

# Riconoscimento identità digitali fornite da Regione Lombardia con sistema preesistente a SPID

Ver. 1.0  
2 marzo 2018

## Autori:

Daniele Crespi – Lombardia Informatica SpA  
Alberto Zanini – Lombardia Informatica SpA  
Pierluigi Valenti – Lombardia Informatica SpA  
Mario Martinelli – Lombardia Informatica SpA  
Daniela Quetti – Lombardia Informatica SpA  
Luca Augello – Lombardia Informatica SpA

## Sommario

1	CONTESTO.....	3
2	SCOPO DEL DOCUMENTO.....	5
3	IL PROCESSO DI RILASCIO DELLE <b>IDENTITA' DIGITALI</b> .....	6
3.1	Disamina normativa.....	6
3.2	Descrizione del processo di erogazione credenziali mediato da un Operatore SISS .....	7
3.3	Composizione delle credenziali.....	12
3.3.1	UserID.....	12
3.3.2	Password.....	13
3.3.3	One Time Password (OTP).....	13
3.4	Ulteriore processo di rilascio.....	14
3.4.1	Richiesta identità digitale in autonomia .....	14
3.4.2	Gestione delle credenziali in autonomia .....	14
3.4.3	Disattivazione credenziali.....	15
3.4.4	Utente deceduto.....	15
3.4.5	Servizi a supporto .....	15
3.5	Evidenze del processo .....	16
4	TRANSIZIONE DELLE CREDENZIALI VERSO SPID.....	17
5	RIFERIMENTI NORMATIVI .....	18
6	RIFERIMENTI DOCUMENTALI.....	19
7	ALLEGATI.....	20
7.1	ALLEGATO 1 Richiesta delle credenziali per l'accesso ai servizi on line e attivazione dei servizi socio-sanitari.....	20
7.2	ALLEGATO 2 Modulo prima parte della password.....	21
7.3	ALLEGATO 3 Password policy fornita al cittadino.....	22
7.4	ALLEGATO 4 Processo di produzione delle attestazioni GASS .....	23

## 1 CONTESTO

Regione Lombardia, dopo aver completato la distribuzione a tutti i cittadini della Carta Regionale dei Servizi CRS (conforme allo standard nazionale CNS – Carta Nazionale dei Servizi), nel corso del 2007 ha sviluppato e reso disponibile a tutti gli Enti Locali (di seguito 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), **garantisce l'accesso ai servizi in rete** erogati dalle pubbliche amministrazioni nel rispetto delle disposizioni normative nazionali (art. 64 del **Codice dell'Amministrazione Digitale**) gestendo **l'accesso sicuro da parte dei cittadini a servizi qualificati che hanno la necessità di assicurarsi dell'identità dell'utente, tramite l'uso della Carta Nazionale dei Servizi CNS** (e più precisamente per i Cittadini in possesso di una CRS o CNS con relativa chiave privata, PIN, e certificato digitale in corso di validità).

L'IdPC è stato utilizzato, a partire dal 2009, come unico servizio per identificare cittadini e imprese che accedono ai servizi online di Regione Lombardia, affiancando alla modalità di autenticazione **“forte”** tramite smartcard CRS/CNS, una modalità di accesso **“basic”** (username e password).

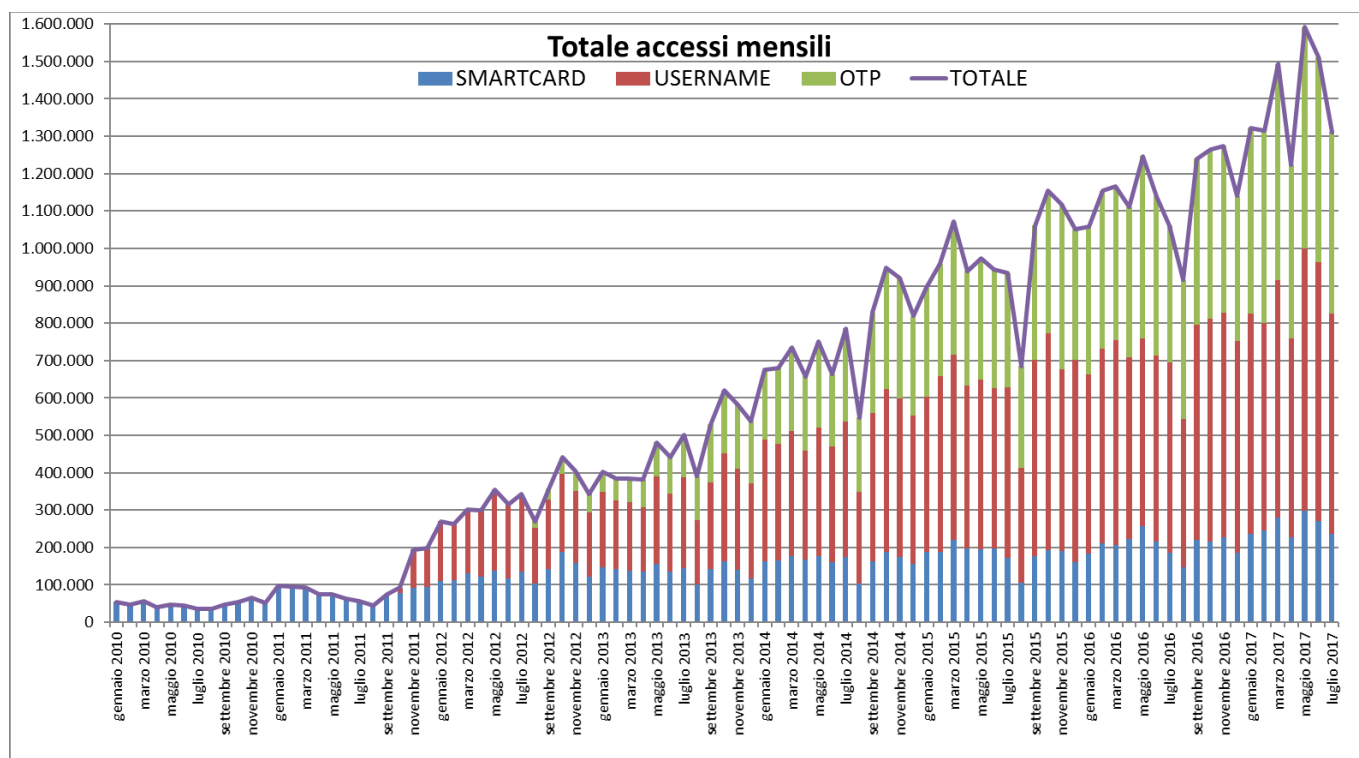
Nel 2012 Regione Lombardia, al fine di avvicinare i Cittadini all'utilizzo dei servizi di sanità digitale ha adottato una modalità di autenticazione ai propri servizi svincolata dal lettore di **smartcard**, composta da una userID, una password personale che solo l'utente conosce e una password usa e getta (OTP). Tale modalità permette l'individuazione del soggetto richiedente il servizio dato che l'identità digitale viene rilasciata **solamente da un operatore abilitato a fronte dell'identificazione certa del Cittadino** (si rimanda al par. 3.2).

Si completa così il panel delle modalità di autenticazione a disposizione degli utenti attuale:

userID e password	userID, password + OTP	CRS o TS-CNS
• autenticazione light	• autenticazione strong	• autenticazione strong

I servizi online di Regione Lombardia che si avvalgono di IdPC sono oltre 90, mentre gli EELL che utilizzano IdPC direttamente o tramite portali “aggregati” sono oltre 500.

L'utilizzo di IdPC è cresciuto nel tempo sia a causa dell'aumento dei servizi integrati sia per l'aumento dell'utilizzo da parte degli utenti, arrivando a superare il milione di accessi al mese:



In particolare, l'introduzione nel 2012 delle credenziali username/pawword, e nel 2013 delle credenziali OTP, hanno contribuito significativamente all'aumento delle transazioni:

	2012	2013	2014	2015	2016
CNS	1.578.322	1.664.188	1.969.718	2.182.792	2.477.914
U/Pwd	2.182.779	2.638.385	4.177.913	5.597.467	6.277.559
OTP	201.131	1.328.216	2.863.500	4.003.434	5.014.740
<b>totale</b>	<b>3.962.232</b>	<b>5.630.789</b>	<b>9.011.131</b>	<b>11.783.693</b>	<b>13.770.213</b>

	2012	2013	2014	2015	2016
CNS	40%	30%	22%	19%	18%
U/Pwd	55%	47%	46%	48%	46%
OTP	5%	24%	32%	34%	36%

Alla data del 5 marzo 2018 le credenziali OTP rilasciate a maggiorenni sono 1.048.049, già depurate dei cittadini deceduti.

Sono stati escluse le credenziali rilasciate a minorenni ed a maggiorenni tramite delega.

## 2 SCOPO DEL DOCUMENTO

Il presente documento descrive le peculiarità del processo di rilascio delle identità digitali, basate su userID, password personale e password usa e getta (OTP) posto in essere da Regione Lombardia **prima dell'introduzione normativa di SPID** (Sistema Pubblico per la gestione dell'Identità Digitale). **Lo scopo è di sottoporre al vaglio di AgID** il riconoscimento delle credenziali pregresse al fine di facilitare la transizione verso SPID dei possessori, come previsto dal **"Regolamento SPID: identità pregresse"** e dalla Determinazione 27/2108.

### 3 IL PROCESSO DI RILASCIO DELLE IDENTITÀ DIGITALI

#### 3.1 Disamina normativa

Le identità digitali basate su UserID, password e OTP sono state rilasciate nel 2012 ai cittadini **basandosi sull'art. 64 del D.Lgs. n. 82 del 7 marzo 2005 Codice dell'Amministrazione digitale**. In base al secondo comma del citato articolo, le Pubbliche Amministrazioni possono, consentire **l'accesso ai servizi in rete da esse erogati** per i quali richiedono **l'identificazione informatica non solo mediante strumenti quali Carta d'Identità Elettronica (CIE) e Carta Nazionale dei Servizi (CNS), ma anche con strumenti diversi "purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio"**.

È pertanto stato adottato un processo che garantisca l'individuazione del soggetto, come richiesto dalla normativa per il rilascio delle identità digitali, avendo come obiettivo primario quello di diffondere tra i Cittadini una nuova modalità di accesso, più semplice di quella con **smartcard** CRS/CNS, lettore e PIN.

Le identità digitali erogate, come già anticipato, si basano su una UserID, una password personale e la ricezione di un OTP sul cellulare dell'utente. Tale modalità è stata qualificata come **strong authentication**, prevedendo il ricorso ad una procedura che implica l'utilizzo coordinato di differenti strumenti, ed in particolare:

Qualcosa che abbiamo	Qualcosa che conosciamo	Qualcosa di cui disponiamo
User id composta dal <b>"Numero di identificazione della tessera"</b> della CRS/CNS	Password una <b>"prima password"</b> composta da: <ul style="list-style-type: none"> <li>una prima metà riportata sul modulo consegnato al <b>momento dell'adesione al servizio</b>;</li> <li>una seconda metà inviata, via SMS, al numero di cellulare <b>fornito dall'utente in fase di rilascio dell'identità</b>;</li> </ul> tale <b>"prima password"</b> al primo accesso deve essere cambiata <b>dall'utente</b> .	Codice usa e getta o OTP inviato al numero di cellulare fornito dall' <b>utente in fase di rilascio dell'identità</b>

### 3.2 Descrizione del processo di erogazione credenziali mediato da un Operatore SISS

Il Cittadino può richiedere la propria identità digitale per accedere ai servizi online di Regione Lombardia presso gli appositi punti di erogazione quali: gli sportelli delle ATS, gli sportelli di accettazione delle ASST, i Comuni, i punti SpazioRegione, gli Uffici Territoriali Regionali (ex STER), i punti presenti durante specifiche manifestazioni, ecc..

Per poter **rilasciare** l'identità digitale è necessario che vengano rispettati alcuni prerequisiti:

- **l'operatore deve autenticarsi al Sistema Informativo Socio Sanitario (SISS)** di Regione Lombardia tramite Carta Operatore con SSO;
- il Cittadino deve essere in disponibilità fisica di una CRS o CNS;
- il Cittadino deve essere identificato in maniera certa;
- **il Cittadino deve fornire all'operatore un recapito telefonico**, al fine di ricevere:
  - metà della prima password;
  - e quando richiesto, la One-Time Password (OTP) di accesso.

Una volta verificato il rispetto dei prerequisiti di base, l'inizio del processo di erogazione dell'identità per l'accesso ai servizi online prevede i seguenti passaggi:

- 1) L'identificazione telematica, **da parte dell'operatore SISS**, del Cittadino Interessato tramite inserimento nel lettore di **smartcard della postazione di lavoro dell'operatore**, della Carta CRS/CNS del Cittadino.
- 2) L'identificazione ai sensi di legge del Cittadino **richiedente l'identità digitale** (D.P.R. 445/2000 **Errore. L'origine riferimento non è stata trovata.**), richiedendogli l'esibizione di un documento di riconoscimento in corso di validità.
- 3) La raccolta, **da parte dell'Operatore SISS**, del numero di cellulare (dato obbligatorio) e **dell'indirizzo di posta elettronica (dato facoltativo) da associare all'identità**.

NOTA: si precisa che dal 2016 ogni identità digitale deve essere obbligatoriamente arricchita da parte dell'utente inserendo nel Profilo Utente correlato un indirizzo di posta elettronica validato.

- 4) La precisazione della posizione del Cittadino **che richiede il rilascio dell'identità**: se diretto interessato, se soggetto rappresentante, se tutore o genitore di minore ecc..<sup>1</sup>
- 5) La raccolta **da parte dell'operatore SISS** della richiesta, mediante raccolta del modulo sottoscritto in modo autografo **da parte del Cittadino "Richiesta delle credenziali per l'accesso ai servizi on line e attivazione dei servizi socio-sanitari"** (ALLEGATO 1 par.7.1). Contemporaneamente, è raccolto il suo consenso al trattamento dei recapiti personali forniti ai fini della gestione delle credenziali di accesso ai servizi online ai sensi del Codice Privacy.

La sottoscrizione dell'istanza di richiesta delle credenziali è autenticata ai sensi della disciplina dettata dall'art. 21 del D.P.R. 445/2000 essendo sottoscritta **dall'interessato**, dal tutore o dal genitore del minore in presenza del dipendente addetto.

I dipendenti addetti svolgono la loro attività presso i punti di raccolta dell'istanza di richiesta credenziali delle ATS, ASST, IRCCS e Enti Gestori Privati Accreditati al SSR, pertanto rivestono il ruolo di pubblici ufficiali nello svolgimento di tali attività.

---

<sup>1</sup> **NOTA BENE: Sono escluse dal progetto di recupero identità pregresse, quelle rilasciate mediante delega e in favore del tutore o del genitore del minore.**

- 6) Solo a fronte della raccolta della richiesta firmata dal Cittadino, e quindi della sua corretta identificazione, **l'operatore** è abilitato ad proseguire nella procedura e pertanto invia un Documento di Autorizzazione firmato digitalmente al SISS (la Carta CRS/CNS del Cittadino deve essere presente nel lettore al momento della firma digitale da parte dell'Operatore). In tale documento sono riepilogati i dati dell'operatore, del Cittadino e l'oggetto dell'istanza come di seguito riportato:

Regione Lombardia - Progetto CRS-SISS - Registra Credenziali

Data: gg-mm-aaa

Oggetto: Richiesta delle credenziali per l'accesso ai servizi on line messi a disposizione da Regione Lombardia

Documento emesso da **<Ente appartenenza dell'Operatore>**,

In data gg-mm-aaa

Il Sottoscritto:

**<nome e cognome dell'Operatore>**

Codice Fiscale Operatore: **<CF dell'Operatore>**

in qualità di operatore autorizzato dalla struttura: **<Ente appartenenza dell'Operatore>**,

DICHIARA di aver opportunamente accertato, ai sensi dell'art. 45 del DPR 445/2000, l'identità dell'Interessato richiedente le credenziali per l'accesso ai servizi on line messi a disposizione da Regione Lombardia, come segue:

**<nome e cognome Interessato>**, **<Sesso Interessato>**, **<Data di nascita interessato>**

Codice Fiscale Cittadino: **<CF Interessato>**,

Numero CRS Cittadino: **<Numero identificazione CNS del Cittadino>**,

DICHIARA INOLTRE:

- di aver ricevuto la richiesta da parte dell'Interessato delle credenziali per l'accesso ai servizi on line offerti da Regione Lombardia;
- di aver ricevuto la richiesta da parte dell'Interessato di attivazione dell'accesso ai servizi socio-sanitari on-line;
- di aver raccolto dall'Interessato il consenso al trattamento del proprio numero telefonico **<Numero Telefono Cittadino>** per ricevere le password temporanee di accesso ai medesimi servizi on line come da informativa al trattamento dei dati a lui fornita;
- che la sottoscrizione delle richieste di cui sopra e del consenso al trattamento dei dati è stata apposta in sua presenza;
- di conservare, presso la struttura per cui opera, secondo le procedure previste dalla struttura medesima, la copia cartacea delle richieste di cui sopra e del consenso al trattamento dei dati, sottoscritti dall'Interessato

Il presente documento è firmato digitalmente dall'Operatore **<nome e cognome dell'Operatore>**"



- 7) Il Documento di Autorizzazione firmato digitalmente **dall'operatore SISS** è archiviato tramite il servizio di **"giornalizzazione dei log"** (SAFE – si rimanda per un approfondimento al par. 3.5) che permette di loggare le attività dispositive e marcare temporalmente i log delle operazioni in modo che:
- a) **il documento firmato, inviato dall'operatore SISS sia conservato;**
  - b) **sia collocata nel tempo l'azione che ha generato il documento;**
  - c) **sia garantita l'integrità del documento stesso.**

A fronte della ricezione da parte del SISS del Documento di Autorizzazione, vengono comunicate a IdPC tutte le informazioni necessarie per la creazione del Profilo Utente associato **all'identità digitale**.

- 8) L'**operatore SISS**, ricevuto il buon esito dell'invio del Documento di Autorizzazione, consegna al Cittadino un promemoria cartaceo descrittivo delle modalità di fruizione **dell'identità digitale** e contenente i primi caratteri della **"prima password"** per il primo accesso al servizio (ALLEGATO 2 par. 7.2).
- 9) I rimanenti caratteri della **"prima password"** sono inviati al numero di telefono cellulare fornito dal Cittadino richiedente.

NOTA: la suddivisione della consegna della password di primo accesso metà al momento della richiesta e metà ricevuta sul cellulare, garantisce che **neppure l'operatore che rilasci** le credenziali conosca la password completa (che in ogni caso dovrà essere sostituita al primo accesso dal Cittadino) ed è un processo che recepisce raccomandazioni di **standard** internazionali sulla sicurezza delle informazioni.

Si riepiloga quanto sopra descritto graficamente nei punti 8 e 9:

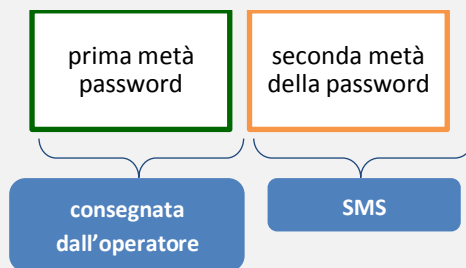
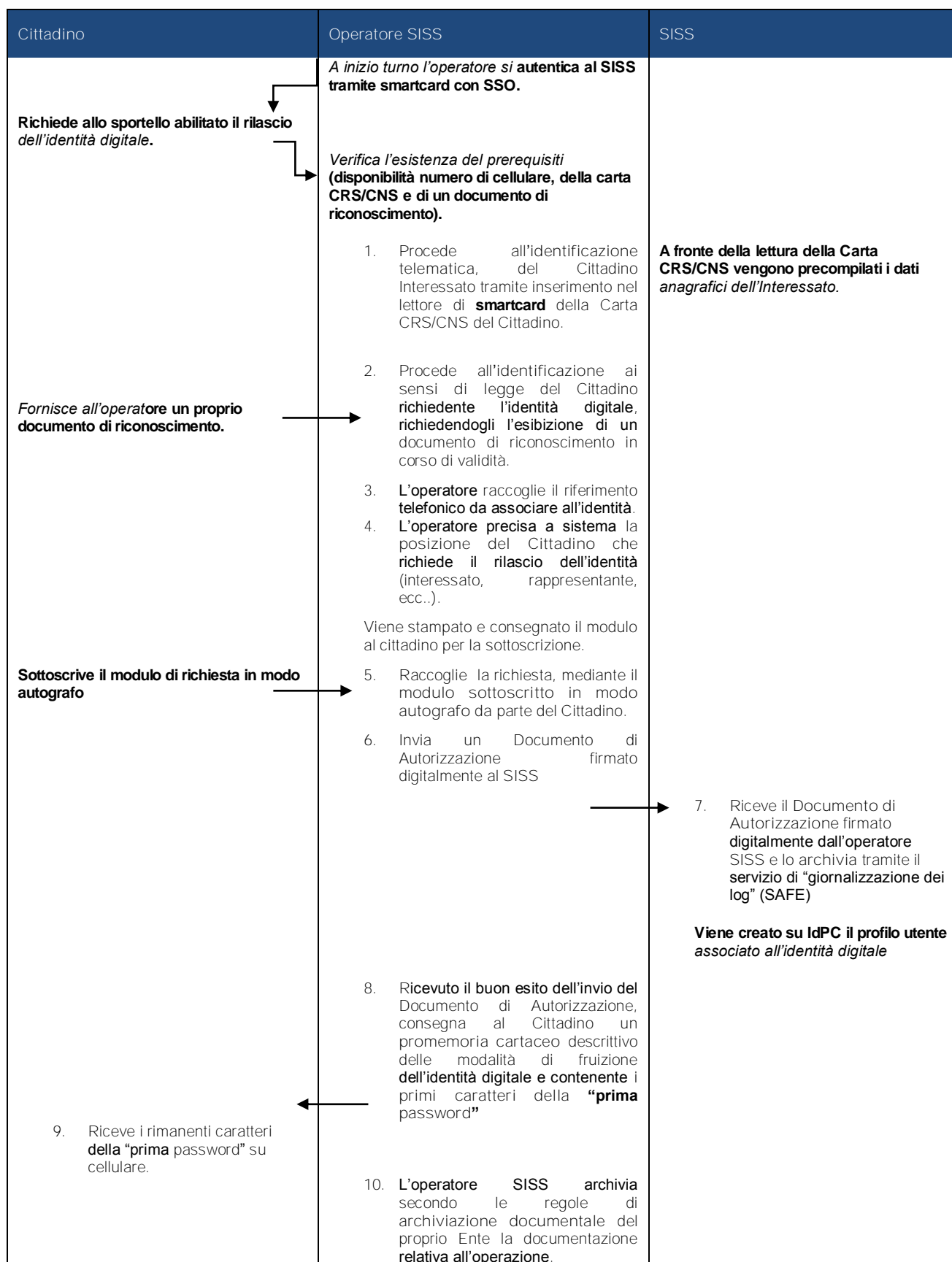


Figura 1 –richiesta credenziali da operatore

- 10) L'**operatore SISS** archivia secondo le regole di archiviazione documentale del proprio Ente la documentazione relativa all'operazione (modulo di richiesta firmato dall'interessato, autocertificazioni, ecc...).

Si riepiloga graficamente il processo descritto:



In aggiunta al processo, l'utente contestualmente al rilascio dell'identità digitale può facoltativamente richiedere:

- l'attivazione del servizio di notifiche telematiche in ambito sanitario;
- la registrazione del consenso al trattamento dei dati personali effettuato tramite Fascicolo Sanitario Elettronico.

### 3.3 Composizione delle credenziali

#### 3.3.1 UserID

L'UserID della credenziale è composto **dall'intero numero di identificazione** della CRS/CNS del Cittadino (c.d. European Code).

Essendo il numero di identificazione della CRS/CNS un codice numerico lungo 20 caratteri normalmente con gli stesse cifre per le carte CRS/CNS emesse da Regione Lombardia per agevolare un utilizzo di routine da parte del cittadino tramite web, è stata pensata una soluzione che minimizza il numero di cifre che il Cittadino deve inserire pur identificando in modo univoco l'UserID: **l'utente in possesso di una CRS/CNS emessa da Regione Lombardia** deve digitare solo gli ultimi 10 caratteri. Nel caso di assistiti lombardi con CNS emesse da altre regioni è possibile modificare anche i primi 10 caratteri.



Figura 2 – Cifre richieste del numero di identificazione della CRS/CNS emesse da RL.

##### 3.3.1.1 Precisazione

Il numero di identificazione della CRS/CNS del Cittadino cambia nel tempo, ad esempio perché, a scadenza, la carta viene rinnovata o perché in caso di smarrimento, è previsto che il Cittadino possa chiederne la ri-emissione. Ad ogni Carta sarà sempre associato un numero di identificazione univoco, differente da quello associato alla carta precedente. Il servizio IdPC implementa un meccanismo di aggiornamento del Profilo Utente a fronte del verificarsi di una delle seguenti condizioni:

1. **se il Cittadino usa l'UserID associato alla vecchia CRS/CNS**, l'accesso viene consentito fino alla data di scadenza della carta a meno che la stessa non risulti revocata.
2. **se il Cittadino usa l'UserID associato alla nuova carta CRS/CNS**, IdPC verifica fruendo di servizi interni al SISS **l'attribuzione della nuova Carta al Cittadino** e da quel momento in avanti il Cittadino può accedere con il nuovo UserID (c.d. riconciliazione).

### 3.3.2 Password

#### 3.3.2.1 Primo Accesso

Quando l'utente si autentica per la prima volta ad uno dei siti di servizi online della Regione Lombardia deve inserire la propria **"prima password"** composta dalla prima metà ricevuta dall'operatore (o a seguito del processo **online**, si rimanda al par. 3.4.1) e la seconda ricevuta via SMS. Viene **successivamente richiesto all'utente di scegliere una propria password personale**, che deve rispettare la password policy di IdPC (vedi ALLEGATO 7 par. 7.3).

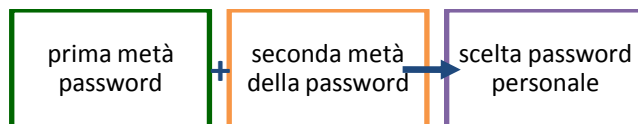


Figura 3 – primo accesso

L'utente viene successivamente invitato a completare il proprio Profilo Utente, inserendo un indirizzo di posta elettronica (che dovrà essere validato tramite link inviato via email) e la risposta a una domanda segreta, che potrà essere utile in caso di reset password (**es. se l'utente ha dimenticato la propria password personale**).

#### 3.3.2.2 Scadenza password

Decorsi sei o tre mesi dall'ultimo cambio della password effettuato dall'utente, la password scade e pertanto l'utente, al primo tentativo di accesso, deve definirne una nuova rispettando la password policy vigente. La tempistica di sei o tre mesi dipende dalla tipologia di dati trattati dai servizi del sito.

#### 3.3.3 One Time Password (OTP)

Il codice **One Time Password** OTP viene inviato via SMS al numero di cellulare indicato dal Cittadino in fase di richiesta dell'identità.

Il Codice si compone di 8 cifre numeriche ed ha una spendibilità di 3 minuti da quando viene consegnato l'SMS al provider. Ogni OTP è spendibile per una sola autenticazione.

## 3.4 Ulteriore processo di rilascio

### 3.4.1 Richiesta identità digitale in autonomia

L'utente autenticato al sito dei servizi sanitari online con **smartcard** CRS/CNS può richiedere l'identità digitale composta da "UserID, password e OTP" in autonomia, il processo è possibile in quanto l'identificazione dell'utente è già avvenuta in fase di rilascio dei codici PIN/PUK della carta. In questo caso l'utente può scaricare un documento PDF con metà della "prima password" e riceve la seconda metà della "prima password" tramite SMS al numero di telefono indicato in fase di richiesta.

Si riepiloga quanto sopra descritto graficamente:

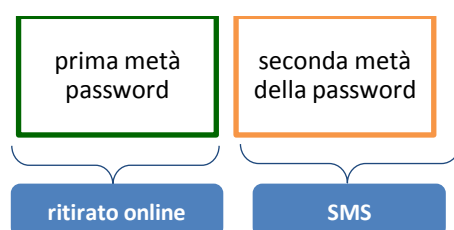


Figura 4 → richiesta credenziali in autonomia online

### 3.4.2 Gestione delle credenziali in autonomia

Gestendo il proprio Profilo Utente dal sito dei Servizi Sanitari di Regione Lombardia (<https://www.crs.regione.lombardia.it/sanita>) il Cittadino può:

- modificare il numero di telefono associato **alla propria identità** (l'istanza inviata telematicamente è soggetta al servizio di giornalizzazione par. 0);
- gestire il proprio indirizzo di posta elettronica (l'istanza inviata telematicamente è soggetta al servizio di giornalizzazione par. 0);
- modificare la password personale.

#### 3.4.2.1 Reset password

Nel caso in cui il Cittadino non ricordi la propria password personale dal sito dei Servizi Sanitari di Regione Lombardia (<https://www.crs.regione.lombardia.it/sanita>) può chiederne il reset indicando:

- UserID;
- Codice Fiscale;
- numero di telefono **cellulare fornito in fase di rilascio dell'identità**;

a fronte della correttezza dei tre dati inseriti l'utente riceve tramite SMS un codice di autorizzazione per l'operazione, inserito tale codice, il sistema provvederà a generare una nuova password che sarà consegnata per una prima metà via SMS al numero di cellulare fornito in fase di rilascio e per una seconda metà direttamente a video. Anche in questo caso, al primo utilizzo della password il Cittadino dovrà scegliere una propria password personale (vedi ALLEGATO 7).



Figura 5 –reset password

In alternativa all'SMS di autorizzazione il Cittadino potrà scegliere di rispondere ad una domanda segreta precedentemente valorizzata dall'utente nel proprio **Profilo Utente**.

#### 3.4.3 Disattivazione credenziali

Il Cittadino può disattivare la propria identità digitale in qualsiasi momento, presentando apposita istanza all'**Ufficio Privacy SISS** (fruendo della modulistica presente sul sito CRS) oppure direttamente online in autonomia dal **Profilo Utente** del sito Servizi Sanitari di Regione Lombardia (<https://www.crs.regione.lombardia.it/sanita>).

#### 3.4.4 Utente deceduto

Quando un Cittadino decede viene aggiornata la sua posizione anagrafica.

Il servizio di autenticazione IdPC verifica se è valorizzato il campo del decesso in anagrafica per **l'utente che cerca di autenticarsi, nel caso in cui l'utente risulti deceduto** è visualizzato un messaggio che avvisa dell'impossibilità di procedere con l'autenticazione e fornisce indicazioni su come esercitare il diritto d'accesso per gli eredi.

#### 3.4.5 Servizi a supporto

Il Cittadino può reperire informazioni sulle credenziali di accesso ai servizi online sia tramite web, sul sito informativo di Regione Lombardia sia tramite gli specifici siti tematici in cui è possibile autenticarsi (ad esempio alla pagina del sito Servizi Sanitari di Regione Lombardia <https://www.crs.regione.lombardia.it/sanita>), sia presso i punti di erogazione delle identità digitali, grazie ad opportuna cartellonistica.

È inoltre attivo un Contact Center Regionale reperibile al numero verde 800.030.606 (attivo dal lunedì al sabato, dalle 8.00 alle 20.00) o **tramite posta elettronica all'indirizzo** [callcenter-crs@regione.lombardia.it](mailto:callcenter-crs@regione.lombardia.it), viene fornito al Cittadino un servizio informativo e di supporto.

### 3.5 Evidenze del processo

I Documenti di Autorizzazione, definiti nei paragrafi precedenti, sono sottoscritti con firma elettronica qualificata dagli operatori addetti a questo servizio e sono pertanto non modificabili e riconducibili ai sottoscrittori. Gli operatori, che effettuano questa attività, sono identificati ed autorizzati dal servizio di Single Sign On del Sistema Informativo Socio Sanitario di Regione Lombardia (SISS).

Questi documenti sono versati in un sistema di giornalizzazione (SAFE) che provvede alla loro archiviazione e collocazione nel tempo tramite il servizio di **Time Stamp** di una **Certification Authority** accreditata.

SAFE effettua i seguenti trattamenti sui singoli documenti da giornalizzare:

- memorizzazione di una copia integrale del documento in una apposita tabella di db Oracle (tabella 1);
- memorizzazione dei metadati, associati al documento in una differente tabella di db Oracle (tabella 2) che costituisce l'indice ricercabile della registrazione.

In differita sono generati specifici documenti di giornalizzazione che aggregano i riferimenti ad uno o più documenti, afferenti ad un determinato intervallo di tempo dell'ordine di minuti e per ciascuno di questi il riferimento alla posizione nella tabella 1 e nella tabella 2. Inoltre è registrato il valore dell'Hash di ciascuno dei documenti referenziati e dei riferimenti di tabella 2.

Il documento di giornalizzazione viene marcato temporalmente al fine di garantirne la sequenzialità, la collocazione nel tempo e l'integrità della registrazione.

I documenti di giornalizzazione sono salvati in apposite tabelle del db oracle.



## 4 TRANSIZIONE DELLE CREDENZIALI VERSO SPID

In merito al processo di transizione delle credenziali pregresse verso SPID, si farà riferimento alla Determinazione 27/2108 di AgID, del 7 febbraio 2018.

In particolare, **si ritiene di poter adottare la “Procedura per la richiesta di rilascio di Identità SPID da Identità pregressa”**.

## 5 RIFERIMENTI NORMATIVI

- [1] Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000 e s.m.i., **“Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”** denominato anche **“TUDA”**.  
[www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:2000-12-28:445!vig=](http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:2000-12-28:445!vig=)
- [2] Decreto Legislativo n. 196 del 30 giugno 2003 e s.m.i., **“Codice in materia di protezione dei dati personali”** denominato anche **“Codice Privacy”**.  
[www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30:196!vig=](http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30:196!vig=)
- [3] Decreto Legislativo n. 82 del 7 marzo 2005 **“Codice dell’Amministrazione Digitale”** c.d. CAD  
<http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07:82!vig=>
- [4] DPCM 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014  
[http://www.agid.gov.it/sites/default/files/leggi\\_decreti\\_direttive/dpcm\\_24\\_ottobre\\_2014a.pdf](http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_24_ottobre_2014a.pdf)
- [5] **Determinazione AgID n. 44/2015, contenente i quattro regolamenti previsti dall’articolo 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014:**
  - 1. Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2)
  - 2. Regolamento recante le regole tecniche (articolo 4, comma 2)
  - 3. **Regolamento recante le modalità per l’accreditamento e la vigilanza dei gestori dell’identità digitale (articolo 1, comma 1, lettera I)**
  - 4. **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)**[http://www.agid.gov.it/sites/default/files/circolari/determinazione\\_dg\\_n. 44 - 28 luglio 2015 - emanazione regolamenti spid 0.pdf](http://www.agid.gov.it/sites/default/files/circolari/determinazione_dg_n.44_28_luglio_2015_-_emanazione_regolamenti_spid_0.pdf)
- [6] **Determinazione N. 32/2016 del 16 febbraio 2016 del Direttore Generale di AgID contenente 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**  
[http://www.agid.gov.it/sites/default/files/circolari/32 - dt dg n. 32 - 16 feb 2016 - convenzione spid-idp ver.2.0.pdf](http://www.agid.gov.it/sites/default/files/circolari/32_-_dt_dg_n.32_-_16_feb_2016_-_convenzione_spid-idp_ver.2.0.pdf)
- [7] **Determinazione N. 27/2018 del 7 febbraio 2018 del Direttore Generale di AgID contenente le procedure per il riuso delle identità pregresse**  
[http://www.agid.gov.it/sites/default/files/circolari/27 - dt dg n. 27 - 7 feb 2018 - approvazione procedure acquisizione identita pregressesp\\_id 20180206.pdf](http://www.agid.gov.it/sites/default/files/circolari/27_-_dt_dg_n.27_-_7_feb_2018_-_approvazione_procedure_acquisizione_identita_pregressesp_id_20180206.pdf)

## 6 RIFERIMENTI DOCUMENTALI

[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>

## 7 ALLEGATI

### 7.1 ALLEGATO 1 Richiesta delle credenziali per l'accesso ai servizi on line e attivazione dei servizi socio-sanitari



Regione Lombardia

**RICHIESTA DELLE CREDENZIALI**

**PER L'ACCESSO AI SERVIZI ON LINE MESSI A DISPOSIZIONE DA REGIONE LOMBARDIA**

---

Io sottoscritto/a \_\_\_\_\_

Sesso ☐ M ☐ F      Nato/a il \_\_\_\_\_

Codice fiscale

con la presente dichiaro:

- di richiedere le credenziali per l'accesso ai servizi *on line* messi a disposizione da Regione Lombardia;
- di prestare il consenso al trattamento dei miei dati personali, per la gestione delle credenziali di cui sopra, consapevole che i dati da me forniti verranno trattati secondo le modalità previste dall'Informativa sotto riportata.

Numero di telefono abilitato:

\_\_\_\_\_

*Data*

\_\_\_\_\_

*Firma dell'interessato*

**INFORMATIVA RELATIVA AL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO PER LA GESTIONE DELLE CREDENZIALI PER L'ACCESSO AI SERVIZI ON LINE**

(ART. 13 D. LGS. N. 196/2003 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI")

I dati da Lei forniti, verranno trattati esclusivamente per finalità strettamente connesse e strumentali alla gestione:

- a) delle credenziali per l'accesso ai servizi *on-line* messi a disposizione, quali l'attivazione dei codici di accesso ai servizi e l'invio di notizie sul funzionamento dei servizi stessi.

Il consenso al trattamento dei dati personali è da Lei prestato, in quanto interessato al quale i dati si riferiscono. Se Lei è minorenne o sotto tutela, sono i soggetti che hanno la rappresentanza legale a esprimere il consenso al trattamento dei dati.

Il trattamento avverrà con l'ausilio di supporti informatici e cartacei nel rispetto delle regole di riservatezza e di sicurezza previste dalla vigente normativa sulla protezione dei dati personali. Il trattamento attiene ai dati anagrafici e ai recapiti telematici (recapito di telefonia, indirizzo di posta elettronica) da Lei forniti. I dati trattati potranno essere comunicati esclusivamente in adempimento di un obbligo previsto dalla legge. I dati non verranno in alcun modo diffusi.

Il conferimento dei dati personali:

- non è di natura obbligatoria per il trattamento di cui alla finalità a), il rifiuto al conferimento comporta l'impossibilità del Titolare del trattamento a prestare il servizio di gestione delle credenziali per l'accesso ai servizi *on-line*.

Titolare del Trattamento dei dati necessari alla gestione delle credenziali per l'accesso ai servizi *on-line* messi a disposizione è Regione Lombardia.

Per un maggior dettaglio su tali servizi e sui relativi trattamenti effettuati, si rimanda al sito web [www.crs.regione.lombardia.it](http://www.crs.regione.lombardia.it).

Responsabili del trattamento sono Lombardia Informatica S.p.A. e altri soggetti designati dai Titolari.

L'elenco completo dei Titolari e dei Responsabili dei trattamenti relativi ai servizi messi a disposizione è disponibile sul sito web [www.crs.regione.lombardia.it](http://www.crs.regione.lombardia.it).

Il Titolare del trattamento dei dati effettuerà indagini di rilevamento della qualità e dell'utilizzo dei servizi *on line*, avvalendosi dei recapiti da Lei forniti. La partecipazione all'indagine non è obbligatoria e la raccolta delle informazioni è finalizzata esclusivamente ad elaborazioni statistiche. I risultati delle indagini potranno essere diffusi soltanto in forma anonima.

**INFORMAZIONI PRATICHE:** Lei potrà far valere i Suoi diritti di cui all'art. 7 del Codice in materia di protezione dei dati personali (es. aggiornamento, rettificazione, integrazione, cancellazione dei propri dati, ecc.), rivolgendo istanza al Titolare tramite i punti abilitati al servizio di attivazione delle credenziali.

**PER ULTERIORI INFORMAZIONI:**

contatti il numero verde della Carta Regionale dei Servizi.



## 7.2 ALLEGATO 2 Modulo prima parte della password



### Come effettuare l'accesso ai Servizi online

Data gg/mm/aaaa

Gentile <NOME COGNOME>,

sul sito dei Servizi-Socio Sanitari online di Regione Lombardia puoi ritirare i referti dal tuo Fascicolo Sanitario Elettronico, prenotare le visite sanitarie e gli esami specialistici, scoprire i canali di pagamento abilitati, cambiare il medico di famiglia, consultare l'elenco delle tue esenzioni, autocertificare le tue esenzioni per reddito, richiedere il PIN della Tessera Sanitaria, consultare il budget celiachia, conoscere le app SALUTILE e molto altro ancora...

Per effettuare il **primo accesso** ai Servizi Socio-Sanitari online di Regione Lombardia segui questi passaggi.

- 1 Collegati al sito **www.crs.regione.lombardia.it/sanita**.
- 2 Clicca sul tasto **ACCEDI**.
- 3 Inserisci i dati nella sezione "Autenticazione con userid, password e codice usa e getta".
  - **Numero di identificazione della tessera**  
Composto dalle ultime 10 cifre del numero di identificazione presente sul retro della Tessera Sanitaria Carta Nazionale dei Servizi;
  - **Password**  
È provvisoria ed è costituita da due parti ognuna di cinque caratteri.  
La prima è **XXXXX** mentre la seconda ti è stata inviata via SMS quando hai ritirato questo foglio.  
L'unione delle due parti deve costituire una password unica di 10 caratteri.
- 4 A questo punto ti verrà chiesto di impostare una **password personale** in sostituzione di quella provvisoria. Confermandola, riceverai un SMS con il **codice usa e getta** che devi inserire per concludere il primo accesso ai Servizi Socio-Sanitari online.



Ti ricordiamo che è necessario seguire la procedura sopra indicata soltanto la prima volta che accedi ai Servizi Socio-Sanitari online di Regione Lombardia. Per gli accessi successivi invece dovrai inserire:

- il tuo **numero di identificazione della tessera** (3);
- la **password personale** da te scelta (4);
- il **codice usa e getta** che riceverai via SMS ad ogni accesso.



Ti confermiamo che è stato acquisito il tuo consenso al trattamento dei dati personali secondo le modalità indicate nell'informativa relativa ai trattamenti dei dati per la gestione delle credenziali.



[www.crs.regione.lombardia.it/sanita](http://www.crs.regione.lombardia.it/sanita)



### 7.3 ALLEGATO 3 Password policy fornita al cittadino

Per definire la tua password personale dovrai rispettare le seguenti regole:

- la lunghezza dovrà essere di otto caratteri;
- nella tua password dovranno esserci obbligatoriamente:
  - caratteri maiuscoli e minuscoli;
  - uno o più caratteri numerici;
  - almeno un carattere speciale ad es #, \$,% ecc.
- non inserire nella password più di due caratteri identici consecutivi;
- non utilizzare come password dati comuni (es. Codice fiscale, numero di identificazione della carta CNS, ecc..);
- non potrai riutilizzare una password prima di 5 variazioni

Ti ricordiamo che la tua password personale, per motivi di sicurezza, dovrà essere cambiata ogni 3 mesi.

#### 7.4 ALLEGATO 4 Processo di produzione delle attestazioni GASS

La procedura di archiviazione tramite SAFE delle attestazioni firmate digitalmente dai funzionari delle aziende Sanitarie sta evidenziando come una discreta percentuale sia stata firmata con un certificato che alla data odierna è scaduto o revocato.

Di seguito si descrive il processo di firma messo in atto al fine di dimostrare che le condizioni in cui il documento è stato firmato sono tali per cui si possa ritenere valida la firma.

**Il processo con il quale sono prodotte le “attestazioni di rilascio di credenziali GASS” prevede che:**

1. **l'operatore della A.S. è dotato di una “carta operatore” contenente un certificato di firma digitale** (emesso da una CA accreditata) ed un certificato di autenticazione; le date di scadenza dei due certificati sono allineate in fase di produzione dei certificati;
2. **l'operatore della A.S. , per poter utilizzare il servizio GASS, deve eseguire il SIGN-ON** sulla Extranet SISS; in fase di SIGN-ON si verifica:
  - a. che il certificato di autenticazione si valido (non scaduto e non revocato);
  - b. **che l'orologio della postazione di lavoro sia allineato con l'orologio del sistema di SSO**, con uno scostamento massimo tollerato di 15 minuti, pena il rifiuto del Logon al SISS (la sessione di Logon al SISS ha una durata massima di 8 ore);
3. **l'applicativo del servizio GASS appone la firma digitale sul documento informatico** utilizzando il certificato di firma digitale presente sulla carta operatore, previa verifica che il certificato non sia scaduto, il **Signing Time** viene impostato con data/ora della postazione di lavoro;
4. il documento informatico firmato digitalmente viene trasmesso alla Porta Applicativa dei Domini Centrali del SISS, la quale verifica la validità della firma digitale (sia la scadenza che la revoca del certificato); in caso di mancata verifica viene rifiutata la registrazione della nuova utenza.

**L'insieme delle misure tecniche adottate assicura che la firma sia apposta, ed il documento acquisito, durante il periodo di validità del certificato qualificato, inoltre il **Signing Time** inserito durante la firma è ragionevolmente certo che corrispondesse all'ora effettiva di apposizione.**