AGID | Agenzia per l'Italia Digitale

Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD

AGID

13 feb 2020

Indice dei contenuti

1 Definizioni **3**

2 Riferimenti normativi, scopo e ambito di applicazione **5**
2.1 Natura vincolante delle Linee Guida 5

3 Procedura di sottoscrizione ex articolo 20 comma 1-bis del CAD **7**
3.1 Predisposizione alla sottoscrizione (presso il SP) 7
3.2 Consenso alla sottoscrizione (presso l'IdP) 8

4 Regole tecniche del documento sottoscritto **9**
4.1 Formato del documento 9
4.2 Convenzioni di nomenclatura dei documenti 9
4.3 Apposizione del QSeal del Service Provider 10
4.4 Apposizione del QSeal dell'Identity Provider 10
4.5 Certificati qualificati di sigillo elettronico 11
4.6 Metadata nel registro SPID 12

5 Richieste e risposte di autenticazione per la firma **15**
5.1 SAML 15
5.2 Sistema di trasferimento sicuro dei documenti 17
5.2.1 Interfaccia applicativa 17

6 Algoritmi crittografici **21**

7 Codici di ritorno applicativo **23**

8 Obblighi degli enti federati **25**
8.1 Obblighi in capo agli Identity Provider 25
8.2 Obblighi in capo ai Service Provider 25

9 Servizio di conservazione dei documenti firmati **27**

10 Convalida dei documenti firmati con SPID **29**

11 Norme transitorie **31**

Indice **33**

Linee guida ex art. 71 del CAD

consultation

La consultazione pubblica relativa al presente documento è attiva fino al **20 dicembre 2019** (termine prorogato al 28 dicembre). Questo documento raccoglie il testo delle Linee guida in oggetto, disponibile per la consultazione pubblica.

Versione	Data	Tipologia modifica
0.6α	03/dic/2018	Prima versione interna delle LL.GG.
0.9α	23/lug/2018	Priva versione post Gruppo di Lavoro
1.0β	14/ott/2018	Prima bozza per la consultazione pubblica
1.4β	11/nov/2019	Miglioramenti del processo
1.5β	13/nov/2019	Minori revisioni metadata SAML di SP e IdP
1.6β	18/nov/2019	Revisioni minori pre-consultazion
1.0	20/nov/2019	Versione stabile in consultazione pubblica
1.1	29/nov/2019	Proroga per la consultazione pubblica

CAPITOLO 1

Definizioni

Ai fini delle presenti Linee guida, oltre ad applicarsi le definizioni di cui all'articolo 1 del CAD, e del DPCM 24 ottobre 2014 *Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*, si intende per:

- **Agenzia** o **AgID**: Agenzia per l'Italia Digitale;
- **CAD**: D.Lgs. 7 marzo 2005 №82[1], *Codice dell'Amministrazione Digitale*, e sue successive modificazioni;
- **documento firmato con SPID**: il documento sottoscritto ai sensi delle presenti Linee guida;
- **documento predisposto per la firma**: il documento preparato dal SP per essere sottoscritto ai sensi delle presenti Linee guida;
- **ente federato**: gestore di identità digitali ovvero fornitore di servizi della federazione SPID;
- **firma**: vedi sottoscrizione;
- **firmatario**: la persona fisica che, utilizzando la propria identità digitale SPID di livello 2 o superiore, conferisce al documento informatico il valore e l'efficacia previsti dall'articolo 20 del CAD attraverso il processo di firma di cui al presente provvedimento;
- **hash**: cfr. impronta crittografica;
- **impronta**: impronta crittografica, risultante dell'applicazione di una funzione di hash crittografica a un'evidenza informatica;
- **evidenza informatica**: sequenza finita di bit che può essere elaborata da una procedura informatica;
- **LL.GG. identità digitali ad uso professionale**: *Linee guida per il rilascio dell'identità digitale per uso professionale*, pubblicate con Determinazione AgID №318/2019[2] e successive modificazioni;
- **LL.GG. sui certificati elettronici**: *Linee guida contenenti Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*, pubblicate con Determinazione AgID №121/2019[3] e successive modificazioni;
- **LL.GG. sulle misure minime di sicurezza**: Circolare AgID №1/2017[4] e successive modificazioni, recante *Misure minime di sicurezza ICT per le pubbliche amministrazioni*;
- **registro SPID**: elenco dei soggetti appartenenti alla federazione SPID, previsto dalla vigente normativa;

[1] https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2018-09-28/
[2] https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_identita_digitale_per_uso_professionale_v.1.0.pdf
[3] http://www.agid.gov.it/sites/default/files/repository_files/regole_e_raccomandazioni_v1.1.pdf
[4] https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

- **Regolamento eIDAS**: Regolamento (UE) №910/2014[5] del Parlamento Europeo e del Consiglio, 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;
- **Regolamento GDPR**: Regolamento (UE) №679/2016[6] del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **richiesta di autenticazione**: l'evidenza informatica con la quale un SP richiede l'avvio di una sessione di autenticazione presso un IdP (cioè l'*authentication request*);
- **risposta di autenticazione**: l'evidenza informatica con la quale un IdP comunica i dati personali, o il diniego a fornirli, presso un SP (*response*);
- **sottoscrizione**: il processo di cui all'articolo 20, comma 1-bis del CAD;

Sono anche utilizzati i seguenti acronimi o abbreviazioni:

- **API**: interfaccia applicativa (*application programming interface*);
- **IdP**: gestore di identità digitali nel contesto della federazione SPID;
- **JSON**: *JavaScript Object Notation*, come previsto dalla norma **RFC 8259**[7];
- **JWA**: algoritmi crittografici JSON (*JSON Web Algorithm*), come previsto dalla norma **RFC 7518**[8];
- **JWS**: pacchetto JWT firmato (*JSON Token Signature*), come previsto dalla norma **RFC 7515**[9];
- **JWT**: pacchetto JSON per applicazioni web (*JSON Web Token*), come previsto dalla norma **RFC 7797**[10];
- **QSeal**: sigillo elettronico qualificato, come da Regolamento eIDAS;
- **QTSP**: prestatore di servizi fiduciari elettronici qualificati, come da Regolamento eIDAS;
- **SAML**: Security Assertion Markup Language[11], versione 2.0, pubblicato da OASIS;
- **SP**: fornitore di servizi nella federazione SPID;
- **SPID**: il Sistema Pubblico di Identità Digitale, introdotto con il DPCM del 24 ottobre 2014, pubblicato sulla *G.U.* Serie Generale №285 del 9 dicembre 2014.

[5] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014R0910
[6] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679
[7] https://tools.ietf.org/html/rfc8259.html
[8] https://tools.ietf.org/html/rfc7518.html
[9] https://tools.ietf.org/html/rfc7515.html
[10] https://tools.ietf.org/html/rfc7797.html
[11] http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

CAPITOLO 2

Riferimenti normativi, scopo e ambito di applicazione

L'articolo 20 del *CAD* (pagina 3) dispone il soddisfacimento del requisito della forma scritta e l'efficacia prevista dall'articolo 2702 del Codice Civile del documento informatico formato previa identificazione informatica del suo autore,

> attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

Le presenti Linee guida regolano le modalità atte a garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

Destinatari delle Linee guida sono i fornitori di servizi e i gestori dell'identità che intendono realizzare quanto previsto dal sopracitato articolo 20; gli utenti in qualità di fruitori del servizio.

Le presenti Linee guida sono applicabili anche dai *soggetti aggregatori*.

2.1 Natura vincolante delle Linee Guida

Come precisato dal Consiglio di Stato nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, №2122/2017 del 10 ottobre 2017 le Linee Guida adottate da *AgID* (pagina 3), ai sensi dell'articolo 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*. Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'articolo 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'articolo 17 del CAD, istituito presso l'AgID.

CAPITOLO 3

Procedura di sottoscrizione ex articolo 20 comma 1-bis del CAD

Il processo di cui all'articolo 20 comma 1-*bis* del *CAD* (pagina 3) non può essere adoperato utilizzando identità digitali *SPID* (pagina 4) per persona giuridica; possono essere utilizzate esclusivamente le identità digitali della persona fisica e le identità digitali per uso professionale (quest'ultime regolamentate dalle LL.GG. identità digitali ad uso professionale).

Tutti i SP interessati hanno il diritto di avvalersi del servizio in oggetto delle presenti Linee guida.

I metadati SPID indicano se l'ente federato offre il servizio in oggetto o meno (cfr. §*4.6* (pagina 12)).

Il servizio di sottoscrizione oggetto delle presenti Linee guida è realizzato per permettere al medesimo utente di sottoscrivere un documento, (anche in più punti), attraverso un'unica sessione di autenticazione SPID e, al contempo, a utenti distinti di sottoscrivere il medesimo documento, in tempi e con sessioni di autenticazione SPID distinte.

3.1 Predisposizione alla sottoscrizione (presso il SP)

Il processo prevede che il SP conosca il codice fiscale del firmatario; il SP quindi:

Procedura

1. Presenta all'utente il bottone "**Firma con SPID**", alla cui selezione il SP mostra l'elenco degli IdP che offrono il servizio di firma. L'utente seleziona il proprio IdP. Qualora l'utente sia già autenticato presso il SP, con l'identità digitale di un IdP che offre il servizio di firma con SPID, la selezione dell'IdP può essere saltata
2. Il SP predispone il documento (*documento predisposto per la firma*), apponendovi un proprio *sigillo elettronico qualificato* (pagina 4), secondo quanto prescritto nei §§*4.1* (pagina 9) (formato del file), *4.2* (pagina 9) (nome del file), *4.3* (pagina 10) (QSeal) e sottoponendolo, presso la propria piattaforma, all'utente affinché possa essere visionato, eventualmente scaricato e conservato.
3. Il SP rendendo manifesto all'utente che il processo prevede l'invio del documento all'IdP prescelto, acquisendone il consenso esplicito (*opt-in*). L'utente è anche avvisato in modo chiaro e manifesto che tale documento gli sarà reso successivamente disponibile dal proprio IdP e gli viene consigliato di leggerlo nuovamente in tale occasione. Per proseguire l'utente seleziona il bottone "**Prosegui con la Firma**".

4. Il SP invia il documento predisposto per la firma al punto 2 all'IdP e, avuta evidenza del successo dell'invio, inoltra la sessione dell'utente al relativo IdP con una richiesta di autenticazione speciale (di livello pari almeno a 2), denominata "*firma con SPID*", conforme alle caratteristiche tecniche di cui al §*5* (pagina 15) e con le modalità descritte nel §*5.2* (pagina 17). Tale richiesta contiene il codice fiscale del soggetto che deve apporre la firma, acquisito al punto 1.

3.2 Consenso alla sottoscrizione (presso l'IdP)

L'IdP:

Procedura

1. Procede con l'autenticazione dell'utente con credenziali di livello 2 o superiore, verificando che si tratti del firmatario atteso dal SP in base al codice fiscale ricevuto con la richiesta di cui al punto 4 del §*3.1* (pagina 7).
2. Informa l'utente che il processo di autenticazione è volto alla sottoscrizione, comunicando all'utente:

   il nome del SP che sta richiedendo la sottoscrizione del documento,

   il nome del file contenente il documento in oggetto.
3. Consente all'utente di visionare il documento e scaricarlo.
4. Propone all'utente di procedere con la sottoscrizione, raccogliendone il consenso. Il dissenso alla sottoscrizione da parte dell'utente comporta l'invio di una risposta di autenticazione con esito negativo al SP e il termine del processo.
5. Visualizza la pagina destinata a contenere il contenuto grafico del sigillo elettronico qualificato informando l'utente in merito alla obbligatorietà o facoltatività della firma.
6. Acquisisce il consenso dell'utente ad apporre la firma.
7. Procede alla apposizione del sigillo elettronico qualificato (o di più sigilli nel caso siano previste più firme), formando dunque il *documento firmato con SPID*, secondo quanto prescritto ai §§*4.2* (pagina 9) (nome del file), *4.4* (pagina 10) (QSeal).
8. Propone all'utente di inviargli il documento firmato con SPID via posta elettronica, e/o di scaricarne una copia, e/o di renderglielo disponibile nella propria area riservata in base al servizio di cui al §*9* (pagina 27).
9. Invia al SP il documento firmato con SPID con le modalità descritte nel §*5.2* (pagina 17):.
10. Invia al SP la risposta di autenticazione della firma SPID recante l'esito positivo della procedura reindirizzando l'utente presso il SP. Nel caso in cui il punto precedente non abbia successo, l'IdP informa l'SP e l'utente in merito al mancato successo del processo di firma.

Il processo di cui ai punti 6 e 7 è reiterato per ogni firma.

Al termine del processo qui descritto, salvo che l'utente non abbia scelto di avvalersi dei servizi di conservazione dei documenti firmati (cfr. §*9* (pagina 27)), l'IdP rimuove dai propri sistemi il documento oggetto della sottoscrizione, nel pieno rispetto di quanto disposto dal Regolamento *GDPR* (pagina 4).

CAPITOLO 4

Regole tecniche del documento sottoscritto

4.1 Formato del documento

Il documento predisposto dal SP per il processo di firma rispetta le specifiche PDF versione 1.7 o successive, profilo PDF/A-2a, secondo lo standard ISO/IEC 32000-1[12]. Inoltre rispetta le seguenti caratteristiche tecniche:

1. il documento non richiede alcun controllo di accesso per essere aperto o modificato;
2. è consentita la modifica del documento esclusivamente per quanto concerne l'apposizione dei previsti sigilli elettronici PAdES;
3. né il contenuto del documento né i suoi metadati sono cifrati.

4.2 Convenzioni di nomenclatura dei documenti

Il nome del documento predisposto per la firma, di cui al §*3.1* (pagina 7) punto 2 è costituito da tre parti obbligatorie variabili, una parte facoltativa (indicata tra parentesi quadre "`[`" e "`]`"), più alcune parti fisse (in tondo):

```
usID_dataTora[_001].tmp.pdf
```

Il nome del *documento firmato con SPID*, di cui al §*3.2* (pagina 7) punto 11, è derivato dal precedente nome, senza il suffisso `.tmp`:

```
usID_dataTora[_001].pdf
```

In particolare:

- `usID` — Indivdua chi ha predisposto il documento per la firma. È una stringa costituita da un minimo di 3 a un massimo di 10 caratteri ASCII a scelta tra "`01234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_`".
- `data` — È la data di creazione del documento predisposto per la firma (rispetto al fuso orario italiano), rappresentata da una stringa di 8 caratteri numerici così ripartiti:
  - quattro cifre per l'anno solare (da "`2019`" in poi),

[12] http://wwwimages.adobe.com/www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

  - due cifre per il mese dell'anno (da "`01`" per gennaio a "`12`" per dicmebre),
  - due cifre per il giorno del mese (da "`01`" a "`31`");
- `ora` — È l'ora di creazione del documento predisposto per la firma, rispetto all'orario di sistema del SP, *riportato al fuso orario italiano*. È una stringa di 6 caratteri numerici così ripartiti:
  - due cifre per l'ora nell'arco delle ventiquattrore (da "`00`" per la mezzanotte alle "`23`"),
  - due cifre per il minuto primo (da "`01`" a "`59`"),
  - due cifre per il minuto secondo (da "`01`" a "`59`");
- `num` — È un numero incrementale di 3 cifre che può essere facoltativamente utilizzato dal SP per differenziare più documenti che sono predisposti nell'arco del medesimo minuto secondo È facoltà del SP scegliere se usare sempre il campo aggiuntivo "`_001`" ovvero solo a partire dal secondo documento predisposto nel medesimo minuto secondo.

A titolo di esempio, il documento predisposto per la firma dall'Agenzia per l'Italia Digitale (abbreviativo unico: "`AgID`"), il 21 marzo 2019 all'ora locale 08:34:10, è "`AgID_20190321T083410.tmp.pdf`". Il nome del corrispondente documento firmato con SPID (da una persona fisica presso il proprio IDP), sarà "`AgID_20190321T083410.pdf`".

---

example

A titolo di esempio, il documento predisposto per la firma dall'Agenzia per l'Italia Digitale (identificativo unico: "`AgID`"), il 21 marzo 2019 all'ora locale 08:34:10, è "`AgID_20190321T083410.tmp.pdf`". Il nome del corrispondente documento firmato con SPID (da una persona fisica presso il proprio IdP), sarà "`AgID_20190321T083410.pdf`".

4.3 Apposizione del QSeal del Service Provider

Il SP appone il proprio *QSeal* (pagina 4) mediante firma elettronica di tipo PAdES, non visibile (senza alcuna componente grafica), nei formati previsti dal Regolamento *eIDAS* (pagina 3) e dalle conseguenti Decisioni di Esecuzione (UE).

Prima di apporre il proprio QSeal, il SP predispone il documento prevedendo adeguato spazio per contenere la componente grafica (o più componenti se richiede più firme) del QSeal che verrà apposto dall'IdP, il cui testo (cfr. §*4.5* (pagina 11)) deve essere agevolmente leggibile, almeno fino a 256 caretteri ASCII di lunghezza.

4.4 Apposizione del QSeal dell'Identity Provider

A completamento del processo di firma, l'IdP appone il proprio *QSeal* (pagina 4) nel documento che è, per ciascuna firma, graficamente localizzato nello spazio previsto dal SP e indicato nella richiesta di autenticazione (cfr. §*5* (pagina 15)). La componente visibile del sigillo contiene il seguente testo:

```
Il %data% alle %ora%, %firmatario% ha confermato la volonta' di
apporre qui la propria sottoscrizione ai sensi dell'art. 20, comma
1-bis del CAD.
```

Dove:

- La parte variabile `%firmatario%` è così costituita in base alla seguente alternativa (cfr. *LL.GG. identità digitali uso professionale* (pagina 3)):
  - nel caso si utilizzi un'**identità digitale** *non* ad uso professionale, *ovvero* ad **uso professionale per la persona fisica**: il nome e cognome del firmatario (separati fra loro da uno spazio – esadecimale *0x20*), seguiti da uno *slash* ascendente '`/`' (esadecimale *0x2F*), seguito dalla stringa '`TINIT-`', seguito dal codice fiscale del firmatario; ad esempio: "`Mario Rossi/TINIT-RSSMR064T30H501H`";

  - nel caso si utilizzi un'**identità digitale per uso professionale della persona giuridica**: il nome e il cognome del firmatario (fra di loro separati da uno spazio) seguiti da uno slash ascendente '`/`', seguiti dalla denominazione dell'organizzazione, seguita da un altro *slash* ascendente '`/`', seguito da un identificativo unico *dell'organizzazione* (privo di spazi in testa e in coda), valorizzato seguendo le alternative proposte nel §*4.5* (pagina 11), punto 1.a. Ad esempio, nel caso di Mario Rossi che utilizza l'identità digitale uso professionale della persona giuridica 'Agenzia per l'Italia Digitale': "`Mario Rossi/Agenzia per l'Italia Digitale/TINIT-97735020584`".

- La parte variabile `%data%` contiene la data di sottoscrizione, espressa come una stringa di 8 caratteri numerici separati in tre gruppi da uno *slash* ascendente '`/`' e ripartiti come:
  - due cifre per giorno del mese (da "`01`" a "`31`"),
  - due cifre per il mese dell'anno (da "`01`" per gennaio a "`12`" per dicembre),
  - quattro cifre per l'anno solare (da "`2019`" in poi).
- La parte variabile `%ore%` contiene l'ora di sottoscrizione (*sempre riportata al fuso orario italiano*), espressa come una stringa di 8 caratteri numerici separati in tre gruppi da due-punti '`:`' e ripartiti come:
  - due cifre per l'ora nell'arco delle ventiquattrore (da "`00`" per la mezzanotte a "`23`"),
  - due cifre per il minuto primo (da "`00`" a "`59`"),
  - due cifre per il minuto secondo (da "`00`" a "`59`").

Il documento può contenere già una o più firme elettroniche qualificate o sigilli elettronici qualificati, o può già essere stato oggetto di altri processi di sottoscrizione come previsti dalle presenti Linee guida.

La richiesta del SP può prevedere più firme dello stesso soggetto sul documento; in tal caso l'IdP appone altrettanti sigilli.

4.5 Certificati qualificati di sigillo elettronico

SP e IdP si dotano, presso un *QTSP* (pagina 4), di un certificato elettronico qualificato per la creazione di sigilli elettronici.

Detti certificati qualificati sono conformi alle raccomandazioni emanate con le *LL.GG. sui certificati elettronici* (*cit.* (pagina 3)), allo standard X.509 versione 3, e contengono le seguenti informazioni aggiuntive:

1. Il campo `SubjectDN`, contenente i seguenti attributi:
   a. `serialNumber` (2.5.4.5[13]) — contiene per gli IdP e i SP, alternativamente, secondo il seguente ordine:
      - la partita IVA indicata con il prefisso '`VAT`', come prescritto dal §5.1.4 punto 1 della norma ETSI EN 319-412-1[14] (es. "`VATIT-12345678901`");
      - il codice fiscale indicato con il prefisso '`CF:`', come prescritto dal §5.1.4 punto 3 della suddetta norma (es. "`CF:IT-01234567890`");
      - il numero assegnato dal Registro Imprese, indicato con il prefisso '`NTR`', come prescritto dal §5.1.4 punto 2 della suddetta norma (es. "`NTRIT-1234567890`");
      - per gli SP pubblici, il codice IPA, così come risulta nel campo `ipaEntityCode` del registro SPID, preceduto dal prefisso '`PA:`', come prescritto dal §5.1.4 punto 3 della suddetta norma (es. "`PA:IT-agid`").

   b. `commonName` (2.5.4.3[15]) — contenente, mediante un elemento di tipo `dNSName`, il nome di dominio – privo di qualsiasi carattere *wildcard* – di cui al punto 5.
2. Il campo `CertificatePolicies` (2.5.29.32[16]), contenente i seguenti attributi:

[13] http://oid-info.com/get/2.5.4.5
[14] http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf
[15] http://oid-info.com/get/2.5.4.3
[16] http://oid-info.com/get/2.5.29.32

a. `PolicyIdentifier` — valorizzato come:

   - `spidSignature` (1.3.76.16.4.11[17]);

b. una limitazione d'uso indicata mediante la presenza di un campo `userNotice` (2.5.29.49[18]), di tipo `explicitText`, valorizzato con la seguente stringa bilingue: "`Certificato usabile solo per il processo di sottoscrizione di cui all'art.20 del CAD/This certificate may be used only for elecrronic signing pursuant to the Italian Digital Administration Code, art.20.`".

3. `keyUsage` (2.5.29.15[19]) — contenente i valori `digitalSignature` e `keyEncipherment`, cioè i bit #0 e #2, valorizzati a `1`, come da specifica **RFC 5280**[20].

4. `extendedKeyUsage` (2.5.29.16[21]) — contenente sia l'elemento `id-kp-serverAuth` (1.3.6.1.5.5.7.3.1[22]) che l'elemento `id-kp-clientAuth` (1.3.6.1.5.5.7.3.2[23]).

5. `subjectAltName` (2.5.29.17[24]) — valorizzata con elemento unico di tipo `dNSName` e contenente il dominio dell'URL completo (così come riportato nel registro SPID) presso il quale l'ente federato rende disponibile, agli enti federati della tipologia opposta, il servizio di trasferimento sicuro di cui al §*5.2* (pagina 17).

4.6 Metadata nel registro SPID

Qualora un IdP, un SP ovvero un soggetto aggregatore offra il servizio in oggetto, il relativo metadata pubblicato nel registro SPID contiene l'estensione `<SignatureArt20>` (*namespace* `spid`) come figlio dell'elemento `<Extensions>` (*namespace* `samlp`), al cui interno è specificata la modalità tecnica tramite la quale l'ente federato espone tale servizio.

La suddetta modalità è costituita da:

[17] http://oid-info.com/get/1.3.76.16.4.11

[18] http://oid-info.com/get/\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ÿ(U+1D7F8)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ż(U+1D7FB)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ÿ(U+1D7F8)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§¿(U+1D7FF)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.49

[19] http://oid-info.com/get/\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ÿ(U+1D7F8)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ż(U+1D7FB)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§ÿ(U+1D7F8)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup\protect\begingroup\immediate\write\@unused\def\MessageBreak˙\let\protect\edefYourcommandwasignored.\MessageBreakTypeI<command><return>toreplaceitwithanothercommand,\MessageBreakor<return>tocontinuewithoutit.\errhelp\let\def\MessageBreak˙(inputenc)\def\errmessagePackageinputencError:UnicodecharðÍ§¿(U+1D7FF)\MessageBreaknotsetupforusewithLaTeX.¨˙Seetheinputencpackagedocumentationforexplanation.˙TypeH<return>forimmediatehelp\endgroup.15

[20] https://tools.ietf.org/html/rfc5280.html

[21] http://oid-info.com/get/2.5.29.16

[22] http://oid-info.com/get/1.3.6.1.5.5.7.3.1

[23] http://oid-info.com/get/1.3.6.1.5.5.7.3.2

[24] http://oid-info.com/get/2.5.29.17

- l'elemento `<FileTransferService>` (*namespace* `spid`), dotato del seguente attributo:
  - `Location` — URL completo (comprensivo del relativo schema HTTPS) ove l'ente rende disponibile il sistema di trasferimento sicuro dei documenti di cui al §5.2 (pagina 17).

Si veda a tale scopo il seguente esempio:

```
<md:EntityDescriptor>
    <ds:Signature>...</ds:Signature>
    ...
    <samlp:Extensions
          xmlns:spid="https://spid.gov.it/saml-extensions">
        <spid:SignatureArt20>
            <spid:FileTransferService
                  Location="https://indirizzo/al/DataIO/" />
        </spid:SignatureArt20>
    </samlp:Extensions>
    <md:Organization>...</md:Organization>
    ...
</md:EntityDescriptor>
```

Qualora l'elemento `<SignatureArt20>` non sia presente nel metadata, è da intendersi che l'ente federato *non* offre tale servizio.

Il metadata dei SP che offrono il servizio in oggetto contiene, all'interno dell'`<EntityDescriptor>` (*namespace* `md`):

- Un *Attribute Consuming Service* specifico:
  a. il cui attributo `index` è valorizzato con il valore "`77`";
  b. privo di alcun attributo nel servizio (nessun elemento `<RequestedAttribute>`);
  c. contenente almeno un elemento figlio `<ServiceName>` (*namespace* `md`), valorizzato con il nome del servizio in lingua italiana: "`Sottoscrizione elettronica ex art.20 CAD`".

Il metadata del SP comprende dunque la seguente struttura:

```
<md:EntityDescriptor>
    ...
    <md:SPSSODescriptor>
        <md:AttributeConsumingService index="77">
            <md:ServiceName xml:lang="it">
                Sottoscrizione elettronica ex art.20 CAD
            </md:ServiceName>
        </md:AttributeConsumingService>
    ...
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Tutte le evidenze informatiche SAML che si riferiscono al servizio in oggetto (descritte sia qui che al §5.1 (pagina 15)) indicano il riferimento URN https://spid.gov.it/saml-extensions al *namespace* XML dell'Agenzia riservato a SPID — nel proprio elemento radice, ovvero in tutti i singoli elementi interessati (qui genericamente indicati come `<Element>` di *namespace* `ns`), come riportato nell'esempio sotto:

```
<ns:Element xmlns:spid="https://spid.gov.it/saml-extensions">
    ...
</ns:Element>
```

CAPITOLO 5

Richieste e risposte di autenticazione per la firma

La **richiesta di autenticazione** per la firma SPID, introdotta al punto 4 della procedura di cui al §*3* (pagina 7), contiene i seguenti metadati aggiuntivi:

a. il nome del file del documento predisposto per la firma;

b. l'impronta dell'evidenza informatica ottenuta calcolando l'*hash* (pagina 3) del file di cui al punto a, calcolata dal SP conformemente a quanto indicato al §*6* (pagina 21);

c. l'identificativo della funzione di *hash* crittografico utilizzato al punto b;

d. il codice fiscale del soggetto che deve apporre la firma.

La **risposta di autenticazione** per la firma SPID contiene obbligatoriamente i seguenti metadati:

e. il nome del file del documento firmato con SPID;

f. l'impronta dell'evidenza informatica ottenuta calcolando l'*hash* (pagina 3) del file di cui al punto e, calcolata dall'IdP conformemente a quanto indicato al §*6* (pagina 21);

g. l'identificativo della funzione di *hash* crittografico utilizzato al punto f.

L'identificativo unico della sessione di autenticazione (*session ID*), sempre presente in ogni richiesta e risposta di autenticazione, associa in modo univoco il documento informatico scambiato tra SP, IdP e vice versa, ad un'unica autenticazione di firma con SPID.

La durata delle sessioni di autenticazione descritte nell'ambito del processo di sottoscrizione di cui alle presenti Linee guida è estesa adeguatamente per permettere lo svolgimento dell'intera procedura di sottoscrizione.

Le richieste e risposte di autenticazione per la firma SPID seguono la sintassi descritta nei seguenti paragrafi.

5.1 SAML

La richiesta di autenticazione *SAML* (pagina 4) si riferisce, nell'elemento `<AuthnRequest>` (*namespace* `samlp`), all'attributo *AttributeConsumingServiceIndex* corrispondente all'*Attribute Consuming Service* specifico, di indice "`77`", introdotto al §4.6.

Le richieste e risposte di autenticazione SAML impiegano *session ID*, nei loro rispettivi attributi `ID`, valorizzati come stringhe uniche che cominciano con `sig-`. Le richieste e risposte di autenticazione contengono entrambe un'estensione `<Signature>` (*namespace* `spid`) contenuta nella sezione prevista dallo standard per le estentioni *SAML* (pagina 4). I metadati sopra elencati sono realizzati mediante i seguenti elementi:

- punti a. e d. tramite elemento `<Filename>` (*namespace* `spid`), contenente il nome del file del documento, comprensivo della corretta estensione, composto come descritto in §*4.2* (pagina 9);
- punti b. e f. tramite elemento `<DigestValue>` (*namespace* `ds`), contenente un'impronta rappresentata applicandole la trasformazione *Base64* (cfr. **RFC 4648**[25]);
- punti c. e g. tramite elemento `<DigestMethod>` (*namespace* `ds`), contenente la codifica W3C della funzione di *hash* utilizzata per il calcolo dell'impronta del documento;
- l'identificativo univoco di sessione è indicato nell'attributo `ID` dell'elemento `<AuthnRequest>` per la richiesta di autenticazione, il cui valore combacia con quello dell'attributo `InResponseTo` dell'elemento `<Response>` per la corrispondete risposta di autenticazione.

Qui sotto è riportato un esempio di richiesta di autenticazione SAML, comprensiva dell'*Attribute Consuming Service* specifica e dell'elemento `<Signature>` (*namespace* `spid`) per la richiesta di autenticazione relativa a un documento in formato PDF predisposto dal SP e successivamente inviato all'IdP per la sottoscrizione.

```
<samlp:AuthnRequest
      AttributeConsumingService="77"
      Destination="https://url-IdP-destinatario"
      ID="sig-SessionID"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:spid="https://spid.gov.it/saml-extensions"
      xmlns:enc="http://www.w3.org/2001/04/xmlenc#">
    <saml:Issuer>https://url-SP-inviante</saml:Issuer>
    ...
    <samlp:Extensions>
        <spid:Signature>
            <spid:Filename>AgID_YYYYMMDDThhmmss.tmp.pdf</spid:Filename>
            <ds:DigestMethod Algorithm="http://funzione_hash" />
            <ds:DigestValue>ImprontaDocumento1</ds:DigestValue>
        </spid:Signature>
        <spid:Signer>
            <saml:Attribute
                  xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                  Name="fiscalNumber">
               <saml:AttributeValue xsi:type="xs:string">
                   CodiceFiscaleFirmatario
               </saml:AttributeValue>
            </saml:Attribute>
        </spid:Signer>
    </samlp:Extensions>
</samlp:AuthnRequest>
```

Qui sotto è riportato un esempio di elemento `<Signature>` per la risposta di autenticazione SAML relativa alla richiesta di autenticazione di cui al precedente esempio, ove l'IdP comunica al SP i metadati del documento firmato con SPID.

```
<samlp:Response
      xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
      Destination="https://url-SP-destinatario"
      ID="_ResponseID"
      InResponseTo="sig-SessionID">
    <saml:Issuer>https://url-IdP-inviante</saml:Issuer>
    ...
    <samlp:Extensions
          xmlns:spid="https://spid.gov.it/saml-extensions">
        <spid:Signature>
            <spid:Filename>AgID_YYYYMMDDThhmmss.pdf</spid:Filename>
```

(continues on next page)

[25] https://tools.ietf.org/html/rfc4648.html

(continua dalla pagina precedente)

```
            <ds:DigestMethod Algorithm="http://funzione_hash" />
            <ds:DigestValue>ImprontaDocumento2</ds:DigestValue>
        </spid:Signature>
    </samlp:Extensions>
</samlp:Response>
```

5.2 Sistema di trasferimento sicuro dei documenti

Ogni ente federato si dota di un sistema di trasferimento dedicato ai documenti oggetto delle presenti Linee guida, costituito da uno storage dedicato, un protocollo di comunicazione sicura che garantisce un adeguato livello di confidenzialità, integrità e disponibilità, e da un sistema di gestione dei file ricevuti.

L'interfaccia applicativa fornita dal protocollo di comunicazione per il trasferimento di documenti dall'esterno è resa nota da ciascun ente federato verso tutti gli enti federati, mediante l'URL che l'ente medesimo pubblica nel metadata SPID e il cui dominio è contestualmente riportato nei campi `commonName` e `subjectAltName` del proprio certificato qualificato di sigillo elettronico, di cui al §*4.5* (pagina 11), punti 1.b e 5. Tale URL indica esplicitamente il protocollo di comunicazione sicuro, i cui dettagli sono dati in §*5.2.1* (pagina 17).

Il sistema di trasferimento è, nella sua interezza, protetto da misure di sicurezza logica, fisica e amministrativa conformi almeno alle *LL.GG. sulle misure minime di sicurezza* (pagina 3). Esso è inoltre adeguatamente protetto logicamente affinché solamente gli enti federati possano trasferire file mediante uno dei seguenti due flussi:

A. il sistema dell'IdP è configurato per la sola ricezione di evidenze informatiche provenienti dagli SP in modalità *push* (cioè con trasferimenti iniziati in *upstream* dal SP);

B. il sistema del SP è configurato per la sola ricezione di evidenze informatiche provenienti dagli IdP in modalità *push* (cioè con trasferimenti iniziati in *upstream* dall'IdP).

Il sistema di trasferimento possiede, inoltre, le seguenti caratteristiche:

1. SP e IdP controllano che ogni file creato presso il proprio storage soddisfi quanto prescritto nel §*4.2* (pagina 9).
2. L'IdP rimuove dallo storage i file ricevuti per i quali non sia pervenuta, entro un tempo limite di **10 secondi**, una richiesta di autenticazione proveniente dal SP.
3. IdP e SP verificano l'integrità dei documenti ricevuti ricalcolandone l'impronta e confrontandola con quella contenuta, rispettivamente, nella richiesta e nella risposta di autenticazione che le accompagnano.
4. IdP e SP verificano l'autenticità dei *QSeal* (pagina 4) della controparte e l'integrità del documento ricevuto.

5.2.1 Interfaccia applicativa

SP e IdP si scambiano evidenze informatiche in formato *JWS* (pagina 4), su canale HTTPS (porta 443/TCP) tramite un'*API* (pagina 4) che prevede lo scambio di messaggi tramite metodo HTTP *POST*. Le evidenze sono formate mediate la seguente procedura:

1. predisposizione di una struttura *JSON* (pagina 4) contenente sia il **dato** (cioè il documento oggetto di sottoscrizione) che i suoi **metadati**, di seguito elencati:
    a. il nome del documento da inviare, predisposto come da §*4.2* (pagina 9),
    b. l'impronta del docuento da inviare sigillato elettronicamente,
    c. la funzione di *hash* impiegata al punto 1.b,
    d. la posizione ove collocare la/le componente/i grafica/he del *QSeal* (pagina 4) (§*4.4* (pagina 10)),
    e. l'eventuale obbligatorietà di ciascuna firma.
2. codifica del messaggio di cui al punto 1 in un pacchetto *JWT* (pagina 4);

3. conversione in *JWS* (pagina 4) del pacchetto di cui al punto 2, mediante metodo *JWS Compact Serialization* (cfr. **RFC 7515**[26]), utilizzando il *QSeal* (pagina 4) di cui al §*4.5* (pagina 11).

Gli algoritmi crittografici utilizzati lungo l'intera procedura sopra descritta sono definiti in §*6* (pagina 21). I pacchetti JWS sono caratterizzati dalla presenza degli identificativi unici di sessione (cfr. §*5* (pagina 15)).

Le strutture JSON in base alle quali sono prodotti i pacchetti JWS scambiati durante i flussi *A* (pagina 17) e *B* (pagina 17) sono chiamate, rispettivamente, **pacchetto di andata** e **pacchetto di ritorno**.

L'intestazione (*header*) comune ai pacchetti di andata e ritorno contiene i seguenti parametri obbligatori:

- `typ` — valorizzato con la stringa "`JOSE`";
- `alg` — valorizzato con l'identificativo JWA dell'algoritmo crittografico utilizzato per la firma del pacchetto JWS, secondo quanto indicato al §*6* (pagina 21);
- `x5c` — valorizzato con il certificato qualificato di sigillo elettronico dell'ente inviante (codificato in *Base64*, cfr. **RFC 4648**[27]), come definito al §*4.5* (pagina 11);
- `crit` — valorizzato con una lista di un unico elemento "`x5c`", ad indicare che la convalida del certificato di cui al punto precedente è obbligatoria;

Un esempio di intestazione sopra definita è:

```
{
    "typ" : "JOSE",
    "alg" : "ES256",
    "x5c" : "Certificato/codificato+Base64",
    "crit": ["x5c"]
}
```

Il *payload* dei pacchetti di andata e ritorno contiene i seguenti parametri obbligatori:

- `jti` — valorizzato con identificativo unico del pacchetto *JWT* (pagina 4);
- `iss` — valorizzato con l'`entityId`: (URL con schema HTTPS) dell'ente federato inviante; coincide con il valore dell'elemento `<Issuer>`:
- `aud` — valorizzato con l'`entityId` (URL con schema HTTPS) dell'ente federato destinatario; coincide con il valore dell'attributo `Destination`, rispettivamente, dell'elemento *SAML* (pagina 4):
  - `<AuthnRequest>` per il pacchetto di andata (flusso *A* (pagina 17)), *ovvero*
  - `<Response>` per il pacchetto di ritorno (flusso *B* (pagina 17)).
- `iat` — valorizzato con l'orario in cui il messaggio è generato e inviato (rispetto al fuso orario italiano), codificato come campo di tipo *NumericDate*;
- `sessionID` — valorizzato con il *session ID*, così come dichiarato nella richiesta di autenticazione per firma SPID – coincide con il valore che, nei pacchetti di andata e di ritorno, si trova rispettivamente nell'attributo:
  - `ID` dell'elemento SAML `<AuthnRequest>` per il flusso *A* (pagina 17) (andata), *ovvero*
  - `InResponseTo` dell'elemento SAML `<Response>` per il flusso *B* (pagina 17) (ritorno).
- `filename` — valorizzato con il nome del file del documento inviato; coincide con il valore dell'elemento `<Filename>` come specificato nel §*4.2* (pagina 9);
- `cty` — valorizzato con la tipologia MIME del documento di cui al punto precedente (quindi come "`pdf`", come da normativa **RFC 7515**[28]);
- `payload` — valorizzato con l'evidenza del documento informatico da trasferire, codificato in *Base64* (cfr. **RFC 6848**[29]);

[26] https://tools.ietf.org/html/rfc7515.html
[27] https://tools.ietf.org/html/rfc4648.html
[28] https://tools.ietf.org/html/rfc7515.html
[29] https://tools.ietf.org/html/rfc6848.html

- `hash` — valorizzato con una struttura JSON così costituita:
  - `method` — valorizzato con la codifica W3C della funzione di *hash* utilizzata per il calcolo delle impronte dei documenti e coincidente con il valore dell'emento SAML `<DigestMethod>`,
  - `digest` — valorizzato con l'impronta del documento trasferito e coincidente con il valore dell'elemento SAML `<DigestValue>`.

Nel pacchetto di andata:

- `signatures` — valorizzato con un *array* JSON contenente tanti elementi quante sono le sottoscrizioni richieste; ciascun elemento dell'*array* è una struttura JSON contenente:
  - `id` — valorizzato con un *identificativo univoco della firma* nell'ambito del processo di firma, cioè una stringa alfanumerica di massimo 40 caratteri;
  - `pag` — valorizzato con il numero della pagina del documento ove è richiesto che l'IdP apponga la componente grafica di cui al §*4.4* (pagina 10);
  - `pos` — contenente un *array* JSON con quattro elementi di tipo *number* – `llx`, `lly`, `urx` e `ury` - valorizzati rispettivamente con l'ascissa e l'ordinata del vertice inferiore sinistro, l'ascissa e l'ordinata del vertice superiore destro di un'area rettangolare definita al §*4.4* (pagina 10), per il posizionamento della componente grafica del QSeal all'interno della pagina stessa, secondo quanto previsto tecnicamente per la rappresentazione di oggetti PDF *Rectangles*, §4.40 dello standard ISO/IEC 32000-1[30];
  - `ref` —booleano per indicare se la firma è facoltativa (`false`) ovvero obbligatoria (`true`) per il SP richiedente. Se il firmatario non accetta di apporre anche solo una firma obbligatoria, l'intero processo di sottoscrizione termina senza successo (cfr. §*7* (pagina 23))e l'IdP non restituisce il documento al SP, informandolo della mancanza di volontà del firmatario.

Nel pacchetto di ritorno:

- `sub` — valorizzato con la stringa `%firmatario%` identificativa del firmatario, come definita nel §*4.4* (pagina 10);
- `signatures` — valorizzato con un *array* JSON contenente tanti elementi quante sono le firme richieste nel pacchetto di andata; ciascun elemento dell'*array* è una struttura JSON contenente:
  - `id` — l'identificativo univoco della firma contenuto nel pacchetto di andata;
  - `signed` — il booleano che conferma l'apposizione (`true`) o meno (`false`) della firma.

I pacchetti sono validi se conformi al presente provvedimento e a eventuali successive indicazioni dell'*Agenzia* (pagina 3).

Seguono un esempio del pacchetto di andata e del relativo pacchetto di ritorno per la sottoscrizione di un documento per il quale sono richieste due firme: la prima, a pagina 3, obbligatoria; la seconda, a pagina 7, facoltativa. Nella risposta, l'IdP informa il SP che l'utente ha apposto solo la firma obbligatoria.

Esempio di pacchetto di andata JSON:

```
{
    "jti" : "uuid1",
    "iss" : "https://entityId-SP-inviante",
    "aud" : "https://entityId-IdP-ricevente",
    "iat" : 1563235200,
    "sessionID": "sig-sessionID",
    "filename" : "AgID_20190321T083410.tmp.pdf",
    "cty" : "pdf",
    "digest" : {
        "method" : "schema://funzione_hash",
        "value" : "ImprontaDocumento1"
    },
    "signatures" : [
        {
```

(continues on next page)

[30] http://wwwimages.adobe.com/www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

(continua dalla pagina precedente)

```
            "id"  : "sig1",
            "pag" : 3,
            "pos" : {
                "llx":89.9446,
                "lly":719.976,
                "urx":239.978,
                "ury":751.299
            },
            "req" : true
        },
        {
            "id"  : "sig2",
            "pag" : 7,
            "pos" : {
                "llx":240.734,
                "lly":686.297,
                "urx":390.768,
                "ury":718.421
            },
            "req" : false
        }
    ],
    "payload" : "BlobDocumento1 + [...] + codificatoBase64"
}
```

Esempio di pacchetto di ritorno JSON:

```
{
    "jti" : "uuid2",
    "iss" : "https://entityId-IdP-inviante",
    "aud" : "https://entityId-SP-ricevente",
    "sub" : "Mario Rossi/CF:IT-RSSMR064T30H501H",
    "iat" : 1563235220,
    "sessionID": "sig-sessionID",
    "filename" : "AgID_20190321T083410.pdf",
    "cty" : "pdf",
    "digest" : {
        "method" : "http://funzione_hash",
        "value" : "ImprontaDocumento2"
    },
    "ref" : [
        {
            "id"  : "sig1",
            "signed" : true
        },
        {
            "id"  : "sig2",
            "signed" : false
        }
    ],
    "payload" : "BlobDocumento2 + [...] + codificatoBase64"
}
```

CAPITOLO 6

Algoritmi crittografici

Ai fini del presente regolamento è utilizzata, per il calcolo delle *impronte* (pagina 3), la funzione di *hash* crittografico **SHA-256**, il cui riferimento W3C è `http://www.w3.org/2001/04/xmlenc#sha256`.

Per la realizzazione tecnica di firme digitali (nella fattispecie, di creazione di sigilli elettronici) è utilizzato l'algoritmo **ECDSA** (con uso della curva ellittica P256 e funzione di *hash* crittografico SHA-256), il cui riferimento W3C è `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256` e il cui riferimento *JWA* (pagina 4) è `ES256`. Al di fuori della firma digitale dei pacchetti *JWT* (pagina 4), è usato l'algoritmo **RSA** con lunghezza delle chiavi asimmetriche di 2048 bit (e funzione di *hash* crittografico SHA-256), il cui riferimento W3C è `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`.

La versione del canale di comunicazione TLS utilizzato dagli enti federati è la 1.2 o superiore.

Gli algoritmi crittografici utilizzati per i pacchetti *JWS* (pagina 4) cono conformi a quanto previsto dal presente capitolo e i loro riferimenti tecnici sono pubblicati nella norma **RFC 7518**[31].

Importante: Gli algoritmi e i metodi crittografici contenuti nel presente capitolo possono essere sostituiti, rimossi o integrati con altri mediante pubblicazione di Avvisi sul sito web istituzionale dell'Agenzia.

[31] https://tools.ietf.org/html/rfc7518.html

CAPITOLO 7

Codici di ritorno applicativo

Possono presentarsi errori in due fasi distinte del processo di sottoscrizione:

1. durante l'autenticazione SAML per la firma cn SPID di cui al §*5.1* (pagina 15); ovvero
2. durante il trasferimento sicuro dei documenti di cui al §*5.2* (pagina 17).

Nel primo caso, gli errori sono notificati dall'IdP al SP con la risposta di autenticazione (secondo quanto previsto dal protocollo SAML). Contestualmente, l'utente è visivamente notificato dell'errore presso l'interfaccia dell'IDP.

La *Tabella 1* (pagina 23) qui sotto elenca soltanto gli errori specifici alla procedura di sottoscrizione, potendo venire notificati anche quelli già previsti dalle Regole Tecniche SPID e pubblicati, nel documento SPID – Tabella messaggi di anomalie[32], presso il sito web dell'Agenzia.

Tabella 7.1: Errori specifici per la procedura di sottoscrizione.

#	scenario	binding	HTTP Status Code	SAML Status Code / sub-Status / Status Message	destinatario	schermata IdP
771	L'utente ha negato il consenso ad apporre firme obbligatorie.	HTTP *POST* / *HTTP Redirect*	n.a.	`urn:oasis:names:tc:SAML:2.0:status:Responder` `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr771`	SP	n.a.
772	Il documento non è disponibile.	HTTP *POST* / *HTTP Redirect*	n.a.	`urn:oasis:names:tc:SAML:2.0:status:Responder` `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr772`	SP	n.a.

Nel secondo caso, il mittente del documento è informato dal destinatario secondo le indicazioni della norma **RFC 7807**[33]. Il mittente, ricevuto il messaggio di errore, lo notifica all'utente.

La *Tabella 2* (pagina 24) elenca i possibili codici di ritorno, veicolati nel pacchetto JWT contenente un oggetto di *Content-Type* `problem+json`.

[32] https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/spid-messaggi.pdf
[33] https://tools.ietf.org/html/rfc7807.html

Tabella 7.2: Codici di ritorno del sistema di trasferimento sicuro dei documenti.

HTTP Status Code	code	title	detail
201		*created*	Errore nella richiesta: Pacchetto malformato.
400	1	JWS malformato	Errore nella richiesta: Pacchetto malformato.
400	2	nome del file invalido	Errore nella richiesta: Nome del file non valido.
400	3	file corrotto	Errore nella richiesta: Documento corrotto.
400	4	documento malformato	Errore nella richiesta: Documento malformato.
400	5	formato del file invalido	Errore nella richiesta: Formato del file non previsto.
400	6	*hash* del documento non corretto	Errore nella richiesta: L'impronta crittografica del file non corrisponde con quella dichiarata.
401		QSeal invalido	Errore nella richiesta: Certificato di sigillo elettronico non valido.
503		servizio non disponibile	Servizio temporaneamente non disponibile.

CAPITOLO 8

Obblighi degli enti federati

Gli enti federati sono tenuti al rispetto delle disposizioni di quanto prescritto dal Regolamento *GDPR* (pagina 4) e dal D.Lgs. №101/2018.

8.1 Obblighi in capo agli Identity Provider

Gli IDP che offrono servizi di sottoscrizione di cui alle presenti Linee guida, si impegnano:

- a rendere disponibile ai SP il proprio servizio e garantirne tutte le caratteristiche di confidenzialità, integrità e disponibilità;
- salvo quanto previsto al §9, a *non* conservare i documenti oggetto della firma con SPID che sono depositati presso i propri sistemi, rimuovendoli in modo sicuro al termine del trattamento.

8.2 Obblighi in capo ai Service Provider

I SP che intendono far utilizzare la funzione di firma oggetto del presente provvedimento, hanno l'obbligo improrogabile di consentire agli utenti la sottoscrizione con firma elettronica qualificata.

CAPITOLO 9

Servizio di conservazione dei documenti firmati

Gli IdP possono offrire ai firmatari servizi aggiuntivi di conservazione dei documenti firmati con SPID resi accessibili all'utente attraverso apposito servizio.

L'IdP è titolare del trattamento per finalità diverse da quelle del servizio di sottoscrizione ex art. 20. L'utente è chiaramente informato che i dati personali oggetto del servizio e i documenti firmati con SPID sono ulteriormente trattati dall'IdP.

CAPITOLO 10

Convalida dei documenti firmati con SPID

Al fine della convalida dei documenti, tutti i sigilli elettronici qualificati associati dal documento ai sensi delle presenti Linee guida sono validi ai sensi della normativa vigente in materia.

CAPITOLO 11

Norme transitorie

Le presenti regole tecniche sono adottate dagli enti federati di cui alle definizioni nel §*1* (pagina 3), su base volontaria, a partire dal quindicesimo giorno dalla data di pubblicazione della notizia della loro emanazione sulla *Gazzetta Ufficiale della Repubblica Italiana*.

Indice

R

RFC
    RFC 4648, 16, 18
    RFC 5280, 12
    RFC 6848, 18
    RFC 7515, 4, 18
    RFC 7518, 4, 21
    RFC 7797, 4
    RFC 7807, 23
    RFC 8259, 4