Regione del Veneto
Direzione Sistemi Informativi

Standard Regionali

Disciplinare prodotti

Standard del Cluster

Note legali e Privacy

Versione **0.1.0**

Modello documento
NT_ModelloNotaTecnica_v01.3.dot

SOMMARIO

1 APPROVAZIONI

Attività	Nominativo	Azienda	Tel.	e-Mail
Verifica	Antonino Mola	Regione del Veneto		
Approvazione	Andrea Boer	Regione del Veneto		

2 LISTA DI DISTRIBUZIONE

Nominativo	Azienda	Tel.	e-Mail	Tipo
Territorio	Regione del Veneto			

Tipo: CC=Copia Controllata, PC=Per conoscenza

3 STORIA DELLE MODIFICHE

Versione	Data	Descrizione
1.0	22/12/2014	Prima stesura

4 RIFERIMENTI

N.	Titolo	Autore	Versione	Data

5 COPYRIGHT

6 CONTESTO

MyId è il Sistema di Identità Digitale e Piattaforma di Federazione di Provider di identità digital. Il sistema fornisce sia una piattaforma di identità, con funzioni di registrazione e autenticazione utenti, che una piattaforma di federazione dei sistemi di identità, al fine di condividere e far circolare le identità degli utenti su vari servizi di vari Enti
La Federazione è un insieme di soggetti il cui obiettivo principale è fornire ai cittadini accesso a servizi telematici, attraverso l'utilizzo di una credenziale elettronica unica riconosciuta come valida all'interno della Federazione stessa.
Il Nodo regionale identità federata (NRIF) è l'organizzazione regionale incaricata di sviluppare e manutenere il sistema federato regionale di identificazione. Ha il compito di gestore della federazione come meglio dettagliato in seguito a questo documento. Si occupa dell'assistenza agli utenti operatori del sistema e svolge attività di supporto di secondo livello a favore degli Enti utilizzatori nella risoluzione delle richieste di assistenza provenienti dai cittadini. Partecipa ai tavoli nazionali e regionali per lo sviluppo dei sistemi di identità federata.

7 SCOPO

Il presente documento ha lo scopo di definire il modello organizzativo e gestionale della Federazione, andando a definire i soggetti coinvolti, stabilendone ruoli, responsabilità e le modalità di interazione tra gli stessi.
Analizza in particolare la compatibilità del sistema della federazione con la normativa in materia di privacy e tutela dei dati personali.

8 NOTE LEGALI

8.1 Oggetto del servizio

MyId rappresenta il Sistema Federato Regionale di Identificazione utilizzato dalla Regione del Veneto per gestire l'identificazione per l'accesso delle utenti agli applicativi messi a disposizione.
Il Sistema vede coinvolti diversi attori: il Gestore della Federazione, gli Identity Provider ed i Service Provider.

8.2 Obblighi delle parti

8.2.1 Gestore della Federazione: ruolo di Regione del Veneto

Regione del Veneto è il **Gestore della Federazione**, ovvero il soggetto apicale che gestisce il sistema della Federazione nel suo complesso, governando inoltre l'interazione tra i soggetti.
E' suo onere infatti curare i rapporti tra i vari attori della Federazione, garantendone il funzionamento.

Compiti e attività del Gestore
Il Gestore della Federazione*:*

a) nei confronti del Titolare: si occupa della manutenzione del sistema di gestione dei dati; cura i rapporti tra i membri della Federazione;

b) nei confronti degli Identity Provider (Enti federati): si occupa di far accedere al progetto MyId gli Enti interessati e curarne i rapporti con i Service Provider.

In particolare:
1. attribuendo il ruolo di Identity Provider di MyId agli Enti membri del NRIF:
2. che attualmente raccolgono dati-utente esclusivamente per i propri servizi (consentendo loro di portare all'interno del sistema della Federazione dati utente già posseduti, eventualmente mantenendo la propria infrastruttura tecnologica, integrandola opportunamente con il sistema);
3. che sono sprovvisti di sistema di identificazione utenti;

4. gestendo il Trattamento dei dati raccolti dagli Identity Provider, in relazione all'attività del Service Provider;

c) nei confronti dei Service Provider: si occupa di trasmettere i dati raccolti dagli Identity Provider, integrandoli all'interno del sistema della Federazione al fine di consentire ai Service Provider di rendere i servizi disponibili agli utenti;
d) nei confronti degli utenti: offre servizi agli utenti esclusivamente in maniera indiretta, ovvero garantendo il funzionamento della Federazione e l'espletamento dei compiti dei membri della stessa (back office).

Responsabilità del Gestore
E' responsabilità del Gestore della Federazione garantire:
- il funzionamento dei sistemi di gestione della Federazione nel suo complesso e dei servizi di outsourcing per l'espletamento del ruolo di Identity Provider con i sistemi della Federazione stessa;
- l'aderenza agli standard della Federazione da parte di tutti i soggetti coinvolti, al fine di consentire la corretta interazione tra tutti i soggetti e l'espletamento dei servizi rivolti agli utenti;
- la coerenza semantica dei Circle of Trust in termini di livello di affidabilità delle credenziali digitali ad esso afferenti;
- supporto per soggetti aderenti alla federazione in termini di adesione alla federazione, per l'integrazione dei servizi e per la disponibilità di servizi di help desk.

8.2.2 Identity Provider

Gli Identity Provider sono gli Enti che interagiscono direttamente con gli utenti, raccogliendone i dati sull'identità e verificandone l'identità in fase di accesso ai servizi, trasmettendo poi le informazioni sull'identità stessa al Gestore della Federazione (*Regione del Veneto*).
Al fine di diventare Identity Provider, l'Ente interessato deve aver aderito al NRIF.

L'Identity Provider svolge principalmente due compiti:

- registrazione: servizio di Registration Authority, che permette di identificare l'utente e di registrare le informazioni sulla sua identità digitale associando un livello di affidabilità coerente al processo di acquisizione delle informazioni stesse;
- identificazione: servizio di associazione delle informazioni di identità ad un soggetto interagente con il sistema, sulla base della presentazione di credenziali di riconoscimento attraverso vari meccanismi a vari livelli di sicurezza.

Possono svolgere il ruolo di *Identity Provider di MyId* gli Enti appartenenti alla REGIONE DEL VENETO:
- *già dotati di sistema di identificazione utenti*, che raccolgono dati-utente esclusivamente per i propri servizi;
- sprovvisti di un proprio sistema di identificazione utenti.

Ente già dotato di sistema di identificazione utenti
Nel caso in cui il soggetto (*membro REGIONE DEL VENETO*), che diventa Identity Provider sul sistema MyId, disponga di dati utente precedentemente acquisiti su altri sistemi, sarà possibile la migrazione dei dati medesimi, a condizione che l'utente a cui si riferiscono i dati abbia preso visione di un'informativa ai sensi dell' Art. 13 del Codice Privacy (*di cui al capitolo "Privacy e trattamento dei dati: definizione e ruoli")*
.
L'Ente, inoltre, può diventare Identity Provider in MyId utilizzando il sistema MyId oppure mantenendo i propri sistemi. In quest'ultimo caso, l'Ente si impegna a:
- seguire le procedure del sistema MyId per il riconoscimento dell'utente;

- fornire il servizio di registrazione secondo gli standard del sistema MyId;
- fornire il servizio di identificazione aderendo agli standard di comunicazione del sistema MyId in termini di:

- interfacce di comunicazione;
- funzionamento;
- livelli di servizio offerti.

L'Identity Provider che aderisce alla federazione, ma con sistemi propri, assume principalmente due responsabilità:

- riconoscere gli utenti e registrarli, garantendo il servizio ai propri utenti con i propri sistemi (*Registration Authority*);
- identificare gli utenti offrendo loro il servizio di autenticazione con livelli di disponibilità e funzionalità adeguati (*Identificazione*).

Registration Authority

Per l'espletamento dei servizi di Registration Authority, l'Identity Provider deve garantire che il processo di riconoscimento degli utenti avvenga in maniera equivalente ad una delle procedure previste dalla Federazione, stabilendo conseguentemente il livello di fiducia dato dai soggetti aderenti agli utenti registrati.

Identificazione

L'Identity Provider deve implementare gli standard tecnologici MyId. L'adesione dell'IdP locale è subordinato alla positiva esecuzione di un test di interoperabilità con il sistema MyId.

Ente sprovvisto di un proprio sistema di identificazione utenti

Un Ente (*membro della federazione della REGIONE DEL VENETO*), sprovvisto di un proprio sistema di identificazione utenti, può diventare Identity Provider all'interno della Federazione utilizzando il sistema MyId, che offre servizi per la registrazione utenti e per l'autenticazione.
L'Identity Provider che aderisce alla federazione (*sprovvisto di propri sistemi di identificazione*) assume principalmente la responsabilità di riconoscere gli utenti e registrarli, mentre demanda al sistema MyId la responsabilità di identificare gli utenti in fase di accesso ai servizi (*e di far prendere visione all'utente dell'informativa ai sensi dell' Art. 13 del Codice Privacy - di cui al capitolo "Privacy e trattamento dei dati: definizione e ruoli")*).
Per la registrazione degli utenti il sistema MyId mette a disposizione un'applicazione per:

- inserire i dati di un utente nel riconoscimento "de visu", permettendo di consegnare una busta cieca per l'attribuzione di una password;
- modificare i dati dell'utente ad eccezione dei dati anagrafici;
- stampare i dati di un utente per l'accettazione;
- incrementare il livello di affidabilità delle credenziali di un utente;
- sospendere o disabilitare un utente;
- riabilitare un utente;
- rimuovere le informazioni di identità di un utente;
- associare nuovamente una busta cieca all'utente nel caso di necessità.

Registration Authority

Per l'espletamento dei servizi di Registration Authority, l'Identity Provider deve scegliere tra le possibili forme di servizio:

- registrazione de visu: rendere disponibile uno sportello con orari di apertura al pubblico al quale gli utenti verranno indirizzati per il riconoscimento di persona secondo le procedure stabilite per MyId;
- registrazione con invio di documentazione cartacea: rendere disponibile un servizio di ricezione documentazione cartacea via posta ordinaria o via fax che, ricevuta la documentazione, espleti le relative procedure di riconoscimento per MyId;
- registrazione con invio di documentazione elettronica: rendere disponibile un servizio di ricezione di documentazione elettronica (basata sul sistema MyId) che, ricevuta la documentazione elettronica, espleti le relative procedure di riconoscimento per MyId;

- registrazione con invio di Raccomandata AR: rendere disponibile un servizio di invio Raccomandate AR per l'identificazione degli utenti secondo le relative procedure di riconoscimento per MyId.

Identificazione
Verrà creata un'apposita configurazione per ogni Ente della Federazione affinché possa diventare un Identity Provider effettivo del sistema MyId, verso cui gli utenti possono presentare le proprie credenziali per l'identificazione.

8.2.3 Service Provider

Alcuni degli Enti federati si avvalgono di Service Provider per fornire servizi agli utenti. Tali Enti, una volta entrati nella Federazione come Identity Provider, potranno continuare ad avvalersi dei Service Provider, che, però, dovranno integrarsi correttamente con gli Identity Provider stessi.
Il Service Provider, infatti, per potere fornire il servizio all'utente nel progetto MyId dovrà permettere a quest'ultimo di autenticarsi in modo corretto verso l'Identity Provider, che è il solo che lo può riconoscere.
Ovvero, per riconoscere un utente che non si è ancora identificato, il Service Provider deve redirigere l'utente verso un Identity Provider, facendo a quest'ultimo una richiesta di autenticazione secondo gli standard tecnologici del sistema MyId. Una volta autenticato, l'utente ritornerà sul Service Provider che sarà in grado di riconoscerlo.
Il Service Provider ha la responsabilità di trattare i dati provenienti dall'autenticazione di MyId solo ed esclusivamente ove strettamente necessario all'erogazione all'interessato del servizio espressamente richiesto dal medesimo e nei limiti dello stesso.
Per diventare Service Provider è necessario aderire agli standard di comunicazione del sistema MyId per l'interazione con gli Identity Provider.

8.2.4 Organizzazione

Come costituirsi Identity Provider con i propri sistemi
Al fine di costituirsi Identity Provider con i propri sistemi un Ente deve:
- Predisporre tecnicamente il proprio sistema di autenticazione affinché sia conforme allo standard MyId per l'autenticazione utente
- Sottoscrivere un contratto/convenzione con Regione del Veneto in cui si impegna a fornire i servizi di identificazione e registrazione secondo gli standard Regione del Veneto per quanto riguarda:
  - Il riconoscimento degli utenti secondo vari livelli di affidabilità:
    - Auto registrazione,
    - Identificazione certa;
  - e con vari metodi di autenticazione:
    - Userid/password,
    - Utilizzo di smart card di riconoscimento quali CIE o CNS.
  - L'applicazione, agli utenti identificati in modo certo, di password policy conformi alla legge sulla privacy, in particolare tre livelli di policy possibili:
    - nessuna policy,
    - policy per la gestione di dati personali,
    - policy per la gestione di dati sensibili.
  - La conformità agli standard tecnologici di interazione per il sistema di autenticazione, dettati da MyId.
  - La fornitura di End Point di autenticazione secondi i livelli di affidabilità delle credenziali e delle policy relative alla password:

- utente auto registrato (livello C);
- utente riconosciuto personalmente in modo certo (livello A) e senza password policy;
- utente riconosciuto personalmente in modo certo (livello A+) e con password policy per dati personali;
- utente riconosciuto personalmente in modo certo (livello A++) e con password policy per dati sensibili.

Una volta forniti i dati l'Identity Provider verrà censito tra i fornitori di identità del sistema MyId ed entrerà a far parte ufficialmente della federazione con i propri utenti.

Come usare l'Identity Provider di MyId in service

L' Identity Provider:

- fornisce i propri dati identificativi per la configurazione dei sistemi,
- indica gli operatori che saranno preposti a svolgere l'attività di Registration Authority (incaricati del trattamento),
- si impegna a fornire il servizio di registrazione utenti secondo gli standard del sistema MyId.

L'identity Provider dovrà sottoscrivere un apposito contratto/convenzione in cui indica quali servizi di registrazione utilizzerà per gli utenti:

- de visu : riconoscimento diretto dell'utente che si presenta allo sportello;
- invio documentazione cartacea: l'utente esegue una registrazione on-line ed invia la documentazione che ottiene all'ufficio dell'Ente preposto che ne verifica i dati;
- invio documentazione elettronica: l'utente esegue una registrazione on-line e firma digitalmente la documentazione che ottiene e la sottopone attraverso il sistema MyId all'ufficio dell'Ente, che ne deve verificare la validità;
- invio di raccomandate con ricevute di ritorno: l'utente esegue un registrazione on-line e richiede all'ufficio dell'Ente (se si tratta del comune di residenza) di inviargli una raccomandata con ricevuta di ritorno per provare la veridicità dei dati sottoposti;
- dichiara di seguire le procedure di registrazione e riconoscimento utenti dettate da Regione del Veneto e scelte tra quelle citate al punto precedente;
- fornisce i dati degli operatori che eseguiranno le operazioni di registrazione, garantendone l'identità;
- fornisce i dati per l'espletamento dei suddetti servizi, in particolare:

  - nome dell'organizzazione
  - indicazione se trattasi di Ente pubblico o privato
  - tipo organizzazione (Provincia, Comune, altro Ente)
  - indicazione dell'Ente se Provincia o Comune
  - il titolare dei dati trattati
  - numero di FAX
  - email e contatto per la registration authority
  - indirizzo completo presso cui troverà sede la registration authority
  - il tipo di registrazione che intende fare tra quelli citati al Art. 2 comma 4 Lettera A del Protocollo di adesione
  - l'indirizzo internet (URL) a cui l'Ente renderà disponibili informazioni per gli orari e le sedi della registration authority
  - il nome del dominio che l'Identity Provider adotterà
  - il tipo di policy per la password adottata di default per gli utenti
  - il logo dell'Ente

Una volta forniti tutti i dati l'Identity Provider verrà istanziato all'interno del sistema MyId e l'Ente potrà iniziare le operazioni di registrazione degli utenti sul sistema.

Come esporre i propri servizi ad utenti MyId

Un Service Provider che esporrà i propri servizi integrandoli con il sistema MyId dovrà:

1. predisporre tecnicamente i servizi affinché siano conformi allo standard MyId per l'ottenimento delle informazioni dell'utente autenticato attraverso il sistema MyId;
2. sottoscrivere un contratto di adesione alle federazione in cui indicare:
   a. l'indirizzo a cui il servizio sarà reso disponibile
   b. attributi utente di cui il servizio deve disporre tra quelli resi disponibili dal sistema MyId
   c. scopi e modalità di trattamento dei dati del servizio
   d. impegno a non comunicare a terzi i dati utente ricevuti
   e. il bacino di utenza che il servizio ha e i requisiti minimi di affidabilità che il servizio richiede in termini di tipo di identificazione dell'utente

Una volta forniti i dati il Service Provider verrà inserito nel sistema MyId ed entrerà quindi a far parte della federazione.
Il Service Provider riceverà inoltre dati opportuni di configurazione affinché possa far interagire correttamente il proprio servizio con il sistema MyId.

9 PRIVACY

Consultare il seguente documento:

https://myextranet.regione.veneto.it/c/document_library/get_file?p_l_id=88017&folderId=93639&name=DLFE-5940.pdf

10 DISCIPLINARE

I documenti relativi alla Disciplinare del prodotto possono essere soggetti a variazioni nel corso del tempo dovute a normali adattamenti degli standard rispetto alle necessità logistico/organizzative.