Linee Guida per la realizzazione di un modello di R.A.O. pubblico

Versione 1.0 - novembre 2019

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Versione	Data	Determinazione	Tipologia modifica
1.0	Novembre 2019		Prima emanazione

Sommario

Capitolo 1 Introduzione 4
1.1 Scopo 4
1.2 Struttura 4
1.3 Gruppo di lavoro 4
1.4 Soggetti destinatari 5
Capitolo 2 Riferimenti e sigle 6
2.1 Riferimenti Normativi 6
2.2 Termini e definizioni 6
Capitolo 3 8
3.1 Comunicazione all'Agenzia 8
3.2 Modalità di riconoscimento 8
3.3 Dati dell'utente 9
3.4 Sistema 9
3.5 Processo di riconoscimento 10
3.6 Modelli di riferimento 11
3.7 Rilascio dell'identità digitale da parte dell'IdP 11
3.8 Verifiche e rilascio dell'identità 11
3.9 Responsabilità R.A.O. pubblico 12
3.10 Responsabilità IdP 12
3.11 Generazione della *passphrase* 12
3.12 Sigillo elettronico 13

Capitolo 1
Introduzione

1.1 Scopo

Le presenti Linee Guida, sono emesse ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (di seguito CAD) e ai sensi dell'articolo 3, comma 2, del DPCM 24 ottobre 2014.

Obiettivo di queste Linee Guida è quello di permettere alle PA di effettuare l'identificazione delle persone fisiche, attività propedeutica al rilascio dell'identità digitale SPID da parte degli Identity Provider accreditati.

Le presenti Linee Guida nascono dall'esigenza rappresentata dalle pubbliche amministrazioni interessate di incentivare l'uso di SPID per l'identificazione degli utenti dei propri servizi digitali. Le Linee Guida possono trovare applicazione nel processo di rilascio dei documenti di riconoscimento.

1.2 Struttura

Le presenti Linee Guida prevedono l'applicazione dei seguenti documenti tecnici che saranno pubblicati nel sito istituzionale dell'Agenzia:

- *Token* R.A.O. Pubblico;
- Tabella messaggi *token* R.A.O. pubblico inviati dall'IdP.

1.3 Gruppo di lavoro

La redazione del documento è stata curata dal gruppo di lavoro composto da:

- **Agenzia per l'Italia Digitale**
- **Aruba S.p.A.**
- **CSI Piemonte**
- **Infocert S.p.A.**
- **Lepida S.p.A.**
- **Poste Italiane S.p.A.**

- **Provincia Autonoma di Bolzano**
- **Provincia Autonoma di Trento**
- **Regione Piemonte**
- **Register.it S.p.A.**
- **Sielte S.p.A.**
- **TI Trust Technologies S.r.l.**
- **Team per la Trasformazione Digitale**

1.4 Soggetti destinatari

Le presenti linee guida sono applicabili ai:

a) soggetti di cui all'art. 2, comma 2, lett. a) del CAD che intendono, con proprie risorse, effettuare l'identificazione della persona fisica, di seguito utente, in qualità di R.A.O. pubblico del sistema SPID*;*

b) gestori di identità digitale, di seguito IdP, che intendono avvalersi delle procedure di identificazione effettuate dai soggetti di cui al punto precedente.

Capitolo 2

Riferimenti e sigle

2.1 Riferimenti Normativi

- **[Reg. UE n.910/2014]** Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- **[D.Lgs. 82/2005]** Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale";
- **[DPCM 24 ottobre 2014]** recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.";
- **[Regolamento recante le regole tecniche]** (articolo 4, comma 2, DPCM 24 ottobre 2014) e s.m.i.;
- **[Regolamento recante le modalità attuative per la realizzazione dello SPID]** (articolo 4, comma 2, DPCM 24 ottobre 2014) e s.m.i.

2.2 Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati nella presente Linee Guida:

- **[Agenzia]** Agenzia per l'Italia Digitale
- **[AGID]** Agenzia per l'Italia Digitale
- **[Brochure]** documenti realizzati ed aggiornati dagli IdP, reperibili sul sito ufficiale SPID che spiegano brevemente la *user experience* e le caratteristiche del servizio offerto.
- **[CAD]** Codice Amministrazione Digitale, D.Lgs 7 marzo 2005, n. 82
- **[IdP]** Identity Provider o gestore di identità digitale SPID
- **[Operatore]** pubblico ufficiale espressamente incaricato dal R.A.O. pubblico per l'espletamento delle attività di identificazione di cui al par. 3.2

- **[R.A.O.]** Registration Authority Office: la Pubblica Amministrazione che svolge l'attività di verifica dell'identità personale dei cittadini al fine del rilascio dell'identità digitale SPID. Nel seguito *R.A.O. pubblico/i.*
- **[Sistema]** il sistema applicativo in uso dai R.A.O. pubblici, predisposto in conformità all'allegato "*Token* R.A.O. Pubblico", per la compilazione della scheda anagrafica, la formazione e trasmissione dei *token* sulla base dei modelli di riferimento di cui al par.3.6
- **[SPID]** Sistema Pubblico di Identità Digitale
- **[sub CA]** Subordinate certificate authority
- **[*Token*]** *Token* software che contengono i dati dell'utente di cui al par. 3.3 e sono formati in conformità all'allegato "*Token* R.A.O. Pubblico"

Capitolo 3

3.1 Comunicazione all'Agenzia

I soggetti di cui al par. 1.4 lett. a) presentano istanza all'Agenzia al fine di essere riconosciuti come R.A.O. pubblico del sistema SPID in conformità alle presenti Linee Guida, fornendo riferimenti utili agli IdP che intendono avvalersi di tali procedure di identificazione.

L'Agenzia informa gli IdP in merito ai soggetti che hanno richiesto il riconoscimento come come R.A.O. pubblico del sistema SPID.

Gli IdP informano l'Agenzia che intendono avvalersi delle procedure di identificazione effettuate dai R.A.O. pubblici del sistema SPID.

L'Agenzia rende disponibile ad entrambi i predetti soggetti il certificato di sigillo elettronico di cui al par. 3.12.

3.2 Modalità di riconoscimento

L'operatore di un R.A.O. pubblico effettua l'identificazione dell'utente accertando l'identità del richiedente tramite la verifica di un documento di riconoscimento integro e in corso di validità rilasciato da un'Amministrazione dello Stato, munito di fotografia e firma autografa dello stesso e controlla la validità del codice fiscale verificando la tessera sanitaria anch'essa in corso di validità.

Il R.A.O. pubblico, considerata la formazione dei propri operatori, stabilisce quali documenti di riconoscimento accettare.

Se i documenti esibiti dal richiedente risultano carenti delle caratteristiche di cui sopra, deve esserne esclusa l'ammissibilità e il processo di iscrizione deve essere sospeso o bloccato fino all'esibizione di documenti validi e integri.

L'operatore effettuato il riconoscimento *de visu*, compila nel sistema di cui al par. 3.4 una scheda anagrafica con i dati dell'utente di cui al par. 3.3.

3.3 Dati dell'utente

I dati dell'utente sono composti obbligatoriamente da:

1. attributi identificativi SPID:
    - nome,
    - cognome,
    - luogo di nascita,
    - provincia di nascita,
    - data di nascita,
    - sesso,
    - codice fiscale,
    - estremi (tipologia, numero, autorità rilasciante, scadenza) del documento d'identità in corso di validità utilizzato ai fini dell'identificazione.
2. attributi secondari SPID:
    - numero di telefonia mobile,
    - indirizzo di posta elettronica,
    - domicilio fisico,
    - se disponibile, domicilio digitale (casella PEC).
3. ulteriori informazioni anagrafiche:
    - numero seriale della Tessera Sanitaria in corso di validità e relativa scadenza ovvero di quanto previsto dall'Avviso AGID nr. 7 del 25 ottobre 2017;
    - nazione di nascita;
    - nazione del domicilio fisico.

3.4 Sistema

Il sistema è una piattaforma che consente di gestire il processo di verifica dell'identità dell'utente necessario ai fini del rilascio dell'identità digitale attraverso l'inserimento dei dati dell'utente di cui al par. 3.3. e la generazione del *token* necessario per ottenere l'identità digitale da parte dell'IdP prescelto dall'utente.

Il sistema:

- Permette all'operatore di compilare e salvare i dati dell'utente di cui al par. 3.3 nella scheda anagrafica dell'utente;

- Garantisce la collocazione temporale della compilazione della scheda anagrafica;
- Permette la generazione di una passphrase secondo le modalità indicate al par. 3.11;
- Consente la creazione delle diverse tipologie di *token* come descritto nel processo di cui al par. 3.5*;*
- Prevede l'apposizione del sigillo elettronico di cui al par. 3.12;
- Assicura l'individuazione dell'operatore;
- Garantisce la sicurezza dei dati gestiti.

Il sistema può essere realizzato a cura del R.A.O. pubblico o dell'IdP. Qualora entrambi i soggetti dispongano di tale sistema la scelta su quale sistema adottare spetta al R.A.O. pubblico.

3.5 Processo di riconoscimento

L'operatore compila nel sistema una scheda anagrafica con i dati dell'utente di cui al par. 3.3.

Il sistema:

1. salva la scheda anagrafica nel formato stabilito di interscambio generando il *token in chiaro*;
2. genera una *passphrase* secondo le modalità indicate al par. 3.11 e la usa per cifrare il *token in chiaro* ottenendo il *token cifrato;*
3. associa il codice fiscale dell'utente al *token cifrato* e restituisce il *token completo;*
4. appone il sigillo elettronico, di cui al par. 3.12, del R.A.O. pubblico al *token completo* ed ottiene il *token sigillato*.

A seguito della trasmissione del *token sigillato*, effettuata in base ai modelli di riferimento di cui al par. 3.6, l'operatore consegna all'utente metà della *passphrase* in modalità cartacea e metà viene inviata all'indirizzo email fornito dall'utente unitamente alle indicazioni per consultare le brochure, realizzate ed aggiornate dagli IdP, reperibili sul sito ufficiale SPID.

L'operatore informa l'utente che il *token sigillato* può essere utilizzato entro e non oltre 30 giorni.

3.6 Modelli di riferimento

Sono previsti due modelli di riferimento che i R.A.O. pubblici possono mettere a disposizione dell'utente. Il R.A.O. pubblico è libero di scegliere se rendere disponibile uno o entrambi i modelli.

Modelli:

a) L'operatore informa l'utente della possibilità di scegliere il proprio IdP a sportello, in questo caso il *token sigillato* è inviato all'IdP prescelto;
b) il *token sigillato* è inviato all'utente via email all'indirizzo di posta elettronica indicato.

3.7 Rilascio dell'identità digitale da parte dell'IdP

La modalità di rilascio dell'identità digitale dipende dal modello usato (cfr. par 3.6).

L'utente si collega al sito dell'IdP e seleziona la modalità di rilascio con "identificazione tramite P.A.".

Nel caso in cui sia applicabile il modello di riferimento di cui alla lett. a) del par. 3.6, l'utente immette il proprio codice fiscale per permettere all'IdP di recuperare il proprio *token sigillato*.

Nel caso in cui sia applicabile il modello di riferimento di cui alla lett. b) del par. 3.6, l'utente esegue l'upload del proprio *token sigillato*.

L'IdP verifica sigillo e periodo di validità del *token sigillato*. L'IdP richiede l'inserimento della *passphrase* per decifrare il *token cifrato*. Superati i 5 tentativi errati di inserimento della *passphrase* il *token* non è più accettato dall'IdP.

L'IdP estrae i dati dell'utente di cui al par. 3.3, ed effettua la verifica dell'effettivo possesso del cellulare indicato da parte dell'utente.

3.8 Verifiche e rilascio dell'identità

L'IdP utilizza i dati dell'utente di cui al par. 3.3 per compilare la scheda anagrafica collegata all'identità ed effettua le verifiche previste dalla normativa vigente in materia di rilascio dell'identità digitale SPID al netto di quanto eventualmente già verificato dal R.A.O. pubblico.

L'IdP rilascia l'identità elettronica ai sensi dell'art. 7, comma 2, lett. b) del DPCM 24 ottobre 2014 e s.m.i.

Ogni IdP rilascia l'identità SPID secondo le proprie modalità.

3.9 Responsabilità R.A.O. pubblico

I R.A.O. pubblici si assumono la responsabilità della corretta verifica dell'identità personale dell'utente e sono tenuti a mantenere le evidenze per individuare il singolo operatore che ha effettuato il riconoscimento dell'utente per il periodo di cui all'art. 36, comma 6, del DPCM 22 febbraio 2013.

I R.A.O. pubblici si impegnano a formare adeguatamente gli operatori incaricati alla verifica dell'identità degli utenti, fornendo agli stessi ogni informazione in merito alle procedure applicative e alle responsabilità di natura civile e penale nelle quali potrebbero incorrere nello svolgimento di tale attività.

3.10 Responsabilità IdP

L'IdP deve porre in essere tutte le attività necessarie al fine di interoperare con il sistema di cui al par. 3.4.

L'IdP che rilascia l'identità deve mantenere, per il periodo di cui all'art. 36, comma 6, del DPCM 22 febbraio 2013, evidenze atte a dimostrare che la singola identità è stata rilasciata sulla base dell'identificazione di cui al par. 3.7.

L'IdP può essere responsabile o corresponsabile dell'incorretto rilascio di un'identità digitale se non ha correttamente ottemperato alle verifiche di cui al par. 3.8.

3.11 Generazione della *passphrase*

La lunghezza della *passphrase* è di 12 caratteri generati in maniera casuale e deve contenere:

- Almeno una lettera maiuscola;
- Almeno una lettera minuscola;
- Almeno un carattere numerico;
- Almeno un carattere speciale tra quelli elencati: ! $? # = * + - . :

Sono esclusi i caratteri confondibili come i, l, 1, L, o, 0, O.

Ai fini del processo di cui al par. 3.5 la *passphrase* è divisa in due parti da 6 caratteri ciascuno.

3.12 Sigillo elettronico

L'Agenzia emette due sub CA dedicate rispettivamente ai soggetti individuati come R.A.O. pubblici e come IdP, utili alla generazione dei certificati dei sigilli elettronici.

Detti certificati sono caratterizzati dalla presenza dei seguenti OID registrati dall'Agenzia (OID 1.3.76.16):

- 1.3.76.16.4.1 per i certificati dei sigilli elettronici degli IdP;
- 1.3.76.16.4.5 per i certificati dei sigilli elettronici dei R.A.O. pubblici;
- 1.3.76.16.4.12 per entrambe i certificati.

Tali sigilli sono utilizzati dal R.A.O. e dall'IdP per l'instaurazione di un canale di comunicazione tra i predetti soggetti, dal R.A.O. anche per sigillare il *token completo*.

Al fine dell'emissione dei suddetti certificati, i R.A.O. pubblici e gli IdP inviano ad AGID una richiesta di certificazione in formato PKCS#10 basata su una coppia di chiavi RSA con lunghezza di almeno 2048 bit. L'AGID può, con un apposito avviso, modificare detti requisiti.