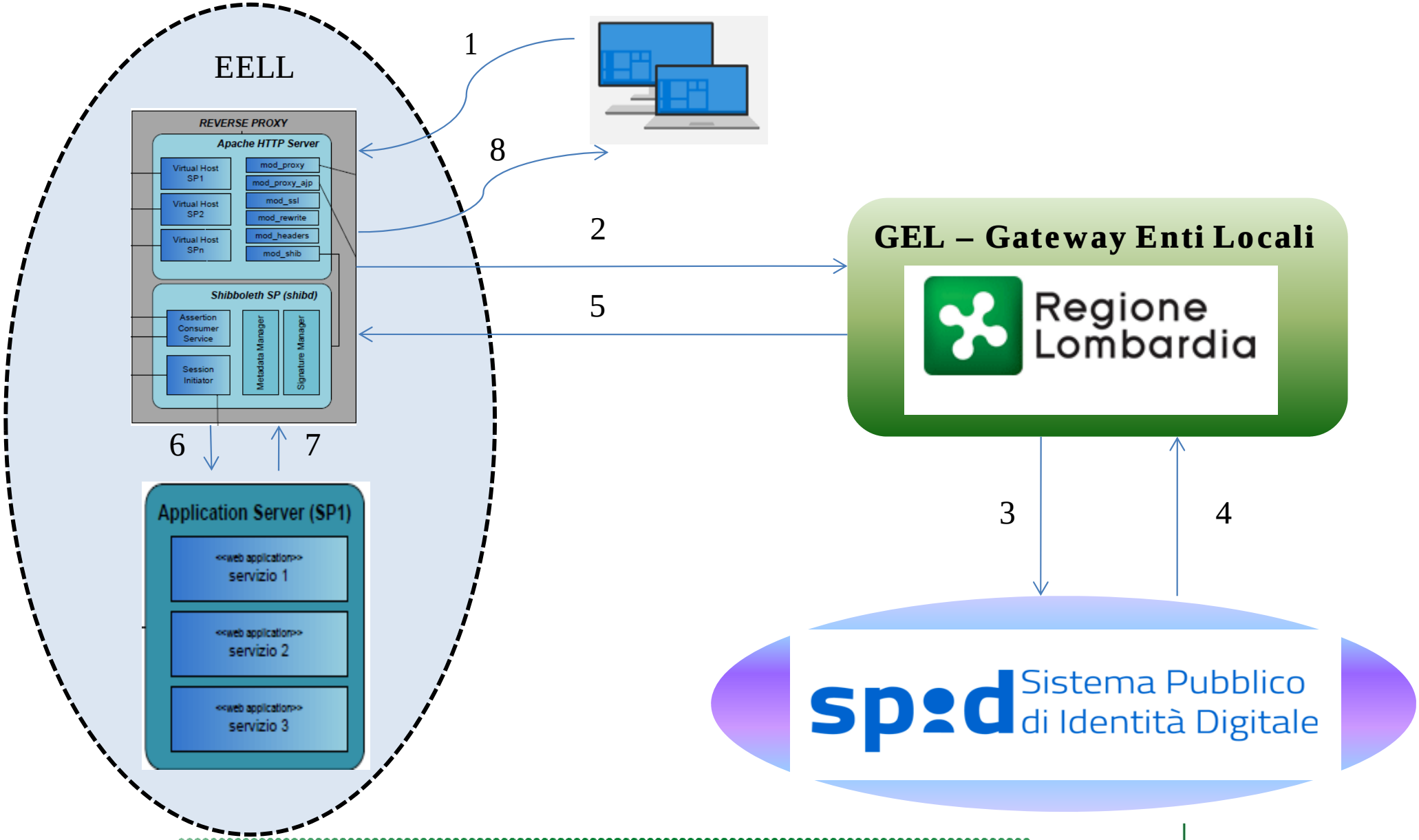
Materiale per sviluppo e test (GEL Kit Integrazione)

1. Documentazione Interfaccia di integrazione a GEL
2. un file (IdpcGelMetadataIntegrazione_locale_PREIT-internet.xml) da installare sulla istanza di Shibboleth del SP per l'istanza di test
3. file attribute_map.xml di Shibboleth
4. una coppia di chiavi crittografiche di test (gel-spid.p12) da utilizzarsi esclusivamente per i test di integrazione al servizio
5. un "componente aggiuntivo" necessario solamente ai SP precedentemente integrati con il sistema di autenticazione di Regione Lombardia tramite le librerie Java denominate «Reference Implementation»
6. utenze di test SPID (solo quelle di PosteItaliane)

Reverse Proxy applicativo Shibboleth (1/3)

- Shibboleth SP è un componente open source con cui si realizza una semplice integrazione ad un IdP (come GEL, o IdPC RL)
- Multipiattaforma; installabile su Apache, IIS
- RP applicativo = RP (es. Apache) + Shibboleth SP
- Ampiamente utilizzato negli anni anche in RL (48% delle odierne transazioni su IdPC)
- Tecnologicamente neutro (applicabile a qualsiasi SP di qualsiasi EELL), dati utente autenticato trasmessi in http header
- SAML impone trust reciproco tra Shibboleth SP e GEL – ciò avviene installazione bilaterale di files "metadata"
- Shibboleth rientra nel dominio del SP, quindi EELL ne ha in carico l'installazione, oltre alla configurazione delle URL da proteggere (no coding)

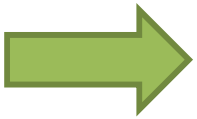
Reverse Proxy applicativo Shibboleth (2/3)



Reverse Proxy applicativo Shibboleth (3/3)

- La configurazione delle URL della applicazione da proteggere con autenticazione avviene in un unico punto (file shibboleth2.xml)

Istruzioni dettagliate per la configurazione sono presenti nella sezione 3.4 del documento di interfaccia di integrazione a GEL



```
...
<RequestMapper type="Native">
<RequestMap applicationId="default">
<Host name="HOST_NAME" [1] scheme="https" port="443">
<Path name="URL_PROTETTO" [2] applicationId="ID_APP" [3] authType="shibboleth" requireSession="true" exportAssertion="true"/>
</Host>
</RequestMap>
</RequestMapper>

...

<ApplicationOverride id="ID_APP" [4] policyId="default" entityID="https://idpcgel.crs.lombardia.it/gelmetadata/COD_ISTAT" [5]
REMOTE_USER="cf" signing="true" encryption="false">
<Sessions lifetime="28800" timeout="3600" checkAddress="false" handlerURL="URL_PROTETTO/Shibboleth.sso" [6] handlerSSL="true"
exportLocation="/GetAssertion" exportACL="127.0.0.1" idpHistory="false" idpHistoryDays="7" cookieProps="; path=/; secure; HttpOnly">
<SessionInitiator type="SAML2" Location="/Login" entityID="https://idpcgel.crs.lombardia.it/idpcgel" >
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="idpcgel" Version="2.0" IssueInstant="2012-01-01T00:00:00Z"
AttributeConsumingServiceIndex="4" [7] >
<samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
<samlp:RequestedAuthnContext Comparison="exact" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
https://www.spid.gov.it/SpidL2oppurehttps://www.spid.gov.it/SpidL3 [8]
</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
<samlp:Scoping ProxyCount="1"></samlp:Scoping>
</samlp:AuthnRequest>
</SessionInitiator>
<md:AssertionConsumerService Location="/SAML2/POST" index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
</Sessions>
<CredentialResolver type="File">
<Key password="PASSWORD_P12" format="PKCS12">[9]
<Path>PATH_P12</Path>
<Name>Regione_Lombardia</Name>
</Key>
<Certificate password="PASSWORD_P12" format="PKCS12">
<Path>PATH_P12</Path>
</Certificate>
</CredentialResolver>
<MetadataProvider type="Chaining">
<MetadataProvider type="XML" file="PATH_METADATA_GEL"/>[10]
</MetadataProvider>
</ApplicationOverride>
...
```

Installazione e configurazione di Shibboleth (1/4)

- Versione di Shibboleth consigliata: almeno 2.6
- Requisiti minimi e procedure di installazione:

  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPInstall
- Distribuzioni ufficialmente supportate ad oggi per Linux:

  Red Hat Enterprise and CentOS 6, 7

  SUSE Linux Enterprise Server 11-SP3, 11SP4, 12SP2, 12SP3
- Download del pacchetto o del repository per la piattaforma appropriata in modo da poter effettuare l'installazione tramite il Software Management System "yum":

  https://shibboleth.net/downloads/service-provider/
- Copiare il repository scaricato nel file:

  /etc/yum.repos.d/CentoOS-Base.repo
- Comandi da eseguire per distribuzione a 32 o 64 bit

  yum install shibboleth

  yum install shibboleth.x86_64

Installazione e configurazione di Shibboleth (2/4)

- Completata l'installazione viene generato il file di configurazione per il caricamento - al riavvio - del modulo di Shibboleth in Apache
- Configurazione del RP Apache:

```
...

ProxyPass        /VerificaGel  http://ip_interno:port_number/VerificaGel
ProxyPassReverse /VerificaGel http://ip_interno:port_number/VerificaGel

ProxyPass /VerificaGel/protected/Shibboleth.sso !

<Location /VerificaGel/protected>
        ShibRequestSetting applicationId VerificaGel
        AuthType shibboleth
        ShibRequireSession On
        ShibUseHeaders On
        require shibboleth
</Location>

...
```

Installazione e configurazione di Shibboleth (3/4)

- */etc/shibboleth/shibboleth2.xml*

```
<ApplicationDefaults ..... >
        .......

<RequestMapper type="Native">
        <RequestMap applicationId="default">
           <Host name="mydomain.example.com scheme="https" port="443">
              <Path name="VerificaGel/protected" applicationId="VerificaGel" authType="shibboleth" requireSession="true" exportAssertion="true"/>
              <Path name="VerificaGel2/protected" applicationId="VerificaGel2" authType="shibboleth" requireSession="true" exportAssertion="true"/>
           </Host>
        </RequestMap>
        </RequestMapper>
        .......
        <ApplicationOverride id="VerificaGel" policyId="default" entityID="https://idpcgel.crs.lombardia.it/gelmetadata/test" REMOTE_USER="cf" signing="true" encryption="false">
        <Sessions lifetime="28800" timeout="3600" checkAddress="false" handlerURL="/VerificaGel/protected/Shibboleth.sso" handlerSSL="true" exportLocation="/GetAssertion"
        exportACL="127.0.0.1" idpHistory="false" idpHistoryDays="7" cookieProps="; path=/; secure; HttpOnly">
         <SessionInitiator type="SAML2" Location="/Login" entityID="https://idpcgel.crs.lombardia.it/idpcgel" >
              <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="ID_UNIVOCO1" Version="2.0" IssueInstant="2012-01-01T00:00:00Z"
        AttributeConsumingServiceIndex="4">
                    <samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
                    <samlp:RequestedAuthnContext Comparison="exact" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                            https://www.spid.gov.it/SpidL2
                        </saml:AuthnContextClassRef>
                    </samlp:RequestedAuthnContext>
                        <samlp:Scoping ProxyCount="1"></samlp:Scoping>
              </samlp:AuthnRequest>
         </SessionInitiator>
         <md:AssertionConsumerService Location="/SAML2/POST" index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        </Sessions>

        <CredentialResolver type="File">
          <Key password="..." format="PKCS12">
         <Path>/etc/shibboleth/gel-spid.p12</Path>
            <Name>Regione_Lombardia</Name>
          </Key>
          <Certificate password="..." format="PKCS12">
         <Path>/etc/shibboleth/gel-spid.p12</Path>
        </Certificate>
        </CredentialResolver>

        <MetadataProvider type="Chaining">
         <MetadataProvider type="XML" file="/etc/shibboleth/GelMetadata.xml"/>
        </MetadataProvider>
        </ApplicationOverride>
```

Installazione e configurazione di Shibboleth (4/4)

```
<ApplicationOverride id="VerificaGel2" policyId="default" entityID="https://idpcgel.crs.lombardia.it/gelmetadata/test" REMOTE_USER="cf"
signing="true" encryption="false">
<Sessions lifetime="28800" timeout="3600" checkAddress="false" handlerURL="/VerificaGel2/protected/Shibboleth.sso" handlerSSL="true"
exportLocation="/GetAssertion" exportACL="127.0.0.1" idpHistory="false" idpHistoryDays="7" cookieProps="; path=/; secure; HttpOnly">
 <SessionInitiator type="SAML2" Location="/Login" entityID="https://idpcgel.crs.lombardia.it/idpcgel" >
      <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="ID_UNIVOCO2" Version="2.0" IssueInstant="2012-01-
01T00:00:00Z" AttributeConsumingServiceIndex="4">
            <samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
            <samlp:RequestedAuthnContext Comparison="exact" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                        https://www.spid.gov.it/SpidL2
                  </saml:AuthnContextClassRef>
            </samlp:RequestedAuthnContext>
                  <samlp:Scoping ProxyCount="1"></samlp:Scoping>
      </samlp:AuthnRequest>
 </SessionInitiator>
 <md:AssertionConsumerService Location="/SAML2/POST" index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
</Sessions>

<CredentialResolver type="File">
  <Key password="..." format="PKCS12">
 <Path>/etc/shibboleth/gel-spid.p12</Path>
    <Name>Regione_Lombardia</Name>
  </Key>
  <Certificate password="..." format="PKCS12">
 <Path>/etc/shibboleth/gel-spid.p12</Path>
</Certificate>
</CredentialResolver>

<MetadataProvider type="Chaining">
 <MetadataProvider type="XML" file="/etc/shibboleth/GelMetadata.xml"/>
</MetadataProvider>
</ApplicationOverride>
```

- Consigliamo di personalizzare, nel file ***bindingTemplate.html***, il messaggio di default visualizzato nel browser durante la fase di redirezione verso GEL, con un messaggio significativo per l'utente.

Scenari di deployment complessi

- **Due applicazioni su stesso dominio** e nello stesso DataCenter (stesso RP/Shib che ridirige): illustrato nelle slide precedenti
- **Due applicazioni in due DataCenter diversi**; sono possibili le seguenti soluzioni:
  - Entrambe devono installare e configurare il proprio RP/Shib utilizzando lo stesso kit di installazione fornito all'Ente
  - Configurare un Link/Redirect dalla prima applicazione verso la seconda. Anche in questo caso entrambe devono installare e configurare il proprio RP/Shib utilizzando lo stesso kit di installazione fornito all'Ente
  - Installare presso un solo DataCenter tutte le applicazioni interessate, in questo caso abbiamo una sola installazione del RP/Shib
  - Istituire una VPN in modo da collegare la rete del RP/Shib con la rete delle applicazioni, in modo sicuro; anche in questo caso abbiamo una sola installazione del RP/Shib
  - Redirigere le chiamate del RP/Shib su internet verso un altro RP che espone l'applicativo/i, instaurando un canale cifrato, con opportuni sistemi di sicurezza; anche in questo caso abbiamo una sola installazione del RP/Shib

Documentazione tecnica


LOMBARDIA INFORMATICA

Classificazione: Pubblico

AGENDA DIGITALE LOMBARDA

– Specifiche di Interfaccia ai Servizi –

Integrazione Gateway Enti Locali (GEL)
tramite Shibboleth

LI-SIS-WS03-GEL#001

Pagina 1 di 1

Documento per tecnici e SW house

Il documento descrive tutte le operazioni che vanno eseguite per una corretta integrazione dei servizi con il GEL.

1. Introduzione
2. Introduzione al servizio GEL
3. Dettagli tecnici
4. Istanza e procedure di test del GEL
5. Architettura del Reverse Proxy Shibboleth SP
6. Configurazione del Reverse Proxy
7. Integrazione di Service Provider con il Reverse Proxy

Processi: messa in esercizio

1. EELL e SH : Download «GEL Kit Esercizio»

2. EELL: Invia «modulo ente» necessario per configurare istanza GEL e definire «amministratore»

3. EELL: Ricevuta email di conferma, accede a GEL per chiedere «materiale crittografico»

4. EELL: Ricevuto certificato/chiave, accede a GEL, crea metadata, lo scarica, lo firma e lo ricarica.

5. EELL: comunica ad AgID i metadata per la verifica e la propagazione agli IdP

6. EELL e/o SH: configura Shibboleth di «esercizio» con parametri della propria istanza GEL

GO LIVE !

Materiale per configurazione (GEL Kit Esercizio)

1. «SPID-GEL Modulo ente.xlsx»

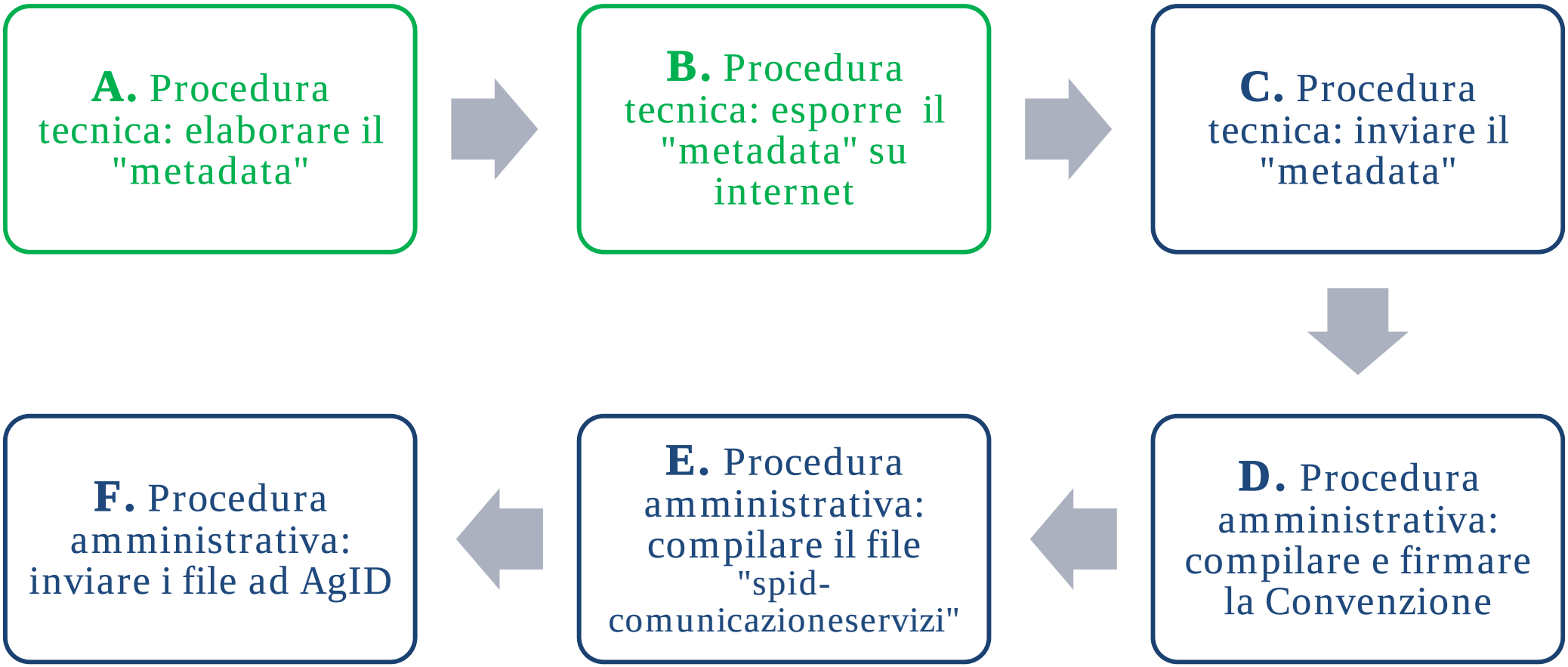
Ente	Cod ISTAT	Nome Referente	Cognome Referente	CF Referente	email Referente	cellulare Referente

2. un file (IdpcGelMetadata_locale.xml) da installare sulla istanza di Shibboleth di visibilità del SP
3. tool per firmare i "metadata" dell'ente
4. tool per decifrare i LOG dell'ente
5. Manuale «Console web per la configurazione self-service dell'Ente Locale»

La Certification Authority LISPA invierà uno ZIP contenente p12 e crt , mentre la password del p12 sarà inviata via SMS.

Il processo di adesione a SPID

Processo di adesione a SPID



https://spid.gov.it/sei-una-pubblica-amministrazione

METADATA (nota sulla definizione dei servizi)

I metadata devono essere composti e firmati secondo le regole tecniche e gli avvisi emessi da AgID, che ne verifica la correttezza formale dei metadata e li approva.

La descrizione dei servizi nei metadata può essere fatta in due modi:

1. Indicando i singoli servizi
2. Raggruppando i servizi per "classi"

Il primo approccio è sconsigliabile essenzialmente perché ogni volta che si introduce un servizio occorre rifare tutto il processo (modificare il metadata, firmarlo, inviarlo ad AgID, attendere la verifica, attendere che gli IdP abbiano ricaricato nei loro sistemi il metadata).

Il secondo approccio, che è quello che è stato seguito per i servizi di Regione e per SPID-GEL, prevede di definire nei metadata secondo "classi" di servizi, che si distinguono unicamente per il **set di attributi che richiedono agli IdPC**.

Questo approccio non solo è consentito, ma è addirittura consigliato nelle regole tecniche, nel paragrafo 1.3.2 SP metadata, in una nota a pag. 20 in basso, che recita:

1 Per la massima tutela della privacy dell'utente il service provider deve rendere minima la visibilità dei servizi effettivamente invocati. In questa ***logica occorre rendere ove possibile indifferenziate le richieste relative a servizi che condividono lo stesso set minimo di attributi necessari per l'autorizzazione***.

METADATA (invio ad AgID)

La procedura per inviare i «metadata» è la seguente:

1. andare su https://helpdesk.spid.gov.it/
2. scegliere "Invia un ticket"
3. scegliere "Assistenza tecnica ai fornitori di servizi"
4. scegliere la Sottocategoria -> "Controllo metadata"
5. indicare la URL, che sarà simile a https://idpcgel.crs.lombardia.it/gelmetadata/Vostro_codice_istat

in questo modo si apre un Ticket che viene preso in carico dalla struttura di AgID che verifica i metadata

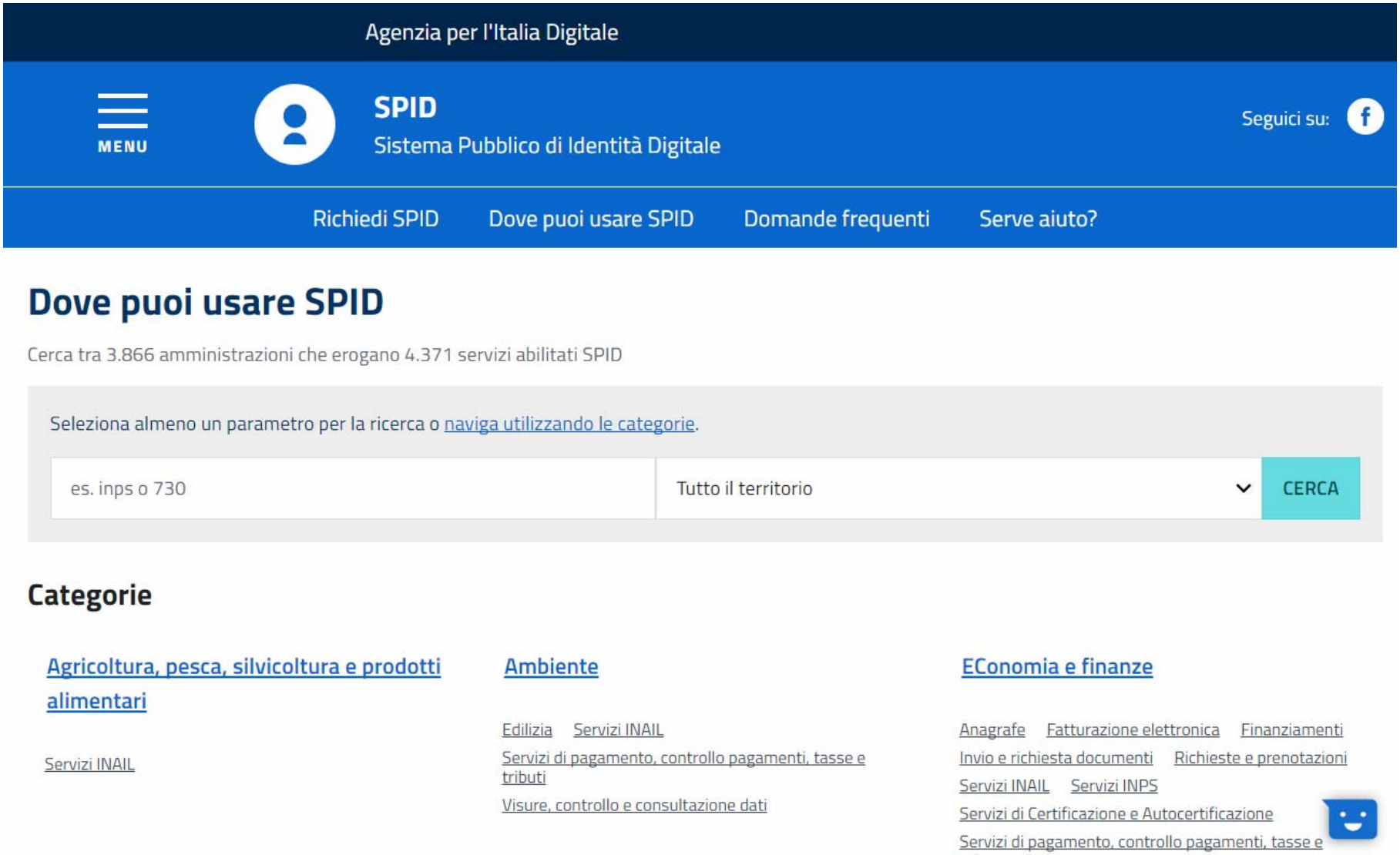
Una volta «validati» , AgID invierà una notifica e comunicherà che i «metadata» saranno configurati dagli IdP entro 24h.

FILE «SPID-ComunicazioneServizi»

AgID ha previsto una comunicazione dei Servizi che il SP integra con SPID, al fine di popolare la directory dei servizi che si trova sul sito di SPID per il cittadino:

FILE «SPID-ComunicazioneServizi»

AgID ha previsto una comunicazione dei Servizi che il SP integra con SPID, al fine di popolare la directory dei servizi che si trova sul sito di SPID per il cittadino:



FILE «SPID-ComunicazioneServizi»

ID Servizio	Id identificativo del servizio, progressivo numerico, la tabella presenta 10 righe, nel caso di più servizi aggiungerne di nuove.	Obbligatorio
Attività di censimento sul servizio	Specificare, dalla lista a tendina: • Nuovo servizio • Aggiornamento servizio • Cancellazione servizio	Obbligatorio
Nome Servizio	Il nome del servizio erogato	Obbligatorio
Descrizione	Descrizione breve del servizio	Obbligatorio
Url del servizio	Url del servizio	Obbligatorio

FILE «SPID-ComunicazioneServizi»

Un parte su cui porre attenzione è quella che richiede di definire gli «attributi»

F	G	H	I
AttributeConsumingService Index su Metadata *	Attributo	Attributo utilizzato (S/N) *	Motivazione *
	Codice identificativo SPID		
	Nome		
	Cognome		
	Luogo di nascita		
	Data di nascita		
	Sesso		
	Ragione o denominazione		
	Sede legale		
	Codice fiscale		
	Partita IVA		
	Documento d'identità		
	Numero di telefono mobile		
	Indirizzo di posta elettronica		
	Domicilio fisico		
	Domicilio digitale		

Regolamento Attuativo - Art. 27 (Uso degli attributi SPID)

I fornitori di servizi, per verificare le policy di sicurezza relativi all'accesso ai servizi da essi erogati potrebbero avere necessità di informazioni relative ad attributi riferibili ai soggetti richiedenti. Tali policy dovranno essere concepite in modo da richiedere per la verifica il set minimo di attributi pertinenti e non eccedenti le necessità effettive del servizio offerto e mantenuti per il tempo strettamente necessario alla verifica stessa, come previsto dall'articolo 11 del decreto legislativo n. 196 del 2003.

Fortemente consigliato AttibuteConsumingServiceIndex = 4
Nome, Cognome, CodiceFiscale, codice identificativo SPID

FILE «SPID-ComunicazioneServizi»

Livello SPID Richiesto -> Consigliato sempre **Livello 2**

Temi
Agricoltura, pesca, silvicoltura e prodotti alimentari (AGRI)
Economia e finanze (ECON)
Istruzione, cultura e sport (EDUC)
Energia (ENER)
Ambiente (ENVI)
Governo e settore pubblico (GOVE)
Salute (HEAL)
Tematiche internazionali (INTR)
Giustizia, sistema giuridico e sicurezza pubblica (JUST)
Regioni e città (REGI)
Popolazione e società (SOCI)
Scienza e tecnologia (TECH)
Trasporti (TRAN)

Sottotemi
Servizi INPS (INPS)
Servizi di Certificazione e Autocertificazione (CERT)
Servizi di pagamento, controllo pagamenti, tasse e tributi (PAGA)
Invio e richiesta documenti (DOCS)
Servizi per dipendenti pubblici (DIPA)
Anagrafe (ANAG)
Servizi Scuola e Università (SCUN)
Servizi di connettività pubblica (SECO)
SUAP Sportello Unico Attività Produttive (SUAP)
Servizi INAIL (INAI)
Richieste e prenotazioni (RIPR)
Visure, controllo e consultazione dati (VICO)
Servizi Sanitari (SESA)
Fatturazione elettronica (FAEL)
Fascicolo Sanitario Elettronico (FSAE)
Finanziamenti (FINA)
Edilizia (EDIL)
Servizi Sociali e della Comunità (SESO)
Servizi di avvisi e notifiche (NOTI)
Servizi Audio, Video e Multimediali (MULT)
Portali del cittadino (POCI)
Iscrizione a servizi (ISCR)
Servizi per le famiglie (FAMI)
Servizi per la viabilità (VIAB)
Utilità (UTIL)

Le funzionalità per gli Enti Locali

Funzionalità per gli Enti Locali

- Gli Enti Locali avranno a disposizione una **console di gestione** con la quale potranno eseguire autonomamente le principali funzioni di configurazione della propria istanza del GEL
- 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;

Manuale GEL per Enti Locali


LOMBARDIA INFORMATICA S.p.A. Classificazione: Uso Pubblico

- Manuale d'uso -

Console web per la configurazione self-service dell'Ente Locale

Revisione del Documento: 02

13-11-2017

LI-SIS-W8B3-GEL@002 - Rev. 02 - Console web per la configurazione self-service d
Pagina 1 di 15

Documento per amministratori EELL

Il documento descrive tutte le operazioni che possono essere eseguite sulla propria istanza di GEL

- ruoli e responsabilità
- creazione di un responsabile operativo/conservatore
- modifica o rimozione di un responsabile operativo/conservatore
- scaricamento dei log a specifiche AgiD
- scaricamento dei log di monitoraggio
- richiesta chiave di firma del servizio
- upload certificato di firma del servizio
- creazione dei metadati EELL
- upload dei metadati EELL firmati
- download dei metadati EELL firmati

Domande e Risposte