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

***Release bozza***

**AGID**

**07 ago 2019**

# Indice

**consultation**

La consultazione pubblica relativa alle Linee Guida per la realizzazione di un modello di R.A.O. pubblico è attiva dal **7 agosto** al **6 settembre 2019**.

CAPITOLO 1

# Le Linee Guida

## 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).

## 1.2 Struttura

Le presenti Linee Guida sono integrate dall'Allegato Tecnico:

- *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
- **[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
- **[R.A.O.]** Registration Authority Office

- **[Sistema]** il sistema applicativo in uso dai RAO 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]** I *token* 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

# Modello di R.A.O. pubblico

## 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.

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 un sigillo elettronico di cui al par. 3.12.

## 3.2 Modalità di riconoscimento

L'operatore di un R.A.O. pubblico deve verificare l'identità personale dell'utente tramite un documento d'identità valido e, in qualità di pubblico ufficiale, è esonerato dall'acquisizione dell'immagine fotostatica del documento stesso.

Tali verifiche sono effettuate con le modalità e i controlli previsti dalla normativa vigente in materia di rilascio dell'identità digitale della persona fisica ai sensi dell'art. 7, comma 2, lett. a) del DPCM 24 ottobre 2014 e s.m.i..

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 da:

1. attributi identificativi SPID:

- nome,

- cognome,
- luogo di nascita,
- provincia di nascita,
- data di nascita,
- sesso,
- codice fiscale,
- estremi del documento d'identità utilizzato ai fini dell'identificazione in corso di validità.

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 o del tesserino del Codice Fiscale in corso di validità;
- nazione di nascita;
- nazione del domicilio fisico.

## 3.4 Sistema

L'operatore compila la scheda anagrafica dell'utente nel sistema.

Il sistema garantisce di collocare temporalmente la compilazione della scheda anagrafica e di individuare l'operatore.

## 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 di interscambio concordato generando il *token in chiaro*;
2. genera una *passphrase* secondo le modalità indicate al par. 3.11 e cifra 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.

- a) L'operatore può informare l'utente della possibilità di scegliere il proprio IdP a sportello, in questo caso il *token sigillato* è inviato all'IdP prescelto;
- b) In mancanza della predetta possibilità o in caso di mancata scelta da parte dell'utente, il *token sigillato* è inviato all'utente via email all'indirizzo di posta elettronica fornito.

## 3.7 Rilascio dell'identità digitale da parte dell'IdP

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.

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 nel tempo le evidenze per individuare il singolo operatore che ha effettuato il riconoscimento dell'utente.

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 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.

L'IdP è esonerato dall'obbligo previsto dall'art. 7, comma 5, del DPCM 24 ottobre 2014.

## 3.11 Generazione della *passphrase*

La lunghezza della *passphrase* è di 12 caratteri generati in maniera casuale e che 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 per i soggetti individuati come R.A.O. pubblici e per gli 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):

- 1.3.76.16.4.20 per i certificati dei sigilli elettronici degli IdP;
- 1.3.76.16.4.21 per i certificati dei sigilli elettronici dei R.A.O.

pubblici.

Tali sigilli sono utilizzati sia per l'instaurazione di un canale di comunicazione tra i predetti soggetti che per sigillare il *token completo*.

# CAPITOLO 4

# Token R.A.O.Pubblico

## 4.1 Obiettivi

Definizione di uno standard condiviso, chiaro e sicuro per il formato dei dati utili al rilascio di una identità SPID a fronte di un avvenuto riconoscimento del futuro titolare dell'identità presso uffici pubblici.

## 4.2 ICRequestData

L'ICRequestData (Identity Creation Request Data) è l'oggetto contenente i dati relativi all'utente che ha eseguito la sua identificazione tramite R.A.O. pubblico e necessari alla generazione di una identità digitale SPID presso uno degli Identity Provider SPID che aderiscono al Modello R.A.O. pubblico.

Tali dati sono rappresentati tramite un documento definito nel formato JSON (JavaScript Object Notation), il cui schema è riportato nell'Appendice 4.10.1 e di cui un esempio è riportato nell'Esempio 1.

In particolare, l'ICRequestData riporta i seguenti dati:

- **info**: elemento che contiene le seguenti informazioni:
  - **id**: codice identificativo unico della richiesta all'interno di uno specifico R.A.O. pubblico.
  - **issueInstant**: istante di generazione della richiesta, codificata secondo il formato UTC.
  - **issuer:** elemento che consente l'identificazione del R.A.O. pubblico emittente le richieste, codificato come:
    - **issuerCode**: P.A. agente come R.A.O. pubblico, identificata tramite il proprio codice IPA.
    - **issuerInternalReference** *(opzionale)* **:** dato avente significato solo per il R.A.O. pubblico e da esso definito liberamente, utile per eventuali verifiche in caso di necessità. Esso non deve essere più lungo di 32 caratteri.
- **electronicIdentification**: elemento che contiene le seguenti informazioni del documento presentato per l'identificazione elettronica:

  - **identificationType**: indica la tipologia del documento. I valori ammessi sono «TS» e "CF", rispettivamente relativi alla Tessera Sanitaria e al Tessera del Codice Fiscale.
  - **identificationSerialCode**: contiene il seriale della tessera utilizzata per l'identificazione.

- **spidAttributes:** elemento che contiene i seguenti dati dell'utente identificato dal R.A.O. pubblico:
  - **mandatoryAttributes:** contiene i seguenti dati necessari per la generazione dell'identità digitale SPID per una persona fisica:
    * **name:** Nome della persona fisica, codificato come previsto dalla Tabella Attributi SPID
    * **familyName:** Cognome della persona fisica, codificato come previsto dalla Tabella Attributi SPID
    * **placeOfBirth:** Luogo di nascita della persona fisica, codificato come previsto dalla Tabella Attributi SPID
    * **countyOfBirth:** Provincia di nascita della persona fisica, codificata come previsto dalla Tabella Attributi SPID
    * **nationOfBirth**: Nazione di nascita della persona fisica, codificata con il codice catastale della nazione definito dall'ISTAT. Ad esempio, nel caso dell'Italia indicare Z000, se invece la nazione è sconosciuta indicare Z998.
    * **dateOfBirth:** Data di nascita della persona fisica, codificata come previsto dalla Tabella Attributi SPID.
    * **gender:** Sesso della persona fisica, codificata come previsto dalla Tabella Attributi SPID.
    * **fiscalNumber:** Codice Fiscale della persona fisica, codificata come previsto dalla Tabella Attributi SPID.
    * **email:** Indirizzo di posta elettronica, codificata come previsto dalla Tabella Attributi SPID.
    * **idCard:** Dati relativi al documento di identità fornito dalla persona fisica al momento della sua identificazione presso il R.A.O. pubblico, indicati come segue:
      · **idCardType:** Tipo del documento, codificato secondo i valori ammessi indicati nella Tabella Attributi SPID.
      · **idCardDocNumber:** Numero del documento.
      · **idCardIssuer:** Nome dell'ente emettitore del documento, codificata come previsto dalla Tabella Attributi SPID.
      · **idCardIssueDate:** data di rilascio del documento, codificata come previsto dalla Tabella Attributi SPID.
      · **idCardExpirationDate:** data di scadenza del documento, codificata come previsto dalla Tabella Attributi SPID.
    * **mobilePhone**: numero di cellulare, codificato come segue:
      · **countryCallingCode**: Prefisso internazionale dell'operatore, codificato secondo standard ITU (ad esempio, +39).
      · **phoneNumber**: numero di telefonia mobile, codificato come stringa numerica senza spazi intermedi.
    * **address**: Domicilio fisico della persona fisica, codificato come segue:
      · **type**: Tipologia del luogo (via, viale, piazza . . . );
      · **addressName**: Nome del luogo
      · **addressNumber**: Numero civico

- **postalCode**: Codice Postale del luogo
- **municipality**: Comune a cui è afferente il luogo, codificato tramite codice catastale (Codice Belfiore).
- **county**: Provincia a cui è afferente il luogo, codificata tramite sigla.
- **nation**: Nazione a cui è afferente il luogo, codificata con il codice catastale della nazione definito dall'ISTAT. Ad esempio, nel caso dell'Italia indicare Z000, se invece la nazione è sconosciuta indicare Z998.

– **optionalAttributes** *(opzionale)* **:** ulteriore informazione che può essere inclusa all'interno dell'identità digitale SPID per una persona fisica:

* **digitalAddress**: Domicilio Digitale.

**Esempio 1: Esempio di ICRequestData**

```
{
 "info": {
  "id": "123456789",
  "issueInstant": "2019-05-27T15:49:53.735Z",
  "issuer": {
    "issuerCode": "c_h501",
    "issuerInternalReference": "03Ab!34T"
  }
 },
 "electronicIdentification": {
  "identificationType": "TS",
  "identificationSerialCode": "123456789"
 },
 "spidAttributes": {
  "mandatoryAttributes": {
   "name": "Giovanni Mario",
   "familyName": "Rossi",
   "placeOfBirth": "F205",
   "countyOfBirth": "MI",
   "nationOfBirth": "Z000",
   "dateOfBirth": "2000-09-24",
   "gender": "M",
   "fiscalNumber": "TINIT-RSSGNN00P24F205L",
   "email": "me@me.com",
   "idCard": {
    "idCardType": "CartaIdentità",
    "idCardDocNumber": "AS09452389",
    "idCardIssuer": "c_h501",
    "idCardIssueDate": "2013-01-02",
    "idCardExpirationDate": "2023-09-24"
   },
   "mobilePhone": {
    "countryCallingCode": "+39",
    "phoneNumber": "3471234567"
   },
   "address": {
    "addressType": "Largo",
    "addressName": "Augusto",
    "addressNumber": "3/b",
    "postalCode": "00129",
    "municipality": "H501",
    "county": "RM",
```

(continues on next page)

(continua dalla pagina precedente)

```
    "nation": "Z000"
   }
  },
  "optionalAttributes": {
   "digitalAddress": "me@meypecprovider.com"
  }
 }
}
```

## 4.3 *Token Completo*

Il *token completo* è formalizzato come un JWT (**JSON Web token),** generato a partire da un payload, definito di seguito e sigillato secondo le indicazioni del paragrafo 4.5.

Il *token* ha validità di 30 giorni, periodo in cui l'utente, a cui fanno riferimento le informazioni contenute nel *token*, può utilizzarlo per ottenere un'identità digitale. Trascorso tale termine, il *token* non è più usabile e, nel caso previsto al punto a) del paragrafo 3.6 delle Linee Guida, l'Identity Provider provvede alla sua cancellazione.

L'header del *token* JWT è costituito dalle seguenti informazioni:

- **typ**: parametro valorizzato come "JWT".
- **alg:** parametro che identifica l'algoritmo crittografico del sigillo elettronico utilizzato.
- **x5c**: parametro contenente il certificato o la catena dei certificati, in formato X.509, corrispondente alla chiave pubblica del certificato di sigillo elettronico utilizzato. Il certificato o la catena dei certificati sono codificati come array JSON di stringhe corrispondenti ai valori dei certificati in formato DER. Ogni stringa nell'array è codificata in Base64. Il certificato contenente la chiave pubblica del sigillo utilizzato per firmare il *token* deve essere la prima stringa dell'array. Il certificato di sigillo elettronico può essere lo stesso eventualmente utilizzato dal client per il protocollo di comunicazione HTTPS.

Il payload è rappresentato da un documento definito nel formato JSON (JavaScript Object Notation), il cui schema è riportato nell'Appendice 4.10.2, contenente le seguenti informazioni:

- **iss:** corrispondente al valore degli elementi *issuerCode* e *issuerInternalReference***dell'elemento** *info* in ICRequestData codificati singolarmente in Base64 e concatenati tramite punto. Esempio: Base64(*issuerCode*). Base64(*issuerInternalReference*)
- **sub:** corrispondente al valore dell'elemento *id* dell'elemento *info* in ICRequestData
- **jti:** identificativo unico del *token*, generato come UUID.
- **aud:** valorizzato con l'entityID dell'IdP come indicato nel registro SPID nel caso previsto dal modello di riferimento di cui al paragrafo 3.6, lett. a) delle Linee Guida, mentre valorizzato come vuoto nel caso previsto dal modello di riferimento di cui al paragrafo 3.6, lett. b) delle Linee Guida.
- **iat:** istante di generazione della richiesta, codificata secondo il formato UTC. A partire da tale riferimento temporale vengono conteggiati i 30 giorni di validità del *token*. Deve corrispondere al valore dell'elemento *issueInstant* in ICRequestData.
- **exp:** tempo di fine validità del *token* calcolato come iat + 30 giorni.
- **fiscalNumber:** codice fiscale della persona fisica che ha eseguito la sua identificazione tramite R.A.O. pubblico.
- **encryptedData**: versione serializzata e cifrata dell'ICRequestData, secondo le specifiche indicate nel paragrafo 4.4

**Esempio 2: Esempio di Payload JSon**

```
{
 "iss": "Y19oNTAx.MDNBYiEzNFQ=",
 "sub": "123456789",
 "jti": "822e653a-d504-420c-9da3-609b329fc6b5",
 "aud": "www.idp.it",
 "iat": "2019-05-27T15:49:53.735Z",
 "exp": "2019-06-27T15:49:53.735Z",
 "fiscalNumber": "RSSGNN00P24F205L",
 "encryptedData":
↪"eyJhbGciOiJSUzI1NiIsImtpZCI6Ijc4YjRjZjIzNjU2ZGMzOTUzNjRmMWI2YzAyOTA3NjkxZjJjZGZmZTEifQ.
↪eyJpc3MiOiJhY2NvdW50cy5nb29nbGUuY29tIiwic3ViIjoiMTEwNTAyMjUxMTU4OTIwMTQ3NzMyIiwiYXpwIjoiODI1MjQ5OD
↪TVKv-pdyvk2gW8sGsCbsnkqsrS0T-
↪H00xnY6ETkIfgIxfotvFn5IwKm3xyBMpy0FFe0Rb5Ht8AEJV6PdWyxz8rMgX2HROWqSo_
↪RfEfUpBb4iOsq4W28KftW5H0IA44VmNZ6zU4YTqPSt4TPhyFC9fP2D_Hg7JQozpQRUfbWTJI"
}
```


## 4.4 Funzione di cifratura

Per la generazione dell'EncryptedData a partire dell'ICRequestData è utilizzato lo standard JWE (JSON Web Encryption).

In particolare, per la cifratura dell'ICRequestData viene utilizzato l'algoritmo di cifratura simmetrico HS256.

La passphrase di cifratura utilizzata è di 256 bit (32 byte), generata tramite funzione di hash crittografica SHA-256 a partire dalla passphrase fornita dall'utente in fase di richiesta di generazione della propria identità digitale.

## 4.5 Sigillo Elettronico

Il *token completo* è oggetto di un sigillo elettronico, basato su un certificato emesso da apposita sub CA generata dall'Agenzia.

## 4.6 Modello interscambio dati – modello a)

Nel caso previsto dal modello di riferimento di cui al paragrafo 3.6, lett. a) delle Linee Guida, al fine di consentire la comunicazione, da parte dei RAO verso gli IdP, del *token* definito nei paragrafi precedenti e la comunicazione, da parte degli IdP verso i RAO, del risultato dell'invio del predetto *token*, si definisce un modello di interscambio dati che prevede:

- Esposizione da parte dell'IdP di un opportuno Endpoint, espresso tramite URL HTTPS, avente i seguenti requisiti:
  1. **Algoritmo di cifratura:** il canale supporta esclusivamente gli algoritmi TLS 1.2 e/o TLS 1.3. Tutti gli altri algoritmi (ad es. SSL3, TLS 1.0) non sono supportati.
  2. **Cipher Suites:** il canale non supporta suite di cifratura anonime.
- Comunicazione fra R.A.O. pubblico ed IdP svolta attraverso API REST esposta dall'IdP (Vedi 7. API – modello a)) il cui accesso dovrà essere limitato ai R.A.O. pubblici, tramite la verifica dell'uso dei rispettivi sigilli del R.A.O. pubblico e dell'IdP per instaurare il canale TLS.

## 4.7 API – modello a)

In conformità con il modello di cui al paragrafo 4.6., gli IdP dovranno esporre un endpoint denominato **/raoic** (Registration Authority Office Identity Creation). La url completa dell'endpoint, esposta su dominio appartenente all'IdP, dovrà essere comunicato all'Agenzia e da quest'ultima pubblicata su apposito registro.

L'endpoint potrà ricevere solo richieste di tipo POST contenenti nel body il *token* JWT come indicato nel paragrafo 4.3. Ogni altro tipo di richiesta inviata tramite diverso binding causerà un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico).

A seguito della ricezione di un *token completo*, l'IdP effettua le verifiche di cui al nel paragrafo 4.9. Al completamento della verifica l'IdP genererà una response coerente con l'esito della verifica stessa.

Ogni response sarà restituita come oggetto JSON in formato JWT firmato indicante l'esito dell'invio e/o la causa del diniego. L'header del *token* JWT della response è costituito dalle seguenti informazioni:

- **typ**: parametro valorizzato come "JWT";
- **alg:** parametro che identifica l'algoritmo crittografico del sigillo elettronico utilizzato;
- **x5c**: parametro contenente il certificato o la catena dei certificati, in formato X.509, corrispondente alla chiave pubblica del certificato di sigillo elettronico dell'IdP. Il certificato o la catena dei certificati sono codificati come array JSON di stringhe corrispondenti ai valori dei certificati in formato DER. Ogni stringa nell'array è codificata in Base64. Il certificato contenente la chiave pubblica del sigillo utilizzato per firmare il *token* deve essere la prima stringa dell'array. Il certificato di sigillo elettronico può essere lo stesso eventualmente utilizzato dal client per il protocollo di comunicazione HTTPS.

Il payload della response è rappresentato da un documento definito nel formato JSON (JavaScript Object Notation), definito secondo lo schema riportato nell'Appendice 4.10.3:

- **iss:** corrispondente all'entityID dell'IdP, come indicato nel registro SPID;
- **sub:** corrispondente al valore dell'elemento *id* dell'elemento *info* in ICRequestData;
- **jti:** identificativo unico del *token*, generato come UUID;
- **aud:** corrispondente al valore *iss* contenuto nella request;
- **iat:** istante di generazione della response, codificata secondo il formato UTC;
- **responseCode:** codice dell'esito;
- **responseMessage:** messaggio relativo all'esito

**Esempio 3: Esempio di Payload del JWT della Response**

```
{
 "iss": "www.idp.it",
 "sub": "123456789",
 "jti": "a7388c12-ea4a-43fe-b5ad-befd4a9edf81",
 "aud": " Y19oNTAx.MDNBYiEzNFQ=",
 "iat": "2019-06-27T15:55:03.405Z",
 "responseCode": 2,
 "responseMessage": "Spiacenti, per questo utente risulta già rilasciata un'identità␣
↪digitale SPID"
}
```

## 4.8 Upload del Token Completo– modello b)

Nel caso previsto dal modello di riferimento di cui al paragrafo 3.6, lett. b) delle Linee Guida, gli IdP forniranno all'utente la possibilità presso il loro sito di selezionare la modalità di rilascio con "identificazione tramite P.A." e procedere all'upload del *token completo.*

A seguito della ricezione di un *token completo*, l'IdP effettua le verifiche di cui al nel paragrafo 4.9. Al completamento della verifica l'IdP notificherà all'utente un messaggio coerente con l'esito della verifica stessa.

## 4.9 Verifiche di validità del *Token Completo*

Alla ricezione del *token* l'IdP dovrà verificare che:

1. Il *token* ricevuto è conforme a quanto previsto dal paragrafo 4.3, in caso contrario verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico);
2. Il valore dell'algoritmo di firma indicato nel campo *alg* sia tra quelli previsti per i certificati emessi da sub CA dell'Agenzia. In caso contrario verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico);
3. Il certificato indicato nel campo *x5c* sia rilasciato da PKI dell'Agenzia e sia valido e non revocato. In caso contrario verrà generato un errore di tipo Unauthorized (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico);
4. Solo nel caso previsto dal modello di riferimento di cui al paragrafo 3.6, lett. a) delle Linee Guida, il valore indicato nel campo *aud* del body corrisponda al proprio entityID. In caso contrario verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico);
5. Il valore indicato nel campo *iat* rientri in un intervallo di 10 minuti nell'intervallo dell'istante corrente (istante attuale - 5min < *iat* < istante attuale + 5min). In caso contrario verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico);
6. Il valore indicato in *exp* corrisponda a *iat* + 30 giorni. In caso contrario verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico).

Effettuate tali verifiche l'IdP potrà decodificare il valore del campo *encryptedData* e verificare che i valori per i campi *id*, *issueInstant* e *issuer* corrispondano rispettivamente a *sub*, *iat*, *aud*, come da specifiche nel paragrafo 4.3.

In caso negativo verrà generato un errore di tipo Bad Request (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico). Altrimenti i dati potranno essere salvati e verrà generato un evento di tipo Ok (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico).

Nel caso in cui l'identità sia già presente presso l'IdP, verrà generato un errore di tipo User Exists (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico).

Nel caso in cui sia già presente un *token* valido per l'identità presso l'IdP, verrà generato un evento di tipo *Token* Exists (vedi l'allegato Tabella messaggi *token* R.A.O. pubblico) e l'IdP procederà a sovrascrivere il vecchio *token* con il nuovo.

## 4.10 Appendice

### 4.10.1 Json Schema per ICRequestData

Il Json Schema utile per la validazione dei ICRequestData è illustrato nella tabella A.1

**Tabella A.1**

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
 "title": "ICRequestData Schema",
 "description": "",
 "type": "object",
 "properties": {
   "Info": {
     "type": "object",
     "properties": {
       "id": {
         "type": "string"
       },
       "issueInstant": {
         "type": "string",
         "format": "date-time"
       },
       "issuer": {
         "type": "object",
         "properties": {
           "issuerCode": {
             "type": "string"
           },
           "issuerInternalReference": {
             "type": "string",
             "maxLength": 32
           }
         },
         "required": [
           "issuerCode",
           "issuerOfficeCode"
         ]
       }
     },
     "required": [
       "ICRequestID",
       "ICRequestIstant",
       "ICRequestIssuer"
     ]
   },
   "electronicIdentification": {
     "type": "object",
     "properties": {
       "identificationType": {
         "enum": [
           "TS",
           "CF"
         ]
       },
       "identificationSerialCode": {
         "type": "string"
       }
     },
     "required": [
       "identificationType",
       "identificationSerialCode"
     ]
   },
```

(continues on next page)

(continua dalla pagina precedente)

```
    "spidAttributes": {
      "type": "object",
      "properties": {
        "mandatoryAttributes": {
          "type": "object",
          "properties": {
            "name": {
              "type": "string"
            },
            "familyName": {
              "type": "string"
            },
            "placeOfBirth": {
              "type": "string",
              "pattern": "[A-Z][0-9]{3}"
            },
            "countyOfBirth": {
              "type": "string",
              "maxLength": 2
            },
            "nationOfBirth": {
              "type": "string",
              "pattern": "Z[0-9]{3}"
            },
            "dateOfBirth": {
              "type": "string",
              "format": "   date"
            },
            "gender": {
              "enum": [
                "M",
                "F"
              ]
            },
            "fiscalNumber": {
              "type": "string",
              "pattern": "TINIT-[A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]
↪{1}"
            },
            "idCard": {
              "type": "object",
              "properties": {
                "IdCardType": {
                  "type": "string"
                },
                "idCardDocNumber": {
                  "type": "string"
                },
                "idCardIssuer": {
                  "type": "string"
                },
                "idCardIssueDate": {
                  "type": "string",
                  "format": "date"
                },
                "idCardExpirationDate": {
                  "type": "string",
```

(continues on next page)

(continua dalla pagina precedente)

```
                "format": "date"
              }
            },
            "required": [
              "idCardType",
              "idCardDocNumber",
              "idCardIssuer",
              "idCardIssueDate",
              "idCardExpirationDate"
            ]
          },
          "mobilePhone": {
            "type": "object",
            "properties": {
              "countryCallingCode": {
                "type": "string",
                "pattern": "\\+[0-9]{2,4}"
              },
              "phoneNumber": {
                "type": "string",
                "pattern": "[0-9]{6,}"
              }
        },
            "required": [
              "countryCallingCode",
              "phoneNumber"
            ]
          },
          "email": {
            "type": "string",
            "format": "email"
          },
          "address": {
            "type": "object",
            "properties": {
              "addressType": {
                "type": "string"
              },
              "addressName": {
                "type": "string"
              },
              "addressNumber": {
                "type": "string"
              },
              "postalCode": {
                "type": "string"
              },
              "municipality": {
                "type": "string"
              },
              "county": {
                "type": "string"
              },
              "nation": {
                "type": "string",
                "pattern": "Z[0-9]{3}"
              }
```

(continues on next page)

(continua dalla pagina precedente)

```
            },
            "required": [
              "addressType",
              "addressName",
              "addressNumber",
              "postalCode",
              "municipality",
              "county",
              "nation"
            ]
          }
        },
        "required": [
          "name",
          "familyName",
          "placeOfBirth",
          "countyOfBirth",
          "nationOfBirth",
          "dateOfBirth",
          "gender",
          "fiscalNumber",
          "idCard",
          "mobilePhone",
          "email",
          "address"
        ]
      },
      "optionalAttributes": {
        "type": "object",
        "properties": {
          "digitalAddress": {
            "type": "string"
          }
        }
      }
    },
    "required": [
      "mandatoryAttributes"
    ]
  }
}
```

### 4.10.2 Json Schema per token completo

Il Json Schema utile per la validazione del token completo è illustrato nella tabella A.2

**Tabella A.2**

```
{
 "definitions": {},
 "$schema": "http://json-schema.org/draft-07/schema#",
 "type": "object",
 "required": [
  "iss",
```

(continues on next page)

(continua dalla pagina precedente)

```
  "sub",
  "jti",
  "aud",
  "iat",
  "exp",
  "fiscalNumber",
  "encryptedData"
 ],
 "properties": {
  "iss": {
    "type": "string"
  },
  "sub": {
     "type": "string"
  },
  "jti": {
    "type": "string"
  },
  "aud": {
    "type": "string"
  },
  "iat": {
    "type": "string",
    "format": "date-time"
  },
  "exp": {
    "type": "string",
    "format": "date-time"
  },
  "fiscalNumber": {
    "type": "string",
    "pattern": "[A-Z]{6}[0-9]{2}[A-Z]{1}[0-9]{2}[A-Z]{1}[0-9]{3}[A-Z]{1}"
  },
  "encryptedData": {
    "type": "string"
  }
 }
}
```

### 4.10.3 Json Schema per Response Payload

Il Json Schema utile per la validazione payload della risposta dell'IdP all'invio di un *token completo* è illustrato nella tabella A.3

**Tabella A.3**

```
{
 "definitions": {},
 "$schema": "http://json-schema.org/draft-07/schema#",
 "type": "object",
 "required": [
   "iss",
   "sub",
   "jti",
   "aud",
```

(continues on next page)

(continua dalla pagina precedente)

```
    "iat",
    "responseCode",
    "responseMessage"
  ],
  "properties": {
    "iss": {
      "type": "string"
    },
    "sub": {
      "type": "string"
    },
    "jti": {
      "type": "string"
    },
    "aud": {
      "type": "string"
    },
    "iat": {
      "type": "string",
      "format": "date-time"
    },
    "responseCode": {
      "type": "number",
      "minimum": 1
    },
    "errorMessage": {
      "type": "string"
    }
  }
}
```

CAPITOLO 5

# Tabella messaggi token R.A.O. pubblico inviati dall'IdP

| Type | responseCode | responseMessage | Codice HTTP | inviate al R.A.O. | inviate all'utente modello a) 3.6 LL GG | inviate all'utente modello b) 3.6 LL GG |
|---|---|---|---|---|---|---|
| Ok | 1 | richiesta autorizzata,token correttamente ricevuto. | 200 | SI | NO | SI |
| User Exists | 2 | spiacenti, per questo utente risulta già rilasciata un'identità digitale SPID. | 403 | SI | NO | SI |
| Unauthorized | 3 | spiacenti, la richiesta non è stata autorizzata in quanto è impossibile identificare l'autore del token. | 401 | SI | NO | SI |
| Bad Request | 4 | spiacenti, il token non è utilizzabile in quanto danneggiato. | 400 | SI | NO | SI |
| Token Exists | 5 | l'attuale richiesta è andata a buon fine sostituendo la precedente. | 201 | SI | NO | SI |
| Invalid Token | 6 | spiacenti, è stato superato il numero massimo di tentativi di inserimento della passphrase . | 403 | NO | SI | SI |
| expired token | 7 | spiacenti, sono passati più di 30 giorni dall'identificazione presso la P.A., il token è scaduto e non più utilizzabile. | 403 | NO | SI | SI |
| generic error | 100 | spiacenti,si è verificato un errore. | 403 | SI | SI | SI |