Linee Guida Attribute Authority

Allegato Tecnico SAML

SISTEMA DI GESTIONE DELLE DELEGHE DIGITALI

Sommario

History of Changes

Date	Pubblicato	Versione	Modifiche
31/05/2021	AgID	1.0	Prima versione

1. Introduzione

Il presente Allegato Tecnico alle *Linee Guida sulle Attribute Authority*, pubblicate dall'Agenzia per l'Italia Digitale (AgID), descrive l'implementazione mediante protocollo SAML adottato inizialmente per un particolare gestore di attributi qualificati: il sistema di gestione delle deleghe digitali (**SGD**).

Nel §2 sono introdotte le definizioni fondamentali (comparandole anche con la nomenclatura più generale nei contesti delle identità digitali nazionali e dello standard tecnologico SAML). Viene inoltre descritto come le componenti principali del SGD siano declinate nelle costituenti principali di un'architettura basata su SAML (metadata, ruoli del Service Provider, dell'Identity Provider e dell'Attribute Authority, protocollo dei messaggi).

Nel §0 viene definito il flusso di consumo dell'attributo qualificato 'delega digitale,' suddiviso in passaggi cronologici (nel caso con esito positivo – il caso con esito negativo è demandato invece al §7).

Nel §4 sono descritti nel dettaglio tutti i messaggi (richieste e risposte di autenticazione SAML) che costituiscono il protocollo di interazione tra gli enti tecnici con-partecipanti al *sistema delle deleghe digitali*: il SGD, i diversi fornitori di servizi con esso federati e gli eventuali altri gestori di attributi (cd. **AA**), sia qualificati che non qualificati.

Nel §5 vengono elencate le caratteristiche obbligatorie e facoltative di una delega digitale, come riportarle nei metadata (cfr. §6) e come fruirne attraverso lo scambio di attributi-delega nei messaggi di protocollo (cfr. §4).

Nel §6 è descritta la struttura dei metadata SAML mediante i quali le entità con-partecipanti al sistema delle deleghe digitali presentano alle rispettive federazioni le proprie caratteristiche tecniche.

Nel §7 sono infine descritti i comportamenti del sistema e i messaggi di protocollo nei casi in cui non è possibile fruire di una delega digitale.

Le modalità di creazione e di modifica di una delega digitale, quelle relative alle operazioni svolte dagli utenti del sistema, così come i riferimenti normativi, saranno descritte nei manuali operativi del SGD.

Le modalità di utilizzo della delega digitale sono oggetto del presente documento solo per quanto riguarda i protocolli di comunicazione, il funzionamento del SGD come gestore di attributi qualificati e la formazione dei relativi metadata; ogni altro aspetto è demandato ai suddetti manuali operativi.

Eventuali modifiche, integrazioni e chiarimenti interpretativi in merito alle regole tecniche del SGD saranno pubblicate dall'Agenzia per l'Italia Digitale mediante il sistema normativo degli Avvisi.

Il presente documento sarà pubblicato anche su docs.italia.it. Tale edizione, revisionabile in maniera continuativa, potrà fungere anche da testo unico coordinato tra il presente Allegato Tecnico, i manuali operativi e gli eventuali suddetti Avvisi. Qualora non vi sia accordo tra le prime fonti (Regole Tecniche integrate tramite Avvisi) e la seconda (docs.italia.it), le prime avranno sempre precedenza sulla seconda.

2. Definizioni e descrizione d'insieme del SGD

Il sistema di gestione delle deleghe digitali (SGD) è un gestore di attributi qualificati (*qualified attribute authority* o q**AA**) operante secondo le specifiche SAML versione 2.0, pubblicate da OASIS. In particolare, gli standard tecnici di

riferimento sono costituiti dai seguenti documenti e relativi URL:

- [**SAMLCore**], *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0*, OASIS;
- [**SAMLMeta**], *Metadata for the OASIS Security Assertion Markup Language (SAML) v2.0*, OASIS;
- [**SAMLProfile**], *Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0*, OASIS;
- [**SAMLDel**], *SAML v2.0 Condition for Delegation Restriction*, versione 1.0, OASIS;
- [**SAMLAC**], *Authentication Context for the OASIS Security Assertion Markup Language (SAML) v2.0*, OASIS;
- [**SAMLUI**], *SAML Metadata Extensions for Login and Discovery User Interface*, versione 1.0, OASIS;
- [**XMLDSig**], *XML Signature Syntax and Processing*, W3C, nella versione utilizzata da SAML versione 2.0;
- [**HTML5**], *Hypertext Markup Language (HTML)*, W3C.

Sono inoltre elencati qui i riferimenti normativi principali:

- [**DLRecovery**], D.L. № ?? del ?? giugno 2021 e ss.mm.ii. – cd. 'Decreto *Recovery*';
- [**eIDAS**], Regolamento (UE) № 910/2014 e ss.mm.ii. – cd. 'Regolamento eIDAS';
- [**CAD**], D.Lgs. № 82 del 7 marzo 2005 e ss.mm.ii. – cd. 'Codice dell'Amministrazione Digitale';
- [**dpcmSpid**], DPCM del 24 ottobre 2014 e ss.mm.ii., pubblicato sulla G.U. № 285 del 9 dicembre 2014;
- [**eDoc**], Allegato 2 ('Formati di file e riversamento') alle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*, pubblicate da AgID sulla G.U. Serie Speciale № 259 del 19 ottobre 2020.

I soggetti che operano come fornitori di servizi delle federazioni CIE o SPID (cd. **SP**) possono offrire alcuni dei loro servizi digitali a soggetti che, già dotati di un'identità digitale nazionale e di una 'delega digitale' (cd. **delegati**) vogliono fruire di tali servizi *per conto* di soggetti terzi (cd. **deleganti**). Tali servizi sono perciò detti *delegabili*.

Per offrire uno o più servizi digitali delegabili, il SP autentica il delegato presso il proprio gestore delle identità digitali nazionali SPID o CIE (cd. **IDP**) e si accerta, presso il SGD, che egli possegga una 'delega digitale' quale attributo *qualificato* ai sensi del [**dpcmSpid**] e del [**DLRecovery**]. Tale attributo qualificato è fornito in conformità con le suddette Linee Guida ai sensi del [**CAD**], di cui il presente documento è parte integrante.

I SP che offrono servizi delegabili devono per prima cosa catalogarli in *classi di servizio delegabili*: si legga il riquadro sottostante per inquadrare le definizioni del presente capitolo nella più generale nomenclatura delle identità digitali basate sui protocolli SAML.

Nel contesto delle identità digitali nazionali, le 'classi di servizi' sono l'unità *atomica* più piccola in cui raggruppare uno o più servizi digitali nell'ambito dei protocolli SAML – cfr. [**samlCore**]. Calate nel contesto di un singolo SP, ciascuna classe di servizi è associata a un unico insieme di attributi, da veicolarsi tra due 'entità' (SP, IDP o AA) con ruoli reciproci fra di loro: il richiedente (SP, AA) e la controparte (IDP o AA). Un SP può ammettere classi di servizi distinte anche se accomunate dal medesimo insieme di attributi e, viceversa, una medesima classe di servizi utilizzata da SP differenti può essere associata a diversi sottoinsiemi di attributi (cfr. deleghe "globali," cfr §5.1).
Ciascuna entità è invece rappresentata in SAML da un *metadata*: documento informatico in formato XML, conforme sia a [**samlMeta**] che alle ulteriori norme specifiche per ciascuno schema di identificazione elettronico (SPID o CIE), sigillato elettronicamente dalla persona giuridica che gestisce tecnicamente l'entità e pubblicato su un registro autorevole a disposizione delle controparti. Infine, ciascun metadata è dotato di un identificativo univoco (stringa di testo), denominato **EntityID**.

In SAML, le classi di servizio sono definite dai SP e rappresentate nei loro metadata dagli elementi `AttributeConsumingService` (cd. **AtCS**), indicizzati mediante numeri interi non-negativi (cd. indici). Esiste perciò una corrispondenza *biunivoca* tra le classi di servizio di un SP e i suoi AtCS, anche se un SP può tecnicamente essere rappresentato da più metadata diversi.
Gli attributi SAML contenuti in una classe di servizio si distinguono ulteriormente in *attributi identificativi* (quando attestati e forniti direttamente da un IDP) e in *attributi-delega* (quando attestati e forniti dal SGD).

I SP che intendono offrire servizi delegabili si accreditano presso il SGD e gli forniscono un metadata SAML, a suo uso specifico (cd. *metadata-deleghe*, cfr. §6.2), che descrive tutte le caratteristiche delle sue classi di servizio delegabili. Gli SP hanno poi uno o più metadata che descrivono tutte le classi di servizio del SP (delegabili e non delegabili), così come presentate a ciascuno schema di identificazione elettronica nazionale e pubblicati nei relativi registri (cd. *metadata-SP*, cfr. §6.1). Il SGD ha, a sua volta, un metadata pubblicato presso il registro nazionale delle AA – come previsto dalle presenti Linee Guida – contenente la descrizione di tutti i ruoli "tecnici" svolti da tale soggetto allo scopo di consentire la creazione, la modifica e – da parte degli altri SP – la fruizione delle 'deleghe digitali' da parte del delegato (cfr. §6.3).

Ciascuna classe di servizi delegabili ha valenza nell'ambito di un SP (delega "locale" – cfr. §5.1), ovvero di più SP (delega "globale" e delega "generale" – cfr. §5.1) ed è univocamente identificata da un AtCS definito nel metadata-deleghe del SP o dei SP per i quali vengono accettate deleghe per tale classe di servizio (cfr. §6.2).

La struttura del metadata-delega del SP è descritta al §6.2 (incluse le modalità di definizione per la classi di servizio "globali"); la struttura del metadata del SGD è descritta al §6.3.

La **delega digitale** è un attributo *qualificato* costituito dall'associazione logico-matematica, creata e conservata dal SGD, tra i seguenti oggetti:

a) identità digitale di un delegato;
b) identità di un delegante;
c) una classe di servizio, ovvero una delega "generale" (cfr. §5.3);
d) *caratteristiche* della delega (quali, ad esempio la sua validità, temporale), definite al §5.

L'identità di cui al punto *a)* è costituita da attributi identificativi attestati dall'IDP del delegato e trasportati per tramite del SGD. Per alcuni scenari di utilizzo un delegato può recarsi presso una sede fisica di un SP e utilizzare la delega digitale previa identificazione *de visu*. Tali scenari, che possono non prevedere l'utilizzo dell'identità digitale del delegato (ad esempio, l'identificazione tramite documento di identità tradizionale o altre modalità previste dal [**CAD**]), sono tuttavia al di fuori dell'ambito del presente Allegato Tecnico.

L'identità di cui al punto *b)* e le caratteristiche di cui al punto *d)* sono rappresentati da attributi-delega attestati dal SGD.

Le classi di servizio (e gli identificativi degli SP) di cui al punto *c)* dipendono dalla tipologia della delega, definita al §5.1. Possono essere create al contempo più deleghe digitali, per classi di servizio delegabili e per più SP (cfr. §5.3) e, in tale fase, il sistema di creazione può riferirsi ad esse come un'unica delega digitale. Tuttavia, essendo il sistema di creazione delle deleghe digitali e della gestione del loro ciclo-cita al di fuori dell'ambito del presente Allegato Tecnico, la distinzione in merito all'unicità e alla valenza di deleghe digitali trattate mediante un'unica azione congiunta è demandata alle suddette regole operative.

I SP che offrono un servizio delegabile lo erogano secondo il flusso illustrato in Figura 1 e in base al seguente elenco

di operazioni ad alto livello, rispetto alle quali la componente qAA del SGD (anche denominato "AAD") svolge il ruolo di gestore dell'attributo qualificato 'delega digitale':

i. autenticazione del delegato presso il SP (mediante identificazione elettronica da parte di un IDP);
ii. autenticazione del medesimo delegato presso il qAA SGD (mediante identificazione elettronica da parte del medesimo IDP di cui al punto *i*);
iii. accertamento, da parte del SGD, che il delegato autenticato ai punti *i* e *ii* sia il medesimo e che disponga di almeno una delega digitale valida per la classe di servizi delegabili richiesta dal SP al punto *ii*;
iv. consenso del delegato all'utilizzo, per la fruizione della classe di servizi, di una delega digitale associata ad uno specifico delegante;[1]
v. fornitura dell'attributo qualificato al SP da parte del qAA SGD, con corrispondente erogazione del servizio digitale, da parte del SP stesso, al delegato e *per conto del* delegante selezionato al punto precedente.

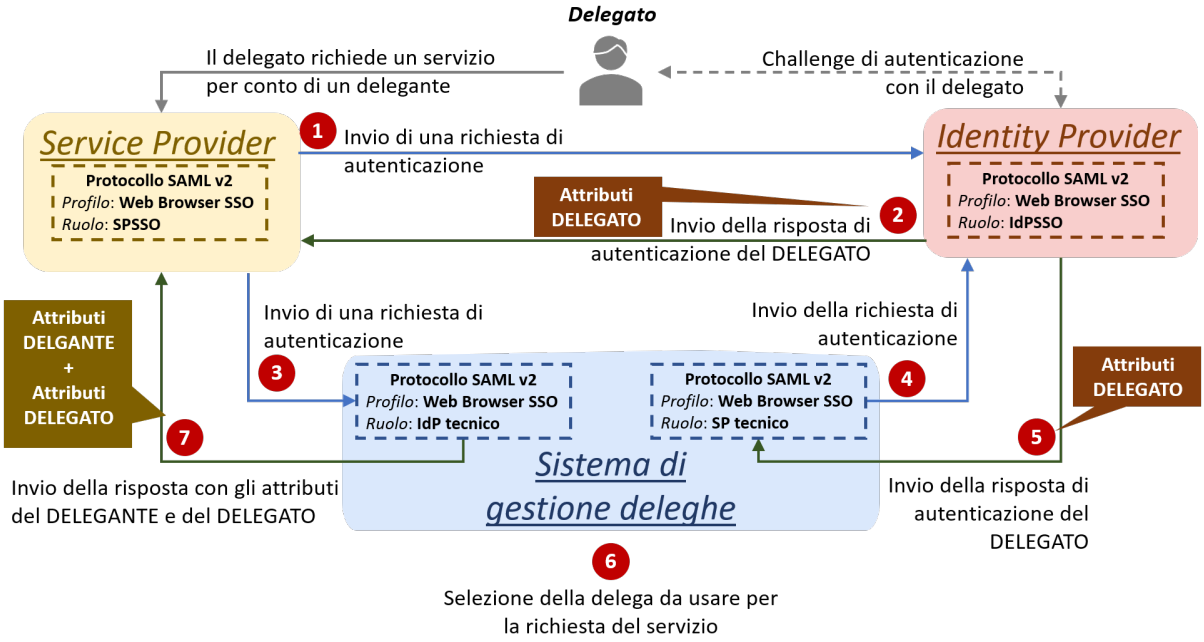

Figura 1 — Architettura generale del sistema di gestione delle deleghe digitali (SGD).

In conformità con il §4.4 delle suddette Linee Guida, il qAA SGD accetta, perciò, richieste di attributo:

- 'puntuali' (cioè contemporanee con l'autenticazione del soggetto presso il SP – cfr. punto *i*);
- 'dirette' (cioè con autenticazione del soggetto anche presso il qAA – cfr. punto *ii*);
- con rilascio del consenso alla fornitura dell'attributo qualificato (cfr. punto *iv*).

[1] È da considerare che un medesimo delegato potrebbe possedere più deleghe digitali per la medesima classe di servizi delegabili, da parte di più deleganti diversi: in tale fase, al delegato viene chiesto dal SGD di selezionare uno dei possibili deleganti per conto del quale fruire del servizio delegabile.

Nel gestire l'utilizzo delle deleghe digitali, il SP DEVE rappresentare chiaramente al delegato – mediante un'esperienza-utente (UX) accessibile secondo la vigente normativa nazionale – quando questi stia operando *per conto del* delegante e quando lo stia facendo invece per conto proprio, tenendone opportunamente traccia nei propri sistemi. Nel fare ciò, il SP PUÒ considerare di rendere "*one-shot*" l'utilizzo dell'attributo qualificato: per la fruizione di un singolo servizio delegabile, richiedendo dunque al delegato di ripetere i passaggi dal punto *ii* in poi, in caso vada utilizzata nuovamente la medesima, ovvero ulteriore delega digitale.

Qualora il sistema presso il quale avvengono le operazioni di cui ai punti *i* e *ii* afferisca alla medesima persona giuridica – dotato perciò sia di una "componente IDP" che di una "componente SGD" in grado di scambiarsi fra di loro, tramite canale *back-to-back* (*B2B*), le informazioni in merito ai soggetti autenticati presso una delle componenti, tale condizione è anche denominata di "*stesso IDP*." In tal caso, la seconda autenticazione al punto *ii* avviene comunque, ma PUÒ essere basata, anziché su un'esplicita azione di autenticazione (*challenge*) che interessi il delegato, sul *digital trust* preesistente tra le due componenti dello stesso IDP e attivato (cfr. §0) durante la prima autenticazione al punto *i*. Questa modalità di autenticazione in condizione di "stesso IDP" è denominata **autenticazione interna**: la sua applicabilità o meno è demandata al SGD e la sua architettura può essere semplificata come riportato in Figura 2 (anziché operare secondo quando mostrato in Figura 1):

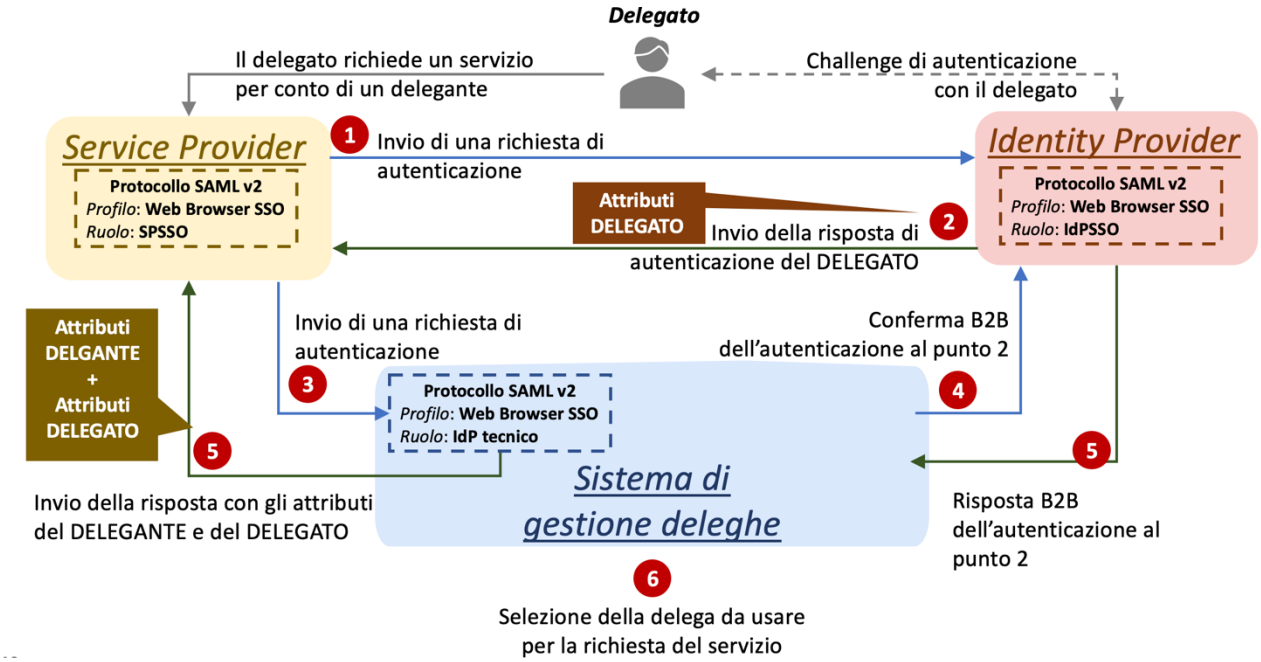

Figura 2 — Architettura generale dell'utilizzo della delega nei casi in cui il SGD e l'IDP utilizzato dal delegato per l'intero processo siano gestiti dal medesimo soggetto che, potendone usufruire tecnicamente, si avvale della modalità tramite autenticazione interna.

Si precisa che, anche nel caso di autenticazione interna, il consenso all'utilizzo della delega (e l'eventuale disambiguazione circa l'identità del delegante per il quale si intenda operare) sono sempre richiesti dal SGD al delegato, come previsto al punto *iv*.

3. Protocollo di comunicazione SAML per le deleghe digitali

Ove non sia espressamente indicato altrimenti, le regole tecniche per lo scambio di messaggi SAML tra le entità tecniche seguono il profilo *Web SSO* (*Single-Sign On*), come normato da ciascuno schema di identificazione elettronica nazionale, a sua volta basato su [**samlProfile**]. In particolare, ove tale standard preveda la possibilità o l'obbligo di apporre una 'firma digitale,' conforme con [**xmlDSig**], sulle evidenze informatiche, tale firma digitale:

a) è realizzata mediante la creazione di un sigillo elettronico avanzato sull'evidenza informatica, cfr. [**eIDAS**];
b) *salvo* ove espressamente indicato altrimenti, tale sigillo elettronico è OBBLIGATORIO;
c) il sigillo è creato mediante la chiave privata afferente a un certificato di sigillo elettronico presente nel metadata dell'ente emittente, secondo quanto normato da [**samlMeta**], dal presente documento e ss.mm.ii..
d) In alcuni casi (cfr. §4), un'evidenza informatica è contenuta (*wrapped*, cfr. [**eDoc**]) in un'altra evidenza informatica. In tal caso sono preservati gli eventuali sigilli elettronici creati su ciascuna evidenza originale, soprattutto qualora l'entità che abbia formato l'evidenza imbustata (*enveloped*) sia diversa da quella che ha formato l'evidenza imbustante (*enveloping*).

Il SGD si può comportare, di volta in volta, rispetto agli altri enti federati (SP, IDP e AA), come un "SP tecnico" ovvero come un "IDP tecnico."

I *livelli di garanzia* (cd. **LoA**) associati all'identificazione elettronica si riferiscono ai livelli 'basso' (LoA 2), 'sostanziale' (LoA 3) ed 'elevato' (LoA 4) previsti da [**eIDAS**] e corrispondono ai Livelli dall'1 al 3 per lo schema SPID. I LoA sono scelti autonomamente dai SP (cfr. Avviso SPID №4/2016) e veicolati nelle richieste di autenticazione (`AuthnRequest`) e nelle corrispondenti risposte di autenticazione SAML (`AuthnResponse`) mediante i *contesti di autenticazione* (cfr. [**samlAC**] e Avviso SPID №5/2016).

Il SGD richiede autenticazioni con livelli di garanzia mai inferiori al LoA 3/'sostanziale' (Livello 2 in SPID), pertanto:

- le richieste di autenticazione veicolate attraverso il SGD sono automaticamente **elevate** a tale LoA minimo prima di essere riformulate agli IDP come provenienti dal SGD, mediante il meccanismo della 'delega SAML' (*proxying*, cfr. [**samlDel**]); altrimenti, sono respinte;
- eventuali risposte di autenticazione che, veicolate attraverso il SGD, non corrispondano a tale LoA minimo, sono automaticamente **respinte** dal SGD, con relativo responso negativo nella fornitura della delega digitale (cfr. §7.2), prima di venire re-inoltrate al soggetto richiedente (*reverse proxying*);
- l'autenticazione interna (opzionalmente viabile solo nel caso in cui il SGD e l'IDP scelto dal delegato siano uno "stesso IDP") non è comunque adottata qualora l'autenticazione di cui al punto al punto *i* non soddisfi già il LoA minimo: in questo caso il SGD effettua una richiesta di autenticazione all'IDP compatibile con il LoA minimo e che prevede un'azione di autenticazione esplicita dell'utente;

Un SP richiede al punto *i* una prima autenticazione dell'utente con LoA minimo pari a 2/'basso' (Livello 1 SPID), ma l'utente si autentica mediante un mezzo di autenticazione con LoA pari a 3/'sostanziale' (Livello 2 SPID). Dopodiché, l'utente decide di utilizzare un servizio delegabile, per il quale al SP è sufficiente un LoA 3. Quando la richiesta di autenticazione è inoltrata al SGD, l'utente ha adottato lo 'stesso IDP' E il LoA con cui l'utente si era già effettivamente autenticato al punto *i* è pari almeno al LoA 3, il SGD PUÒ avvalersi dell'autenticazione interna.
In tutti gli altri casi, invece (stesso IDP ma con autenticazione al punto *i* effettuata con LoA inferiore a 3; stesso IDP ma con autenticazione al punto *ii* richiesta dal SP con LoA minimo pari a 4; 'IDP differente'; altra impossibilità per il SGD di avvalersi dell'autenticazione interna) il SGD richiede al punto *ii* una nuova autenticazione dell'utente presso il medesimo IDP da questi adottato al punto *i*, eventualmente elevando la richiesta ad un LoA minimo 3.

Allo scopo di consentire il corretto flusso di interrogazione dell'attributo qualificato 'delega digitale' in conformità con le Linee Guida di cui il presente documento è parte integrante, l'utilizzo della delega digitale – basato sulle estensioni ufficiali [**samlDel**] e [**samlAC**] dello standard SAML – è visivamente rappresentato nella Figura 3 e declinato nel seguente processo:

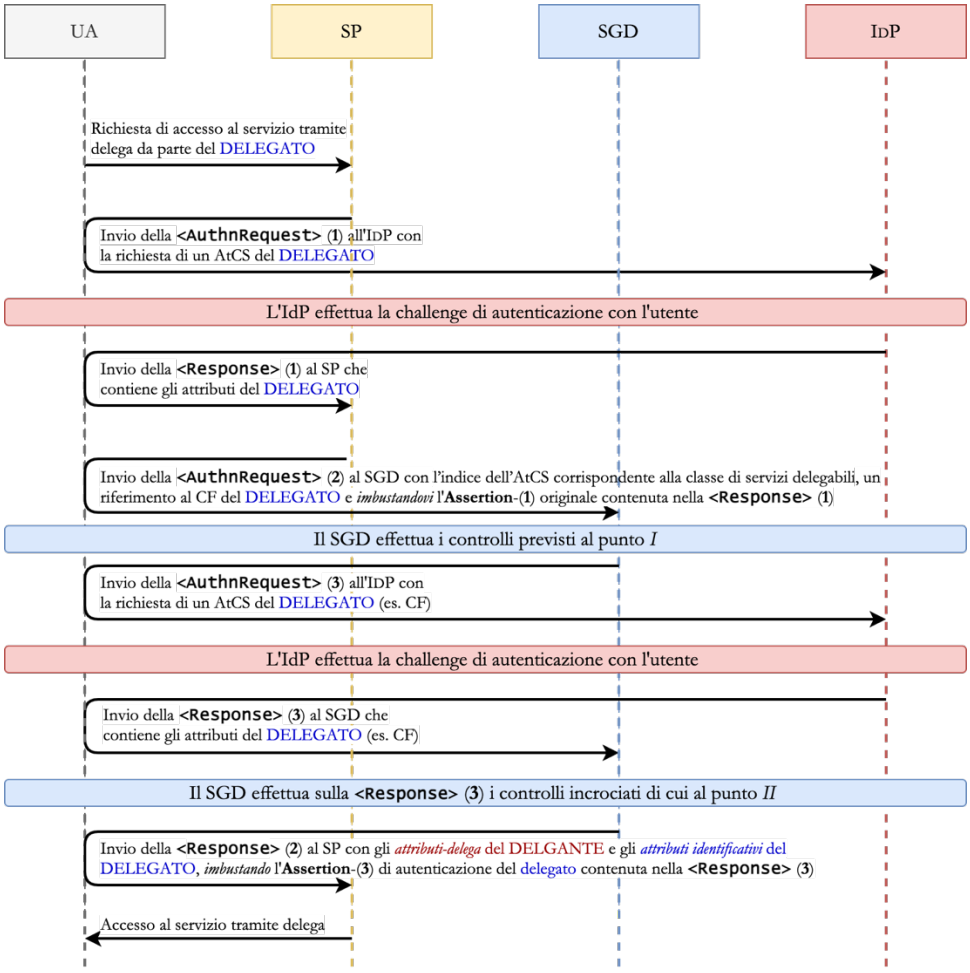

Figura 3 — Sequenza esplicativa circa la richiesta dell'attributo qualificato 'delega digitale'

1. Il soggetto[2] si autentica normalmente presso il SP; il SP invia quindi una richiesta di autenticazione SAML all'IDP scelto dal soggetto (cd. <AuthnRequest>-**1**); tale richiesta contiene l'indice di un AtCS (indicato nel metadata-*SP*) associato ad *almeno* l'attributo identificativo del codice fiscale.
2. Dopo aver effettuato l'autenticazione con opportuno LoA, l'IDP del soggetto invia la relativa risposta di autenticazione al SP (cd. <AuthnResponse>-**1**), instaurando una prima sessione autenticata tra il SP e l'IDP.

[2] In questa fase il soggetto che instaura una sessione di autenticazione presso il SP non ha ancora effettuato una richiesta di attributo qualificato delega: pertanto, non può ancora essere considerato un delegato.

3. Il soggetto indica di voler usufruire di una data classe di servizi delegabili del SP in qualità di delegato. Il SP invia quindi una richiesta di autenticazione *delegata* al SGD (cd. `<AuthnRequest>-2`, cfr. §4.1 e Figura 5), che agisce, in questa veste, da "IDP tecnico"; tale richiesta include l'IDP presso il quale il delegato si è autenticato al punto 2, almeno il codice fiscale[3] del delegato e l'indice dell'AtCS corrispondente, nel metadata-*delega* del SP, alla classe di servizi delegabili. Il SP vi imbusta inoltre l'**`Assertion-1`** originariamente contenuta nell'`<AuthnResponse>-1` di cui al punto 2 (entrambe sigillate dall'IDP), come parte integrante del suo contesto di autenticazione – cfr. [**samlAC**].
4. Il SGD, dopo aver verificato la validità e la corrispondenza tra `<AuthnRequest>-2` e **`Assertion-1`** ivi imbustata (secondo i controlli indicati nel successivo punto *I*), agisce come "SP tecnico," inviando (*proxying*) al medesimo IDP scelto dal delegato al punto 2, una nuova richiesta di autenticazione (cd. `<AuthnRequest>-3`, cfr. §4.2), relativa ad un AtCS nel proprio metadata dell'SGD (associato anch'esso al codice fiscale e ad *almeno* uno tra l'indirizzo email e il domicilio digitale del delegato).
5. L'IDP invia la relativa risposta di autenticazione al SGD (cd. `<AuthnResponse>-3`, con all'interno un'**`Assertion-3`**, entrambe sigillate elettronicamente dall'IDP) instaurando così, in caso di esito positivo, una seconda sessione autenticata – stavolta tra il SGD e l'IDP.
6. Il SGD accoglie la `<AuthnResponse>-3` di cui al punto 5, effettua i controlli specificati nel successivo punto *I.a* e, in caso siano positivi, sfruttando la relativa sessione di autenticazione in essere presso il SGD, richiede al delegato, relativamente alla classe di servizi in oggetto:
    a. qualora vi sia *una sola delega* digitale valida, l'autorizzazione al suo utilizzo (mostrando al delegato gli attributi-delega dell'unico delegante – o almeno il suo nome, cognome e codice fiscale), *ovvero*
    b. qualora vi siano *più deleghe* digitali valide (in generale per conto di deleganti diversi), la scelta di quale utilizzare tra queste, mostrando al delegato i corrispondenti attributi-delega (dei diversi deleganti – o almeno i loro nomi, cognomi e codici fiscali).

    Il SGD forma un'opportuna risposta di autenticazione *delegata* al SP (cd. `<AuthnResponse>-2`, cfr. §0 e Figura 6), contenente l'attributo qualificato 'delega digitale' sotto forma *sia* degli attributi identificativi del delegato *che* degli attributi-delega del delegante, tecnicamente veicolati in due `<Assertion>`:

    - i primi (attributi identificativi del **delegato**) sono veicolati nella prima `<Assertion>-2`***a***, che contiene esplicitamente il codice fiscale del delegato e imbusta inoltre al suo interno l'**`Assertion-3`**, quale evidenza informatica relativa all'avvenuta identificazione elettronica (e consenso) del delegato presso l'IDP (per i dettagli di questa asserzione, si legga più avanti);
    - i secondi (attributi-delega del **delegante**) sono direttamente veicolati nella seconda `<Assertion>`-**2*b*** e i loro nomi di attributo seguono la *naming convention* riportata al §6.

7. Il SP riceve la relativa risposta di autenticazione `<AuthnResponse>-2` di cui al punto 6; è tenuto a verificarne la *validità* (come previsto in [**samlCore**]) e la corrispondenza del delegato e degli attributi-delega con quanto richiesto e, in caso affermativo, concede al delegato di usufruire di un servizio appartenente alla classe di servizi delegabili indicata, per conto del delegante.

[3] Nel caso il SGD supporti deleghe digitali associate a persone fisiche dotate di identità digitali provenienti da schemi di identificazione elettronica stranieri, notificati ai sensi del Regolamento eIDAS (cfr. [**eIDAS**]), il codice fiscale è sostituito dall'identificativo di unicità della persona fisica, cioè dall'attributo eIDAS `personalIdentifier`.

Esclusivamente nel caso di autenticazione interna, secondo quanto descritto alla fine del §2, il SGD *può* semplificare ulteriormente il processo: i passaggi di cui ai punti 4 e 5 sono comunque effettuati, con conseguente produzione di un'<AuthnResponse>-**3** (e dell'**Assertion-3** ivi contenuta) da parte della "componente IDP," ma senza che il SGD richieda per questa al delegato una nuova autenticazione. Si veda a tale proposito la Figura 4.

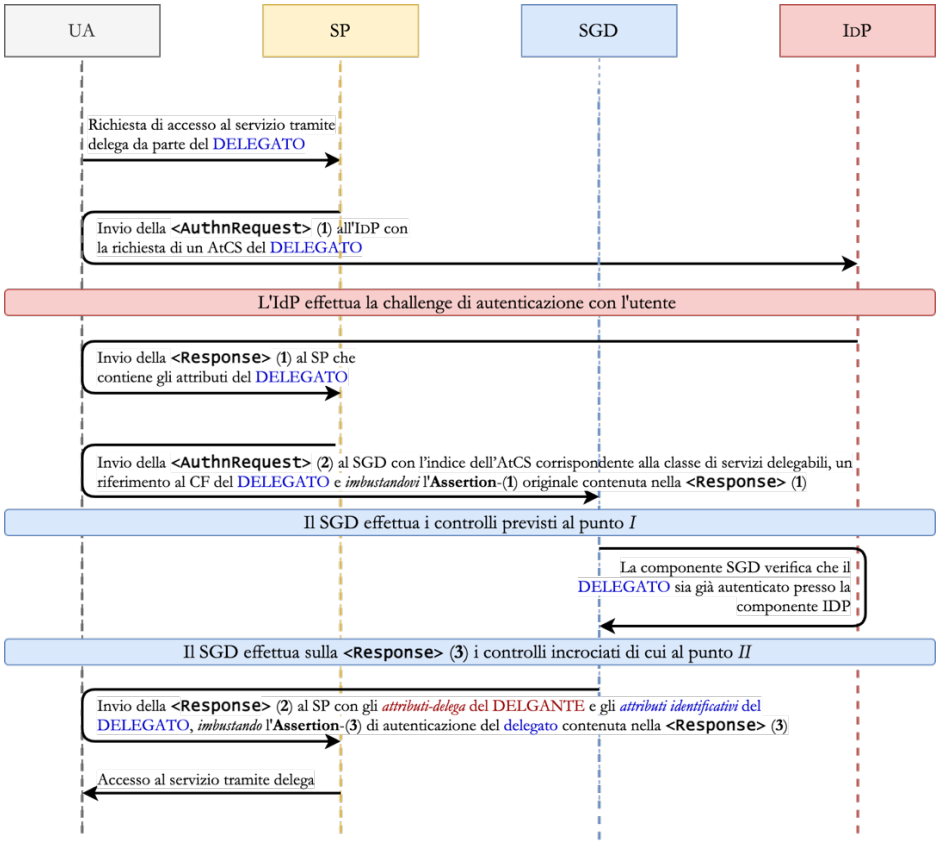

Figura 4 — Sequenza esplicativa in cui il soggetto SGD-ID riutilizza l'atenticazione del delegato.

La fruibilità da parte del delegato dell'attributo qualificato 'delega digitale' è verificata puntualmente dal SGD mediante i seguenti controlli incrociati, divisi in tre famiglie identificate da numeri romani:

I. Validità <AuthnRequest>-**2** (effettuata al punto 4), che comprende:
   - *a.* validità dell'intera richiesta di autenticazione in base allo schema di identificazione elettronica scelto dal delegato – inclusa quella del sigillo elettronico del SP;
   - *b.* validità dell'**Assertion-1** in base allo schema di identificazione elettronica adottato (inclusa quella del sigillo elettronico dell'IDP);
   - *c.* qualora il SGD stia valutando se utilizzare o meno l'**autenticazione interna**, il SGD verifica che l'**Assertion-1** fornita:
     i. esista e provenga dal "proprio IDP,"
     ii. sia associata al medesimo SP che ha effettuato le <AuthnRequest>-**1** e <AuthnRequest>-**2**,
     iii. sia relativa ad un LoA compatibile con quanto richiesto nell'<AuthnRequest>-**2**,

iv. comprenda tutti gli attributi identificativi del delegato richiesti con l'<AuthnRequest>-**2**;

d. controllo che entro il periodo di validità dell'**Assertion-1** sia compresa la validità dell'intera <AuthnRequest>-**2**;

e. controllo che la stessa <AuthnRequest>-**2** non stia venendo riutilizzata nuovamente all'interno del suo periodo di validità (invece l'**Assertion-1** POTREBBE essere riutilizzata, *finché valida*, entro determinati perimetri la cui descrizione è al di fuori dello scopo del presente documento);

f. corrispondenza del soggetto identificato al punto 2 con il delegato per il quale è richiesta l'autenticazione al punto 3 – inclusa la presenza di almeno il codice fiscale del delegato nei relativi AtCS;

g. corrispondenza dell'IDP adottato per l'identificazione presso il SP di cui al punto 2 con quello presso il quale è richiesta una nuova identificazione (presso il SGD) al punto 3;

h. conformità dei LoA rispettivamente ottenuto al punto 2 e richiesto al punto 3, con il minimo richiesto dal SGD (LoA3/'sostanziale' ai sensi di [**eIDAS**]);

i. controllo presso il SGD dell'esistenza di *almeno una* delega digitale *in corso di validità*, che associ il delegato alla classe di servizi delegabili richiesta.[4]

II. Validità dell'<AuthnResponse>-**3** (effettuata al punto 6), che comprende:

a. validità dell'intera risposta di autenticazione in base allo schema di identificazione elettronica adottato – inclusa la validità dei sigilli elettronici dell'IDP;

b. controllo che la stessa <AuthnResponse>-**3** non stia venendo riutilizzata nuovamente all'interno del suo periodo di validità;

c. corrispondenza del delegato e del suo IDP usati nell'identificazione di cui al punto 5 con quelli adottati al punto 2 – inclusa la corrispondenza del codice fiscale del delegato;

d. conformità del LoA ottenuto al punto 5 con quanto richiesto al punto 4 e con il minimo richiesto dal SGD (LoA3/'sostanziale') ai sensi di [**eIDAS**];

e. controllo che il periodo di validità dell'**Assertion-3** sia compreso entro il periodo di validità dell'**Assertion-1** – da effettuarsi *dopo* la sessione asincrona di cui ai punti 6.a o 6.b – in cui il delegato abbia autorizzato l'uso di una particolare delega digitale (per quella classe di servizi delegabili e relativa ad uno specifico delegante);

f. presenza di tutti gli attributi identificativi del **delegato** (acquisiti tramite l'**Assertion-3** al punto 5) e degli attributi-delega – sia del **delegante** che delle eventuali caratteristiche della delega (cfr. §5 in merito a questa distinzione) – così come richiesti nell'<AuthnRequest>-**2** originale al punto 3.

III. Corrispondenza, già descritta alle precedenti famiglie *I* e *II* e più nel dettaglio nel §4, tra i dati ottenuti incrociando diverse fonti (cd. '*punti di ancoraggio*'), quali:

a. le evidenze informatiche di cui ai precedenti punti dall'1 al 6;

b. la validità e i vincoli causali stante le marcature temporali elettroniche (cfr. [**eIDAS**]) nelle suddette evidenze informatiche (di cui ai suddetti punti *I.d* e *I.e*);

c. le caratteristiche della delega digitale depositata presso il SGD (cfr. §5);

d. i metadata delle entità coinvolte (quello del SGD, quello dell'IDP, così come il metadata-deleghe e il metadata-SP del SP, definiti al §6).

Nel §4 è descritta la struttura delle richieste e risposte di autenticazione SAML di cui ai precedenti punti dall'1 al 6, nel

[4] Per motivi di sicurezza, il mancato raffronto di cui al punto *i* può non comportare un immediato rifiuto da parte del SGD.

caso di esito *positivo* dell'utilizzo della delega digitale; sono altresì evidenziati tutti i punti di ancoraggio, introdotti con la famiglia *III*.

L'attributo qualificato è veicolato con esito *positivo*, dal SGD al SP, soltanto in caso abbiano avuto successo:

- l'instaurazione delle sessioni tecniche di autenticazione del delegato di cui ai punti 2, 3 e 5;
- il consenso del delegato all'uso degli attributi-delega di uno specifico delegante di cui al punto 6;
- i controlli incrociati, effettuati dal SGD, descritti nelle famiglie precedentemente numerate dalla *I* alla *III*.

Altrimenti, il SGD veicola l'avvenuto esito *negativo* – al suddetto punto 4 ovvero al punto 6, a seconda di dove questo sia stato appurato – concludendo di fatto il processo mediante l'invio al SP di opportuna risposta di autenticazione negativa, descritta nel §7.

Il SP è invece tenuto a concedere il servizio digitale – al delegato per conto del delegante – solo qualora abbiano successo tutti i controlli presenti nella successiva famiglia:

IV. Validità dell'`<AuthnResponse>`-**2**, ricevuta al punto 7, che comprende:
   a. validità sintattica dell'intera risposta di autenticazione SAML in base a quanto descritto nel §4.3 – inclusa la validità dei sigilli elettronici del SGD, così come di quello dell'IDP nell'`Assertion-3`;
   b. controllo che il periodo di validità dell'`<AuthnResponse>`-**2** e dell'`Assertion-3` sino compresi entro il periodo di validità dell'`Assertion-1`;
   c. controllo che la stessa `<AuthnResponse>`-**2** non stia venendo riutilizzata nuovamente all'interno del suo periodo di validità (invece l'`Assertion-1` e l'`Assertion-3` POTREBBERO essere riutilizzate dal SP, *finché valide*, entro determinati perimetri la cui descrizione è al di fuori dello scopo del presente documento – si legga il capoverso successivo al presente elenco);
   d. conformità del LoA richiesto al punto 4 con quanto ottenuto al punto 5;
   e. corrispondenza del codice fiscale del delegato e del suo IDP tra l'`Assertion-1` e l'`Assertion-3`;
   f. presenza di tutti gli attributi identificativi del **delegato** e degli attributi-delega – sia del **delegante** che delle eventuali caratteristiche della delega (cfr. §5 in merito a questa distinzione) – così come richiesti al punto 3 tramite l'`<AuthnRequest>`-**2**.

Le sessioni di autenticazione instaurate POSSONO essere utilizzate per fornire al delegato una UX di tipo *single sign-on* (SSO) – indipendentemente in ciascun perimetro del SP e del SGD, in conformità sia con l'omonimo profilo SAML (cfr. [**samlProfile**]) che con le normative vigenti per lo schema di identificazione elettronica adottato.[5]

Si precisa che, delle tre sessioni di autenticazione SAML descritte ai punti 2, 3 e 5:

A. la sessione tra il SP e l'IDP dell'utente di cui al punto 2 è sempre instaurata mediante *azione* di autenticazione dell'utente, oppure sfruttando SSO pregresso dell'utente, laddove previsto;
B. la sessione tra il SGD (nel suolo di "SP tecnico") e l'IDP di cui al punto 5 è instaurata mediante azione di autenticazione dell'utente, oppure sfruttando SSO pregresso dell'utente presso il SGD; qualora sia adottata l'autenticazione interna descritta in precedenza, invece, tale sessione è instaurata *automaticamente*, senza alcuna

[5] Si veda ad esempio l'Avviso SPID №3/2016.

ulteriore azione di autenticazione (venendo ereditato l'*authentication token* dalla sessione di cui al punto 2);

C. la sessione di autenticazione 'secondaria,' tra il SP e il SGD (nel ruolo di "IDP tecnico") di cui punto 3 non richiede *mai* alcuna azione da parte dell'utente,[6] essendo sempre subordinata alla sessione instaurata presso il SGD al passo 5 – tramite il meccanismo della 'delega SAML' (*proxying*) previsto in [**samlDel**] – e, in caso di autenticazione interna, a sua volta dipendente da quella di cui al passo 2.

Nel complesso, dunque, le azioni di autenticazione richieste all'utente/delegato sono al massimo *due* (punti 2 e 5), riducendosi a una sola (punto 2) in caso di sfruttamento di autenticazione interna. In caso si possa usufruire di eventuali sessioni pre-esistenti in SSO, anche queste sessioni di autenticazione possono venire instaurate automaticamente, riducendosi ulteriormente.

L'intenzione o meno, da parte dell'ente richiedente, di sfruttare un eventuale SSO pre-esistente, è veicolato dall'attributo `ForceAuthn` della relativa `<AuthnRequest>`; l'esito dell'avvenuta *challenge* o meno è indicata, dall'ente affidatario, mediante il discendente `<SubjectConfirmation>`, della relativa `<Response>`; entrambe le evidenze sono valorizzate in base ai vincoli imposti dallo schema di identificazione elettronica adottato e dal SGD stesso (cfr. §4).

Il SGD PUÒ terminare *autonomamente* entrambe le proprie sessioni di autenticazione con il delegato: quella instaurata al punto 3 presso il SP (agendo come "IDP tecnico" nei suoi confronti) e quella instaurata al punto 5 presso l'IDP (agendo come "SP tecnico" nei suoi confronti) – anche in caso di autenticazione interna. Ciò viene fatto formando messaggi di risposta e di richiesta di *single logout*, opportunamente motivati (cioè con l'attributo `Reason` valorizzato nella `<LogoutRequest>`), sigillati elettronicamente e rispettivamente inviati al SP e all'IDP. Ciò PUÒ essere fatto *automaticamente e contestualmente* con la fornitura dell'attributo qualificato 'delega digitale' al SP mediante l'`<AuthnResponse>`-**2**, al passo 6.[7] La discrezionalità in base alla quale ciò avviene è demandata al SGD e, come specificato al §2, ricade al di fuori dell'ambito del presente Allegato Tecnico.

Invece, in caso di esito *negativo* nella fornitura della delega digitale, il SGD termina *sempre* le sessioni di autenticazione del delegato che lo coinvolgono, sia come SP che come IDP "tecnico," cioè quelle instaurate ai punti 3 e 5.

Qui sotto è riportato un esempio di utilizzo congiunto di SSO e, eveutalmente, di autenticazione interna, in base al quale al delegato sono risparmiate autenticazioni successive nell'ambito di utilizzo di più servizi delegabili per conto di deleganti diversi.

Un utente che disponga di più deleghe digitali per conto di deleganti diversi (ad esempio: un cittadino delegato da diversi membri del proprio nucleo familiare o altri parenti prossimi; un tutore assegnato a più tutelati da un tribunale) si autentica presso un SP per effettuare diverse operazioni per conto proprio. Successivamente, l'utente decide di utilizzare le sue deleghe digitali per richiedere uno o più servizi delegabili per conto dei propri deleganti. In tal caso, il SP PUÒ riutilizzare la sessione di autenticazione già instaurata in base alla quale il SP ha identificato l'utente (regime di SSO), purché i LoA richiesti per tali diversi servizi delegabili siano compatibili con il contesto fornito durante la prima autenticazione.
Non appena l'utente dichiara di voler usufruire di un primo servizio delegabile, il SGD verso il quale è reindirizzato (qualora sia lo "stesso IDP" tramite il quale il delegato si è già autenticato) PUÒ valutare di avvalersi dell'autenticazione interna; in caso contrario, l'utente è chiamato ad autenticarsi una seconda volta presso il SGD in qualità di delegato.
Quando l'utente procede a richiedere nuovamente al SP un servizio delegabile (ad esempio per fruirne per conto di un

[6] Salvo la conferma o la scelta del delegante per conto del quale operare.
[7] In questo caso, è inoltre presente l'elemento `<OneTimeUse>` nell'elemento `<Conditions>` di ciascuna sua `<Assertion>`, cfr. §0.

altro delegante diverso dai precedenti), il SGD verso il quale lo stesso SP lo reindirizza ogni volta PUÒ riutilizzare la sessione di autenticazione già instaurata presso il SGD stesso (altro regime di SSO), presentandogli la sola scelta dei deleganti per i quali operare, senza richiedergli una nuova autenticazione – sempre purché tale sessione di autenticazione sia valida e compatibile con i LoA richiesti.

4. Richieste e risposte di autenticazione

Le evidenze informatiche SAML formate dal SGD seguono le norme [**samlCore**] e le ulteriori regole sintattiche sotto elencate:

a. I *namespace* XML DEVONO essere correttamente adottati in tutte le evidenze SAML.
b. Le estensioni proprie del presente sistema delle deleghe digitali sono associate al *namespace* `https://deleghedigitali.gov.it/saml-extensions`.
c. Quando siano adottati elementi estranei a *namespace* propri di SAML – cioè non definiti attraverso la sua documentazione ufficiale espressamente citata al §2 – i riferimenti a tali *namespace* (ad esempio quello di cui al punto *b*) sono esplicitamente indicati al primo utilizzo nell'evidenza informatica e, ove necessario in caso di ambiguità, in ogni altra sua occorrenza.
d. I *namespace* DOVREBBERO essere definiti tutti all'interno della radice del documento SAML, per evitare la ridondanza nelle definizioni medesime.
e. Ove il punto *d* non sia rispettabile, ad esempio per effetto dell'imbustamento (*enveloping*) di un'evidenza SAML in un'altra, andrebbero spostate quante più dichiarazioni di *namespace* possibili nell'elemento radice dell'evidenza imbustante (*enveloping*), andando ad uniformare tutti i *namespace* definiti in entrambe le evidenze originarie con gli identificativi adottati nell'evidenza imbustante.
f. Andrebbero quanto più possibile uniformate le convenzioni sintattiche circa i caratteri di spaziatura e di "a-capo" (*whitespacing*) e le virgolette adottate per la valorizzazione degli attributi XML – soprattutto nel caso di imbustamento di evidenze informatiche provenienti da sistemi differenti.
g. I punti *e* ed *f* sono derogabili soltanto nel caso in cui l'evidenza imbustata sia a sua volta dotata di sigilli elettronici, evitando così di invalidare tali sigilli.

Per facilitare l'individuazione delle corrispondenze e delle correlazioni tra le varie evidenze informatiche, da questo punto e per il resto del documento, i cosiddetti 'punti di ancoraggio' nei *payload* sono evidenziati con colori diversi, riutilizzati di volta in volta laddove la valorizzazione di un punto di ancoraggio (o il dato cui questo si riferisce indirettamente) corrisponda al valore di un altro punto di ancoraggio. Gli esempi evidenziati nei riquadri gialli si riferiscono infine a entità fittizie cui afferiscono, per gli scopi del presente documento, metadata mostrati tra gli esempi del §6.

Le evidenze informatiche di cui ai punti 1 (`<AuthnRequest>-1`), 2 (`<AuthnResponse>-1`), 4 (`<AuthnRequest>-3`) e 5 (`<AuthnResponse>-3`) del §0 sono formate in base alle regole tecniche in vigore per gli schemi di identificazione elettronica nazionali nei ruoli di IDP e SP. Gli EntityID e gli elementi XML `<AssertionConsumingService>` (cd. **AsCS**) definiti nei metadata di tali entità ed invocati nelle evidenze informatiche ai suddetti punti, sono qui evidenziati in quanto referenziati dalle altre evidenze informatiche descritte nei successivi sotto-capitoli.

Per quanto riguarda i messaggi scambiati con il SGD, gli AtCS e gli AsCS sono sempre passati *per riferimento* al loro

indice[8] nelle richieste e risposte di autenticazione SAML.

- L'<AuthnRequest>-**1** (punto 1) ha un determinato ID (che DEVE cominciare con **id-**) ed è inviata ad un AsCS (definito nel metadata-SP del SP); ha come **<Issuer>** l'EntityID-SP del SP e come **<Audience>** (nonché come attributo **Destination** della radice) l'EntityID dell'IDP;

```
<samlp:AuthnRequest
  AttributeConsumingServiceIndex="40"
  AssertionConsumerServiceURL="https://www.SPdiesempio.it/binding/http-post"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Destination="https://idserver.servizicie.interno.gov.it/idp"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
  ForceAuthn="true"
  IssueInstant="2021-03-21T10:30:00Z"
  ID="id-ZR9KpyZ0h8JFRCRC4eGpuZii-6r52tJlpV7bCsXD"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      NameQualifier="https://www.SPdiesempio.it">
            https://www.SPdiesempio.it
    </saml:Issuer>
    <ds:Signature> [……] </ds:Signature>
    <samlp:NameIDPolicy
      AllowCreate="true"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
    <samlp:RequestedAuthnContext Comparison="minimum">
            <saml:AuthnContextClassRef>
                    https://www.spid.gov.it/SpidL2
            </saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
    <saml:Conditions
      NotBefore="2021-03-21T10:30:00Z"
      NotOnOrAfter="2021-03-21T10:32:00Z">
      <saml:AudienceRestriction>
            <saml:Audience>https://idserver.servizicie.interno.gov.it/idp</saml:Audience>
      </saml:AudienceRestriction>
  </saml:Conditions>
</samlp:AuthnRequest>
```

- L'<AuthnResponse>-**1** (punto 2) ha un priorio ID ed è inviata al sopracitato AsCS; PUÒ essere sigillata elettronicamente dall'IDP; ha come **<Issuer>** l'EntityID dell'IDP, come **<Audience>** l'EntityID-SP del SP e come **<Subject>** l'identità dell'*utente* (identificato tramite un <NameID> generato dall'IDP). Contiene al suo interno una **<Assertion>-1** che DEVE essere sigillata elettronicamente dall'IDP.

```
<samlp:Response
  Destination="https://www.SPdiesempio.it"
  ID="9bcd87d-300e-bb96-c2f1-8eebb276f9a2"
```

[8] Cioè indicati, rispettivamente, tramite attributi **AttributeConsumingServiceIndex** e **AssertionConsumerServiceIndex**.

```
InResponseTo="id-ZR9KpyZ0h8JFRCRC4eGpuZii-6r52tJlpV7bCsXD"
IssueInstant="2021-03-21T10:31:00Z"
Version="2.0"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
          https://idserver.servizicie.interno.gov.it/idp
  </saml:Issuer>
  <ds:Signature>  [……]  </ds:Signature>
  <samlp:Status>
          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion
    ID="_e5cdedd6-36aa-43a8-bce1-0d5ede7344d3"
    IssueInstant="2021-03-21T10:32:00Z"
    Version="2.0">
          <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                  https://idserver.servizicie.interno.gov.it/idp
          </saml:Issuer>
          <ds:Signature>  [……]  </ds:Signature>
          <saml:Subject>
                  <saml:NameID
                    Format="urn:oasis:names:tc:2.0:nameid-format:transient"
                    NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
                    SPNameQualifier="https://www.SPdiesempio.it">
                          AAdzZWNyZXQx/cGt/T65P/3/jHt6frP0TASuN5FvymMCBzfA6IA6Ofps6
                  </saml:NameID>
                  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                          <saml:SubjectConfirmationData
                            InResponseTo="id-ZR9KpyZ0h8JFRCRC4eGpuZii-6r52tJlpV7bCsXD"
                            NotOnOrAfter="2021-03-21T10:36:00Z"
                            Recipient="https://www.SPdiesempio.it/binding/http-post"/>
                  </saml:SubjectConfirmation>
          </saml:Subject>
          <saml:Conditions
            NotBefore="2021-03-21T10:31:00Z"
            NotOnOrAfter="2021-03-21T10:36:00Z">
                  <saml:OneTimeUse/>
                  <saml:AudienceRestriction>
                          <saml:Audience>https://www.SPdiesempio.it</saml:Audience>
                  </saml:AudienceRestriction>
          </saml:Conditions>
          <saml:AuthnStatement
            AuthnInstant="2021-03-21T10:31:00Z"
            SessionIndex="_5af1591d-3203-4ef4-8e1a-02c5dc0d90fc">
                  <saml:AuthnContext>
                          <saml:AuthnContextClassRef>
                                  https://www.spid.gov.it/SpidL2
                          </saml:AuthnContextClassRef>
                  </saml:AuthnContext>
          </saml:AuthnStatement>
          <saml:AttributeStatement>
                  <saml:Attribute
```

```
                    Name="fiscalNumber"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                        <saml:AttributeValue xsi:type="xs:string">
                            TINIT-RSSMROyyMddC999X
                        </saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

- Per la <AuthnRequest>-**3** (punto 4) si veda il §4.2.
- L'<AuthnResponse>-**3** (punto 5), PUÒ essere sigillata elettronicamente dall'IDP, ha un determinato ID (si RACCOMANDA cominci per **del:id-**), è emessa ad un certo orario (IssueInstant), ha come <Issuer> l'EntityID dell'IDP e come <Audience> l'EntityID del SGD. Contiene al suo interno una <Assertion>-**3** che DEVE essere sigillata elettronicamente dall'IDP, emessa dal medesimo <Issuer>, con gli attributi identificativi del *delegato* (identificato da un nuovo <NameID>) e che devono includere *almeno* il codice fiscale.

```
<samlp:Response
  Destination="https://deleghedigitali.gov.it"
  ID="ebb276f-67b4-cbd0-22f1-899bcd87ea2"
  InResponseTo="del:id-pyZ0a1a824dba354bcbba9dh8JFRa8108f55cc19"
  IssueInstant="2021-03-21T10:33:30Z"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature> [……] </ds:Signature>
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
            https://idserver.servizicie.interno.gov.it/idp
    </saml:Issuer>
    <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Assertion
      ID="_de7344d3-36aa-8a34-1ecb-0d5ee5cdedd6"
      IssueInstant="2021-03-21T10:33:30Z"
      Version="2.0"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <ds:Signature> [……] </ds:Signature>
            <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                    https://idserver.servizicie.interno.gov.it/idp
            </saml:Issuer>
            <saml:Subject>
                    <saml:NameID
                      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                      NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
                      SPNameQualifier="https://deleghedigitali.gov.it">
                            AAdzZWNyZXQxDX5jaZEES999t3SRsMjrfFcrQbuxVinXmmQpi/+nv2PFVVyIE
                    </saml:NameID>
                    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                            <saml:SubjectConfirmationData
```

```
                        InResponseTo="del:id-pyZ0a1a824dba354bcbba9dh8JFRa8108f55cc19"
                        NotOnOrAfter="2021-03-21T10:38:30Z"
                        Recipient="https://deleghedigitali.gov.it/saml-sp/asscs/post"/>
                </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
          NotBefore="2021-03-21T10:33:30Z"
          NotOnOrAfter="2021-03-21T10:38:30Z">
                <saml:OneTimeUse/>
                <saml:AudienceRestriction>
                        <saml:Audience>https://deleghedigitali.gov.it</saml:Audience>
                </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
          AuthnInstant="2021-03-21T10:33:30Z"
          SessionIndex="_30cdbc90-36a7-465d-807f-9238edd337a5">
                <saml:AuthnContext>
                        <saml:AuthnContextClassRef>
                                https://www.spid.gov.it/SpidL3
                        </saml:AuthnContextClassRef>
                </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
                <saml:Attribute
                  Name="fiscalNumber"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                        <saml:AttributeValue xsi:type="xs:string">
                                TINIT-RSSMROyyMddC999X
                        </saml:AttributeValue>
                </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

I rimanenti messaggi (inclusa la <AuthnRequest>-**3** di cui al punto 4) sono formati seguendo regole specifiche nel presente Allegato Tecnico, finalizzate sia ad irrobustire il *binding* crittografico, che ad individuare il preciso collocamento di tutte le evidenze necessarie per l'utilizzo e la corretta comunicazione della delega digitale.

4.1. AuthnRequest-2 (passo 3)

Al punto 3 del §0 la <AuthnRequest>-**2** è inviata dal SP (tramite il proprio sistema-deleghe) al SGD, per identificare sia il delegato (tramite attributi identificativi) che il delegante (tramite attributi-delega).

In particolare, la <AuthnRequest>-**2** è costituita da un elemento <samlp:AuthnRequest> il cui soggetto fa riferimento all'identità del delegato (esplicitamente referenziata tramite il suo codice fiscale), già precedentemente autenticato presso il SP. La caratteristica peculiare di questo messaggio è che il suo *contesto di autenticazione* è rappresentato dall'evidenza informatica che garantisce l'instauro di una precedente sessione di autenticazione tra IDP e SP, la cui validità viene contestualmente controllata (anche in caso si adotti l'autenticazione interna, cfr. §2). Ciò è tecnicamente realizzato rappresentando il contesto di autenticazione come un elemento <sgd:Evidence> imbustante l'<saml:Assertion> originale (<Assertion>-**1**), come visivamente rappresentato in Figura 5.

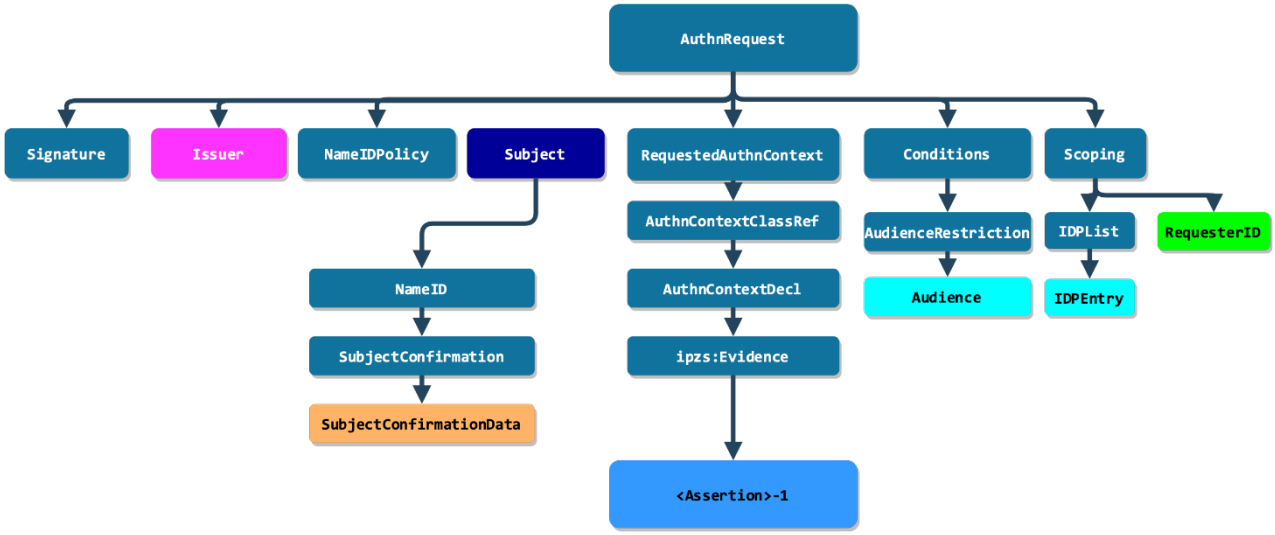

Figura 5 — Anatomia di dettaglio dell'<AuthnRequest>-2: i 'punti di ancoraggio' di questa particolare evidenza SAML con le altre descritte al §4 sono indicati con gli stessi colori utilizzati nel resto del documento.

Più in particolare, la struttura della richiesta di autenticazione SAML è così costituita:

- <AuthnRequest>, DEVE essere sigillata elettronicamente dal SP (in base alla chiave afferente al certificato per la creazione di sigilli elettronici presente nel metadata-delega del SP – cfr. §6.2); contiene inoltre i seguenti attributi ed elementi:
  - `Destination`, pari all'EntityID del SGD;
  - `AttributeConsumingServiceIndex`, valorizzato con l'indice dell'AtCS nel metadata-delega del SP per l'insieme comprendente sia agli attributi identificativi del delegato (inclusivo almeno del codice fiscale) che gli attributi-delega, cioè gli attributi identificativi del delegante più eventuali altre caratteristiche facoltative della delega (p.es. attributi specific), cfr. §5;
  - `AssertionConsumerServiceIndex`, valorizzato con l'indice dell'AsCS nel metadata-delega del SP, relativo ad un *binding* HTTP POST (a scelta del SP nel caso vi sia più di un AsCS con tale *binding*) – e da *non* confondersi con l'AsCS nel metadata-SP del SP e utilizzato in <AuthnRequest>-1 e <AuthnResponse>-1;
  - `Consent`, pari a `urn:oasis:names:tc:SAML:2.0:consent:prior`;
  - `ForceAuthn`, pari a `false`;
  - `IsPassive`, pari a `false`;
  - `ID`, RACCOMANDATO essere un ID univoco (come un *hash* o un UUID) che comincia con la stringa **`del:attr-`**.
- `<Issuer>` contenente l'EntityID-deleghe del SP (che *DOVREBBE* ricavarsi l'EntityID-SP del SP con aggiunto il prefisso `del:`).
- <Subject> (relativo al delegato) contenente i seguenti elementi:
  - <NameID>, valorizzato con l'ID univoco valorizzante l'elemento <NameID> associata al *delegato*, caratterizzante l'<Assertion>- (che è re-imbustata nell'elemento <sgd:Evidence> della presente <AuthnRequest>-2) con, inoltre, i seguenti attributi:

        - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`;
        - `NameQualifier` valorizzato con l'EntityID dell'IDP;
        - `SPNameQualifier` valorizzato con l'EntityID-SP del SP;
    - `<SubjectConfirmation>`, con attributo contenente `Format`pari a `urn:oasis:names:tc:SAML:2.0:cm:bearer` e l'elemento `<SubjectConfirmationData>` dotato dei seguenti attributi:
        - `InResponseTo` valorizzato con l'ID univoco dell'attributo `ID` della `<AuthnRequest>`-**1**;
        - `NotOnOrAfter`, valorizzato con l'orario di scadenza di questa richiesta di autenticazione (entro la quale deve essere fornita la `<AuthnResponse>`-**2** al passo 6 e, quindi, la conclusione dell'intero processo di autenticazione per delega);
        - `Recipient`, valorizzato con l'AsCS originale sulla quale il SP ha ricevuto la `<AuthnRequest>`-**1**;
- `<NameIDPolicy>`, contenente seguenti attributi:
    - `AllowCreate`, pari a `false`;
    - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
- `<RequestedAuthnContext>`, contenente i seguenti elementi:
    - `<AuthnContextClassRef>`, valorizzato come "`urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession`, ex [**samlAC**];
    - `<AuthnContextClassDecl>`, contenente l'estensione `<sgd:Evidence>` (da non confondere con l'elemento `<samlp:Evidence>` previsto in [**samlCore**]), che a sua volta contiene i seguenti:
        - l'attributo `AllowCreate`, pari a `false`;
        - l'intera `<Assertion>`-**1** presente nell'`<AuthnResponse>`-**1** (già sigillata elettronicamente dall'IDP) – che viene perciò usata come un vero e proprio *authentication token* per la sessione instaurata dal delegato presso il SGD:
            - `<NameID>`, valorizzato con il valore del `<NameID>` che identifica il delegato nel contesto dell'IDP (nell'`<AuthnResponse>`-**1**), con i seguenti attributi:
                - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`;
                - `NameQualifier` valorizzato con l'EntityID dell'IDP;
                - `SPNameQualifier` valorizzato con l'EntityID-SP del SP;
- `<Conditions>`, contenente:
    - l'attributo `NotBefore`, valorizzato con l'orario con cui la richiesta stessa è stata emessa;
    - l'attributo `NotOnOrAfter`, valorizzato l'orario più avanzato entro la quale il SP può mantenere attiva la sessione di autenticazione dell'utente in qualità delegato (per distinguerla dalla sessione già instaurata in cui il medesimo soggetto agisce per proprio conto); il SP DOVREBBE mantenere questa durata complessiva al valore minimo possibile per fornire al delegato, in sicurezza, il servizio richiesto; la durata effettiva sarà comunque subordinata alla validità temporale della corrispondente `<AuthnResponse>`-**2** ricevuta dal SGD;
    - l'elemento `<AudienceRestrictions>`, contenente *un solo* elemento:
        - `<Audience>`, valorizzato con l'EntityID dell'IDP utilizzato dal SP `<AuthnResponse>`-**1** per autenticare originariamente il delegato presso il SP e che verrà riutilizzato nell'`<AuthnResponse>`-**3** per identificare nuovamente il medesimo delegato presso il SGD.

- `<Scoping>`, contenente:
  - l'attributo `ProxyCount` pari a `1`;
  - l'elemento `<IDPList>`, contenente *un solo* figlio `<IDPEntry>` con:
    - l'attributo `ProviderID`, pari all'EntityID dell'IDP da usarsi come intermediario;
    - l'elemento `<Name>`, pari al valore dell'elemento `<OrganizationDisplayName>` nel metadata dell'IDP;
  - l'elemento `<RequesterID>`, valorizzato con l'EntityID del SGD.

Qui sotto è riportato un esempio di `<AuthnRequest>`-**2**, con evidenziata l'`<Assertion>-1` imbustata all'interno (cfr. Figura 5).

```
<samlp:AuthnRequest
  AttributeConsumingServiceIndex="2"
  AssertionConsumerServiceIndex="0"
  Destination="https://deleghedigitali.gov.it"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:prior"
  ForceAuthn="false"
  IsPassive="false"
  IssueInstant="2021-03-21T10:32:00Z"
  ID="del:attr-9R9FzkZ0h8JFRCRC4eGpuZii-6r52tJlpV7b5A9e"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:sgd="https://deleghedigitali.gov.it/saml-extensions"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature> [……] </ds:Signature>
    <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      NameQualifier="https://www.SPdiesempio.it">
            del:https://www.SPdiesempio.it
    </saml:Issuer>
    <saml:Subject>
            <saml:NameID
              Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
              NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
              SPNameQualifier="del:https://www.SPdiesempio.it">
                    AAdzZWNyZXQx/cGt/T65P/3/jHt6frP0TASuN5FvymMCBzfA6IA6Ofps6
            </saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData
                      InResponseTo="id-ZR9KpyZ0h8JFRCRC4eGpuZii-6r52tJlpV7bCsXD"
                      NotOnOrAfter="2021-03-21T10:34:00Z"
                      Recipient="https://www.SPdiesempio.it/binding/http-post"/>
            </saml:SubjectConfirmation>
    </saml:Subject>
    <samlp:NameIDPolicy
      AllowCreate="false"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
    <samlp:RequestedAuthnContext>
            <saml:AuthnContextClassRef>
                    urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
            </saml:AuthnContextClassRef>
            <saml:AuthnContextDecl>
```

```
<sgd:Evidence
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Assertion
      ID="_e5cdedd6-36aa-43a8-bce1-0d5ede7344d3"
      IssueInstant="2021-03-21T10:31:30Z"
      Version="2.0">
        <saml:Issuer
          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
            https://idserver.servizicie.interno.gov.it/idp
        </saml:Issuer>
        <ds:Signature> [……] </ds:Signature>
        <saml:Subject>
            <saml:NameID
          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
          NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
              SPNameQualifier="https://www.SPdiesempio.it">
            AAdzZWNyZXQx/cGt/T65P/3/jHt6frP0TASuN5FvymMCBzfA6IA6Ofps6
            </saml:NameID>
            <saml:SubjectConfirmation
              Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData
                  InResponseTo="id-ZR9KpyZ0h8J[……]bCsXD"
                  NotOnOrAfter="2021-03-21T10:32:00Z"
             Recipient="https://www.SPdiesempio.it/binding/http-post"
                  />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
          NotBefore="2021-03-21T10:31:30Z"
          NotOnOrAfter="2021-03-21T10:32:00Z">
            <saml:OneTimeUse/>
            <saml:AudienceRestriction>
                <saml:Audience>
                    https://www.SPdiesempio.it
                </saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement
          AuthnInstant="2021-03-21T10:31:30Z"
          SessionIndex="_5af1591d-3203-4ef4-8e1a-02c5dc0d90fc">
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>
                    https://www.spid.gov.it/SpidL2
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute
              Name="fiscalNumber"
              NameFormat="urn:oasis:[……]:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">
                    TINIT-RSSMROyyMddC999X
                </saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
```

```
                    </saml:Assertion>
                </sgd:Evidence>
            </saml:AuthnContextDecl>
    </samlp:RequestedAuthnContext>
    <saml:Conditions
      NotBefore="2021-03-21T10:32:00Z"
      NotOnOrAfter="2021-03-21T10:34:00Z">
            <saml:AudienceRestriction>
                    <saml:Audience>https://deleghedigitali.gov.it</saml:Audience>
            </saml:AudienceRestriction>
    </saml:Conditions>
    <samlp:Scoping ProxyCount="1">
            <samlp:IDPList>
                    <samlp:IDPEntry
                      ProviderID="https://idserver.servizicie.interno.gov.it/idp"
                      Name="Ministero dell'Interno"/>
            </samlp:IDPList>
            <samlp:RequesterID>https://deleghedigitali.gov.it</samlp:RequesterID>
    </samlp:Scoping>
</samlp:AuthnRequest>
```

4.2. `AuthnRequest-3` (passo 4)

Al punto 4 del §0 l'<`AuthnRequest`>-**3** è inviata dal SGD all'IDP (lo stesso invocato dal SP al passo 1) per autenticare nuovamente il delegato, instaurando questa volta una sessione tra questi e il SGD – ma crittograficamente "legata" alla sessione di autenticazione instaurata, tramite la <`AuthnResponse`>-**1**, tra il SP e il medesimo IDP.

- <**`AuthnRequest`**>, DEVE essere sigillata elettronicamente dal SGD e contiene i seguenti attributi ed elementi:
  - `ProviderName`, valorizzato con una stringa del tipo "*`EntityID-SGD per conto di EntityID-SP`*";
  - `Destination`, pari all'EntityID dell'IDP utilizzato nell'<`AuthnRequest`>-**1**;
  - `AttributeConsumingServiceIndex`, valorizzato con l'indice dell'AtCS nel metadata del SGD per l'insieme comprendente gli attributi identificativi del **delegato**, di cui almeno il codice fiscale. Qualora il SP richiedesse attributi identificativi ulteriori del delegato e questi sono stati veicolati dal SP al SGD con l'**`<Assertion>-1`** imbustata all'interno della <`AuthnRequest`>-**2**, non è necessario che il SGD li chieda nuovamente all'IDP con l'<`AuthnRequest`>-**3**. Qualora, invece, tali attributi ulteriori non siano stati già forniti con l'**`<Assertion>-1`**, il SGD PUÒ richiederli esplicitamente all'IDP con l'<`AuthnRequest`>-**3**, oppure restituire risposta negativa in tal senso al SP (cfr. §7.2).
  - `AssertionConsumerServiceIndex`, valorizzato con l'indice dell'AsCS nel metadata del SGD, relativo ad un *binding* HTTP POST (a scelta del SGD nel caso vi sia più di un AsCS con tale *binding*);
  - `Consent`, pari a `urn:oasis:names:tc:SAML:2.0:consent:prior`;
  - `ForceAuthn`, pari a `false` *solo* in caso l'SGD sia lo "stesso IDP" e stia adottando autenticazione interna – in tutti gli altri casi pari a `true`;
  - `isPassive`, pari a `true` *solo* in caso l'SGD stia adottando autenticazione interna – in tutti gli altri casi pari a `false`;
  - `ID` RACCOMANDATO essere un ID univoco (come un *hash* o un UUID) che comincia con la stringa **`del:id-`**.
- `<Issuer>`, contiene l'EntityID dell'SDG e i seguenti attributi.

  - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`;
  - `NameQualifier` e l'elemento stesso, valorizzati entrambi con l'EntityID del SGD.
- `<NameIDPolicy>`, contenente i seguenti attributi;
  - `AllowCreate`, pari a `false`;
  - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
- `<RequestedAuthnContext>`, contenente, *alternativamente*:
  - qualora ci si trovi nella condizione di "stesso IDP" e il SGD adotti l'autenticazione interna:
    - l'elemento `<AuthnContextDeclRef>`, valorizzato con l'ID dell'`<AuthnResponse>`-**1**;
  - qualora il SP abbia identificato la classe di servizi come usufruibile mediante un'autenticazione solo con il massimo *livello di garanzia* (LoA **4**, equivalente a quello della CIE e al Livello 3 di SPID):
    - l'attributo `Comparison`, pari ad `exact`,
    - l'elemento `<AuthnContextClassRef>`, valorizzato con l'URI corrispondente al LoA 4;
  - in ogni altro caso, il livello di autenticazione richiesto *non deve* essere inferiore al LoA **3**:
    - l'attributo `Comparison`, pari a `minimum`,
    - l'elemento `<AuthnContextClassRef>`, valorizzato con l'URI corrispondente al LoA 3;
- `<Conditions>`, contenente:
  - attributi `NotBefore` e `NotOnOrAfter` valorizzati, rispettivamente, con l'orario con cui la presente richiesta viene emessa e con l'orario di scadenza della stessa, a scelta dell'SGD e che:
    - qualora non sia utilizzato il SSO per la sessione instaurata presso il SGD, o la sessione sarà comunque terminata immediatamente dopo l'utilizzo, non è superiore a due minuti,
    - qualora la sessione attuale sia utilizzabile in regime di SSO presso il SGD, ha una durata massima conforme con la normativa prevista per gli schemi di identificazione nazionale;
  - l'elemento `<AudienceRestriction>`, contenente *un solo* elemento:
    - `<Audience>`, valorizzato con l'EntityID dell'IDP;

Qui sotto è riportato un primo esempio di `<AuthnRequest>`-**3** inviata dal SGD a un IDP generico.

```
<samlp:AuthnRequest
  ProviderName="“SGD:OrganizationDisplayName” per conto di “SP:OrganizationDisplayName”"
  AttributeConsumingServiceIndex="0"
  AssertionConsumerServiceIndex="0"
  Destination="https://idserver.servizicie.interno.gov.it/idp"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:prior"
  ForceAuthn="true"
  IsPassive="false"
  IssueInstant="2021-03-21T10:32:30Z"
  ID="del:id-pyZ0a1a824dba354bcbba9dh8JFRa8108f55cc19"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature>  [……]  </ds:Signature>
    <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      NameQualifier="https://deleghedigitali.gov.it">
            https://deleghedigitali.gov.it
    </saml:Issuer>
    <samlp:NameIDPolicy
```

```
      AllowCreate="false"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
    <samlp:RequestedAuthnContext Comparison="minimum">
            <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL2</saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
    <saml:Conditions
      NotBefore="2021-03-21T10:32:30Z"
      NotOnOrAfter="2021-03-21T10:34:30Z">
            <saml:AudienceRestriction>
                    <saml:Audience>https://idserver.servizicie.interno.gov.it/idp</saml:Audience>
            </saml:AudienceRestriction>
    </saml:Conditions>
</samlp:AuthnRequest>
```

Nell'esempio qui sotto, invece, la medesima <AuthnRequest>-**3** è inviata internamente dal SGD verso la propria "componente IDP" nel caso di autenticazione interna.

```
<samlp:AuthnRequest
  ProviderName="“SGD:OrganizationDisplayName” per conto di “SP:OrganizationDisplayName”"
  AttributeConsumingServiceIndex="0"
  AssertionConsumerServiceIndex="0"
  Destination="https://deleghedigitali.gov.it/idp"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:prior"
  ForceAuthn="false"
  IsPassive="true"
  IssueInstant="2021-03-21T10:32:30Z"
  ID="del:id-p91cc55f8088aRFH8hd9abbcb453abd428a1a0Zyp"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature>  [……]  </ds:Signature>
    <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      NameQualifier="https://deleghedigitali.gov.it">
            https://deleghedigitali.gov.it
    </saml:Issuer>
    <samlp:NameIDPolicy
      AllowCreate="false"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
    <samlp:RequestedAuthnContext>
            <saml:AuthnContextDeclRef>ebb276f-67b4-cbd0-22f1-899bcd87ea2</saml:AuthnContextDeclRef>
    </samlp:RequestedAuthnContext>
    <saml:Conditions
      NotBefore="2021-03-21T10:32:30Z"
      NotOnOrAfter="2021-03-21T10:34:30Z">
            <saml:AudienceRestriction>
                    <saml:Audience>https://deleghedigitali.gov.it/idp</saml:Audience>
            </saml:AudienceRestriction>
    </saml:Conditions>
</samlp:AuthnRequest>
```

4.3. AuthnResponse-2 (passo 6)

Al punto 6 del §0 la <AuthnResponse>-**2** è restituita dal SGD al SP (sul proprio sistema-deleghe) e contiene sia

l'identità del delegato (tramite attributi identificativi) che quella del delegante (tramite attributi-delega).

In particolare, la `<AuthnResponse>`-**2** è costituita da un elemento `<samlp:Response>` che DEVE essere sigillato elettronicamente dal SGD, ha il delegato come soggetto e al cui interno sono contenute due `<saml:Assertion>` distinte, che POSSONO essere sigillate elettronicamente dal SGD,[9] come illustrato visivamente in Figura 6:

- una prima **`<Assertion>`** (denominata "2*a*," formata dal SGD), avente il delegato come soggetto e al suo interno un elemento `<saml:Advice>`, contenente:
    - un *riferimento* all'`<Assertion>-1` (formata e sigillata dall'IDP) proveniente dall'`<AuthnResponse>`-**1** originale, relativa al medesimo delegato; può essere omessa solo in caso di "stesso IDP";
    - l'intera `<Assertion>-3` (anch'essa formata e sigillata dall'IDP), contenente gli attributi identificativi del **delegato** e che:
        - era originariamente imbustata all'interno dell'`<AuthnResponse>`-**3**, *oppure*;
        - nel caso il SGD abbia usufruito dell'autenticazione interna (cfr. §2), può coincidere, ed è perciò un riutilizzo dell'`<Assertion>-1`;
- una seconda **`<Assertion>`** (denominata "2*b*," formata dal SGD), avente il **delegante** come soggetto e contenente i suoi attributi-delega.

[9] Tale possibilità deriva dal fatto che le due `<Assertion>` emesse dal SGD hanno validità solo se considerate insieme, in quanto è la loro mutua associazione a costituire l'attributo qualificato 'delega digitale': separate l'una dall'altra, NON DEVONO essere utilizzate in alcun contesto da parte di entità terze, da cui l'opportunità per il SGD di non creare sigilli elettronici sulle due evidenze singolarmente.

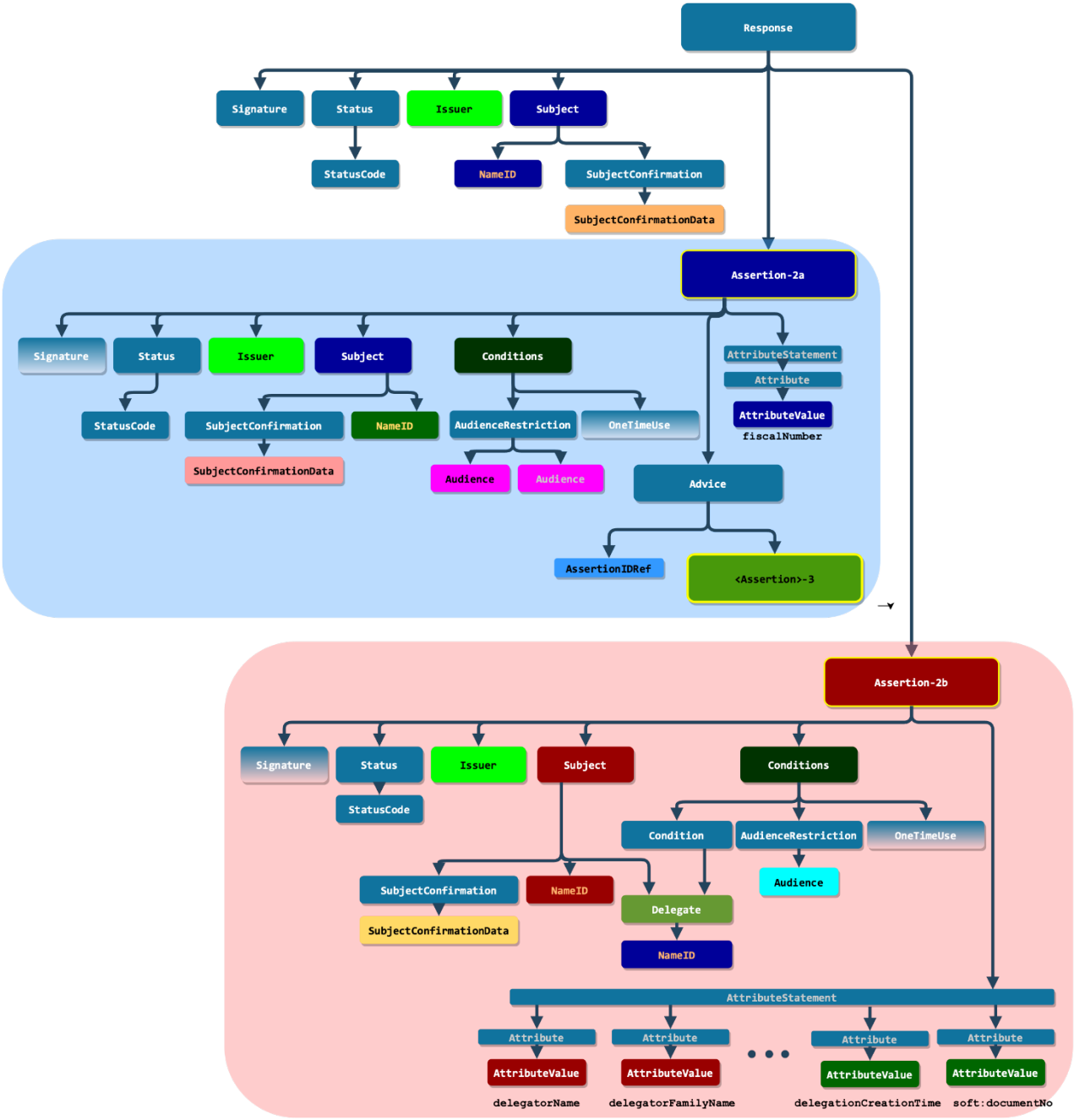

Figura 6 — Anatomia dell'<AuthnResponse>-2, i cui 'punti di ancoraggio' sono evidenziati con gli stessi colori utilizzati nel resto del testo. Gli elementi <Signature> e <OneTimeUse>, presenti sia in <Assertion>-2*a* che in <Assertion>-2*b*, sono *facoltativi* (cfr. loro descrizione nel testo).

Più in particolare, la struttura della risposta di autenticazione SAML è così costituita:

- <Response> DEVE essere sigillata elettronicamente dal SGD e contiene i seguenti attributi ed elementi:

  - `Destination`, valorizzato con l'EntityID-deleghe del SP (quello che dovrebbe cominciare con `del:` seguito dall'EntityID-SP);
  - `InResponseTo` che si riferisce all'ID univoco nell'`<AuthnRequest>`-**2** (cioè quello che comincia per **`del:attr-`**;
  - `IssueInstant`;
  - si raccomanda includa tutti i *namespace* XML richiesti (p.es. `saml`, `samlp`, `ac`, `del`, `ds`, `xsd`, `xsi`, `sgd`).
- `<Status>`, opportunamente valorizzato. In caso di successo, in particolare:
- `<Issuer>`, contiene l'EntityID del SDG e:
  - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:`**`entity`**;
  - l'elemento stesso e, opzionalmente, l'attributo `NameQualifier`, valorizzati entrambe con l'EntityID del SGD.
- `<Subject>`, contenente i seguenti elementi:
  - **`<NameID>,`** valorizzato con la stringa rappresentante il codice fiscale[10] del **delegato**, preceduto dal prefisso "`TIN`," seguito dal codice-paese,[11] seguito dal codice fiscale (come da norma ETSI EN 319-412-1 §5.1.3) e, inoltre, i seguenti attributi:
    - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:`**`persistent`**;
    - `NameQualifier` valorizzato con l'EntityID del SGD
    - `SPNameQualifer` valorizzato con l'EntityID-deleghe del SP;
    - `SPProvidedID`, valorizzato con il `<NameID>` caratterizzante l'**`<Assertion>-1`** generata originariamente dall'IDP nell'`<AuthnResponse>`-**1** (e re-imbustata nell'elemento `<sgd:Evidence>` della presente `<AuthnRequest>`-**2**).
  - `<SubjectConfirmation>`, con attributo contenente `Format` pari a `urn:oasis:names:tc:SAML:2.0:cm:`**`bearer`** e all'interno `<SubjectConfirmationData>` dotato dei seguenti attributi:
    - `InResponseTo` valorizzato con l'ID univoco dell'attributo `ID` dell'`<AuthnRequest>`-**1** (citato nell'`InResponseTo` della **`<Assertion>-1`** imbustata nell'`<AuthnRequest>`-**2**);
    - `NotOnOrAfter`, valorizzato con l'orario di scadenza dell'autenticazione originaria attestata all'SP dall'IDP mediante l'`<AuthnResponse>`-**1** (entro la quale deve essere fornita l'`<AuthnRequest>`-**2** al passo 6 e, quindi, la conclusione dell'intero processo di autenticazione per delega);

- Un *primo* elemento **`<Assertion>`**, denominato la `<Assertion>`-**2*a***; PUÒ essere sigillato elettronicamente dal SGD; contenente l'asserzione circa l'**identità del *delegato***, ottenuta rielaborando gli attributi identificativi forniti dall'IDP con l'`<AuthnResponse>`-**3** (e imbustando all'interno la sua **`<Assertion>-3`** – già sigillata elettronicamente dall'IDP – all'interno dell'elemento figlio `<Advice>` descritto più avanti).
  - `ID`, valorizzato con un ID univoco dell'asserzione (che comincia con **`del:delegated-`**);

[10] Nel caso il SGD supporti deleghe digitali associate a delegati dotati di identità digitali provenienti da schemi di identificazione elettronica stranieri, notificati ai sensi di [**eIDAS**], cfr. nota 3, il codice fiscale è sostituito dall'identificativo di unicità della persona fisica: `personalIdentifier`.

[11] Il "codice-paese" è la stringa a due caratteri maiuscoli del Paese, conforme alla norma ISO 3166-1 α-2.

- `IssueInstant`, contenente l'orario in cui è generata l'asserzione (*entro* la data di validità dell'`<Assertion>-3` imbustata al suo interno);
- `<Status>`, opportunamente valorizzato;
- `<Issuer>`, contiene l'EntityID dell'SDG e:
  - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`;
  - l'elemento stesso (e, opzionalmente, l'attributo `NameQualifier`), valorizzato/i con l'EntityID del SGD;
- L'elemento `<Subject>`, contentente:
  - `<NameID>`, valorizzato con il `<NameID>` identificante l'asserzione SAML nel contesto dell'IDP (così come restituito nella `<Assertion>-3` nell'`<AuthnResponse>-3`), con i seguenti attributi:
    - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`;
    - `NameQualifier` valorizzato con l'EntityID dell'IDP;
    - `SPNameQualifier` valorizzato con l'EntityID-SP del SP;
  - `<SubjectConfirmation>`, valorizzato, in base alla seguente alternativa:
    - nel caso in cui il SGD *non* abbia adottato l'autenticazione interna (cfr. §2), con l'attributo `Method` pari a `urn:oasis:names:tc:SAML:2.0:cm:bearer` e all'interno l'elemento `<SubjectConfirmationData>`, con i seguenti attributi:
      - `NotOnOrAfter`, valorizzato con l'orario di scadenza dell'autenticazione attestata al SGD dall'IDP mediante l'`<AuthnResponse>-3`,
      - `Recipient`, valorizzato con l'EntityID-SP del SP;
      - `InResponseTo`, pari all'ID della richiesta di autenticazione `<AuthnRequest>-3`, effettuata dal SGD presso l'IDP (cioè al valore dell'attributo `ID`, che comincia per `del:id-`);
    - *solamente* nel caso in cui il SGD abbia adottato l'autenticazione interna (cfr. §2), con l'attributo `Method` pari a `urn:oasis:names:tc:SAML:2.0:cm:bearer` e all'interno l'elemento `<SubjectConfirmationData>`, con i seguenti attributi:
      - `NotOnOrAfter`, valorizzato con l'orario di scadenza dell'autenticazione attestata al SGD dall'IDP mediante nell'`<AuthnResponse>-3` (entro la quale deve essere fornita l'`<AuthnRequest>-3` al passo 4),
      - `Recipient`, valorizzato con l'EntityID-SP del SP;
      - `InResponseTo`, pari all'ID della richiesta di autenticazione `<AuthnRequest>-3`, effettuata dal SGD presso l'IDP (cioè al valore dell'attributo `ID`, che comincia per `del:id-`);
- L'elemento `<Conditions>` contenente:
  - l'attributo `NotBefore`, valorizzato con data e ora di inizio validità dell'intera asserzione (cioè il valore dell'attributo `IssueInstant` di emissione dell'elemento-radice `<Response>` dell'intera `<AuthnResponse>-2`);
  - l'attributo `NotOnOrAfter`, valorizzato con l'orario di scadenza dell'autenticazione originaria attestata all'SP dall'IDP mediante l'`<AuthnResponse>-1` (anch'esso già riportato nell'`<AuthnResponse>-2` stessa);

- l'elemento-vuoto <OneTimeUse> – *solo* qualora il SGD, a sua discrezione, *non* riutilizzi la sessione di autenticazione del delegato presso di lui (cfr. §3 punto 3), ad esempio interrompendola subito dopo aver fornito l'<AuthnResponse>-**2**;
- l'elemento <AudienceRestriction>, contenente *due* elementi-fratelli <Audience>, valorizzati rispettivamente con:
  - l'EntityID-deleghe del SP;
  - l'EntityID-SP del SP (cioè l'EntityID precedente *senza* il prefisso del:);

- L'elemento <Advice>, contenente i seguenti figli:
  - l'elemento <AssertionIDRef>, valorizzato con l'ID univoco della <Assertion>-**1** originaria, presentata dall'IDP tramite l'<AuthnResponse>-**1**; in caso di autenticazione interna, la sua presenza indica al SP che il SGD ha utilizzato tale metodo di autenticazione presso di lui, in quanto il presente elemento referenzia direttamente la sottostante:
  - un sotto-elemento <Assertion>-3 (già sigillato elettronicamente dall'IDP) esattamente come contenuto nell'<AuthnResponse>-**3**; tra gli altri, esso contiene l'elemento <Subject> con all'interno:
    - <NameID>, sempre valorizzato con il <NameID> identificante l'asserzione SAML nel contesto dell'IDP (così come restituito nell'<AuthnResponse>-**3**), con i seguenti attributi:
      - Format, pari a urn:oasis:names:tc:SAML:2.0:nameid-format:**transient**;
      - NameQualifier, valorizzato con l'EntityID dell'IDP;
      - SPNameQualifier, valorizzato con l'EntityID del SGD;
    - l'elemento <AttributeStatement>, con all'interno tutti gli attributi-identificativi del delegato (*almeno* il codice fiscale).

- Un *secondo* elemento <**Assertion**>, denominato la <Assertion>-**2*b***, (PUÒ essere sigillato elettronicamente dal SGD) contenente l'asserzione circa l'**identità del *delegante*** e i corrispondenti attributi-delega:
  - ID, valorizzato con un ID univoco dell'asserzione (che comincia con **del:delegator-**);
  - IssueInstant, contenente il medesimo orario della precedente <**Assertion**>-2***a***;
  - <Status>, opportunamente valorizzato;
  - <Issuer>, contiene l'EntityID dell'SDG e:
    - Format, pari a urn:oasis:names:tc:SAML:2.0:nameid-format:**entity**;
    - l'elemento stesso (e, opzionalmente, l'attributo NameQualifier), valorizzato/i con l'EntityID del SGD;
  - L'elemento <Subject>:
    - <NameID>, valorizzato con la stringa rappresentante il codice fiscale[12] del **delegante**, preceduto dal prefisso "TIN," seguito dal codice-paese, seguito dal codice fiscale (come da norma ETSI EN 319-412-1, §5.1.3) e, inoltre, i seguenti attributi:

[12] Nel caso il SGD supporti deleghe digitali associate a deleganti dotati di identità digitali provenienti da schemi di identificazione

- `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`;
- `NameQualifier` valorizzato con l'EntityID del SGD;
- `SPNameQualifier` valorizzato con l'EntityID-deleghe del SP;

▪ `<SubjectConfirmation>`, con l'attributo `Method` pari a `urn:oasis:names:tc:SAML:2.0:cm:bearer` e al cui interno sono presenti i seguenti elementi:

- `<SubjectConfirmationData>`, con i seguenti attributi:
  - `InResponseTo`, pari all'ID dell'`<AuthnRequest>`-**2** effettuata dal SGD presso l'IDP (il valore dell'attributo `ID` che comincia per **`del:attr-`**);
  - `NotOnOrAfter`, valorizzato con l'orario di scadenza dell'autenticazione originaria attestata all'SP dall'IDP mediante l'`<AuthnResponse>`-**1** (anch'esso già riportato nell'`<AuthnResponse>`-**2** stessa);
  - `Recipient`, valorizzato con l'AsCS nel metadata-deleghe del SP, relativo ad un *binding* HTTP POST, originariamente indicato dal SP nell'`<AuthnRequest>`-**2** – e da *non* confondersi con l'AsCS nel metadata-SP del SP e utilizzato in `<AuthnRequest>`-**1** e `<AuthnResponse>`-**1**;
- `<del:Delegate>`, elemento *replicato* (per ottemperare alle raccomandazioni [**samlDel**]) come il discendente dal successivo elemento `<Conditions>`.

o L'elemento `<Conditions>` contenente i seguenti attributi ed elementi:

▪ l'attributo `NotBefore`, valorizzato come il `DelegationInstant` presente nell'elemento `<del:Delegate>` (cioè *non antecedente* all'`IssueInstant` contenuto nell'`<Assertion>`-**3** dell'`<AuthnResponse>`-**3**);

▪ l'attributo `NotOnOrAfter`, valorizzato come quello presente nell'`<Assertion>`-**1** dell'`<AuthnResponse>`-**1**;

▪ l'elemento-vuoto `<OneTimeUse>` – *solo* qualora il SGD, a sua discrezione, *non* riutilizzi la sessione di autenticazione del delegato presso di lui (cfr. §3 punto 3), ad esempio interrompendola subito dopo aver fornito l'`<AuthnResponse>`-**2**;

▪ l'elemento `<AudienceRestriction>`, contenente un solo elemento `<Audience>`, valorizzato con l'EntityID-deleghe del SP;

▪ l'elemento-cardinale `<del:Delegate>`, cfr. [**samlDel**], che lega le due sessioni di autenticazione del delegato (ottenute mediante l'`<AuthnResponse>`-**1** e l'`<AuthnResponse>`-**3**) fra loro, contenete i seguenti:

- `DelegationInstant`, valorizzato con l'orario in cui avviene la delega stessa, cioè il delegato conferma l'identità del delegante presso la pagina del SGD per l'utilizzo della relativa delega;[13] tale orario è *non antecedente* all'`IssueInstant` contenuto nell'`<Assertion>`-**3** dentro l'`<AuthnResponse>`-**3** e *non successivo* al `NotOnOrAfter` contenuto nell'`<Assertion>`-**1** nell'`<AuthnResponse>`-**1** – e

elettronica stranieri, notificati ai sensi di [**eIDAS**], cfr. note 3 e 10, il codice fiscale è sostituito dall'identificativo di unicità della persona fisica: `delegatorPersonalIdentifier`.

[13] Ovvero, in alternativa, l'orario in cui il delegato seleziona uno tra più deleganti possibili, in caso risulti al SGD che questi possiede deleghe multiple, valide per la medesima classe di servizio del medesimo SP.

tale intervallo di tempo consiste in quello in cui la delega digitale è effettivamente e complessivamente "spendibile" presso il SP;

- `ConfirmationMethod`, pari a `urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession`, cfr. [samlAC];
- `<NameID>`, valorizzato con il valore del `<NameID>` identificante il delegante nel contesto dell'IDP (nell'`<AuthnResponse>`-**3**), con i seguenti attributi:
  - `Format`, pari a `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`;
  - `NameQualifier` valorizzato con l'EntityID del SGD
  - `SPNameQualifer` valorizzato con l'EntityID-deleghe del SP;
  - `SPProvidedID`, valorizzato con il `<NameID>` caratterizzante l'`<Assertion>` generata originariamente dall'IdP nella `<AuthnResponse>`-**1** (e re-imbustata nell'elemento `<sgd:Evidence>` dentro nell'`<AuthnRequest>`-**2**).

- L'elemento `<AttributeStatement>`, contenente gli attributi-delega del *delegante*, secondo le norme SAML, ciascuno in un elemento `<Attribute>` che rispetta le seguenti regole:
  - Ciascun attributo-delega può essere la replica di un attributo identificativo del delegante (così come acquisito – *a titolo meramente esemplificativo* – dall'IDP del delegante durante la creazione della delega). In tal caso, l'attributo `Name` dell'attributo identificativo comincia con la stringa "`delegator`," seguita dal nome originario dell'attributo identificativo, sempre rispettando il *camel-casing*. Ad esempio, all'attributo identificativo `familyName` restituito dall'IDP del delegante corrisponde l'attributo-delega **`delegator`**`FamilyName` restituito dall'SGD.[14]
  - In alternativa, l'attributo-delega può essere un attributo *specifico*, fornito in fase di creazione della delega digitale, dal SGD stesso, ovvero dal delegante (in questo caso relativo ad una classe di servizi con granularità della singola operazione);[15] si veda il §5 per le caratteristiche tecniche degli attributi specifici.
  - Deve essere presente l'attributo `NameFormat`, valorizzato come da metadata del SGD corrispondente, cfr. §6.3.
  - Si *raccomanda* di valorizzare l'attribuito `FriendlyName` con un nome identificativo (in lingua italiana) che può essere facoltativamente visualizzato dal SP nelle evidenze informatiche relative al consumo della delega.
  - Ogni attributo-delega contiene un elemento `<AttributeValue>` dotato dell'attributo `xsi:type` valorizzato con il tipo di dato *XML Schema* più attinente alla valorizzazione corrispondente.

Qui sotto è riportato un esempio di `<AuthnResponse>`-**2** (sigillata elettronicamente dal SGD) con, evidenziate a colori, con le due `<Assertion>` (non sigillate) e l'`<Assertion>` (sigillata dall'IDP) imbustata all'interno della prima

[14] Il motivo di tale distinzione è una misura volta a mitigare il rischio che il SP possa tecnicamente confondere la titolarità degli attributi identificativi del delegato e del delegante, creando così una "impersonificazione" tra le due identità digitali.
[15] Ad esempio: il numero identificativo di uno specifico documento informatico o fisico (referto, attestato, numero di protocollo, targa automobilistica, licenza, certificato, ecc.), la data di prenotazione di un appuntamento (ritiro, consegna, visita, ecc.), o altro.

di esse (cfr. Figura 6).

```
<samlp:Response
  Destination="del:https://www.SPdiesempio.it"
  ID="_4d38c302617b5bf98951e65b4cf304711e2166df20"
  InResponseTo="del:attr-9R9FzkZ0h8JFRCRC4eGpuZii-6r52tJlpV7b5A9e"
  Version="2.0"
  IssueInstant="2021-03-21T10:34:00Z"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:del="urn:oasis:names:tc:SAML:2.0:conditions:delegation"
  xmlns:sgd="https://deleghedigitali.gov.it/saml-extensions"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ds:Signature> [……] </ds:Signature>
    <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
    <saml:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
      NameQualifier="https://deleghedigitali.gov.it">
            https://deleghedigitali.gov.it
    </saml:Issuer>
    <saml:Subject>
            <saml:NameID
              Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
              NameQualifier="https://deleghedigitali.gov.it"
              SPNameQualifier="del:https://www.SPdiesempio.it"
              SPProvidedID="AAdzZWNyZXQx/cGt/T65P/3/jHt6frP0TASuN5FvymMCBzfA6IA6Ofps6">
                    TINIT-RSSMROyyMddC999Y
            </saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData
                            InResponseTo="id-ZR9KpyZ0h8JFRCRC4eGpuZii-6r52tJlpV7bCsXD"
                            NotOnOrAfter="2021-03-21T10:36:00Z"/>
            </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Assertion
      ID="del:delegated-f6127a0f-ff7f-4e98-9108-bca9398d5645"
      IssueInstant="2021-03-21T10:34:00Z"
      Version="2.0">
            <samlp:Status>
                    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </samlp:Status>
            <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                    https://deleghedigitali.gov.it
            </saml:Issuer>
            <saml:Subject>
                    <saml:NameID
                      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                      NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
                      SPNameQualifier="https://www.SPdiesempio.it">
                            >AAdzZWNyZXQxDX5jaZEES999t3SRsMjrfFcrQbuxVinXmmQpi/+nv2PFVVyIE
                    </saml:NameID>
```

```
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                        <saml:SubjectConfirmationData
                          InResponseTo="del:id-pyZ0a1a824dba354bcbba9dh8JFRa8108f55cc19"
                          NotOnOrAfter="2021-03-21T10:38:30Z"
                          Recipient="https://www.SPdiesempio.it/binding/http-post"/>
                </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
          NotBefore="2021-03-21T10:34:00Z"
          NotOnOrAfter="2021-03-21T10:38:30Z">
                <saml:OneTimeUse/>
                <saml:AudienceRestriction>
                        <saml:Audience>del:https://www.SPdiesempio.it</saml:Audience>
                        <saml:Audience>https://www.SPdiesempio.it</saml:Audience>
                </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:Advice>
                <saml:AssertionIDRef _e5cdedd6-36aa-43a8-bce1-0d5ede7344d3</saml:AssertionIDRef>
                <saml:Assertion
                  ID="_de7344d3-36aa-8a34-1ecb-0d5ee5cdedd6"
                  IssueInstant="2021-03-21T10:33:30Z"
                  Version="2.0"
                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                  xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                        <ds:Signature>  [……]  </ds:Signature>
                        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                                https://idserver.servizicie.interno.gov.it/idp
                        </saml:Issuer>
                        <saml:Subject>
                                <saml:NameID
                                  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                                  NameQualifier="https://idserver.servizicie.interno.gov.it/idp"
                                  SPNameQualifier="https://deleghedigitali.gov.it">
                                    >AAdzZWNyZXQxDX5jaZEES999t3SRsMjrfFcrQbuxVinXmmQpi/+nv2PFVVyIE
                                </saml:NameID>
                                <saml:SubjectConfirmation Method="urn:oasis:[……]:2.0:cm:bearer">
                                        <saml:SubjectConfirmationData
                                          InResponseTo="del:id-pyZ0a1a824dba[……]a8108f55cc19"
                                          NotOnOrAfter="2021-03-21T10:38:30Z"
                                          Recipient="https://deleghedigitali.[……]/post"/>
                                </saml:SubjectConfirmation>
                        </saml:Subject>
                        <saml:Conditions
                          NotBefore="2021-03-21T10:33:30Z"
                          NotOnOrAfter="2021-03-21T10:38:30Z">
                                <saml:OneTimeUse/>
                                <saml:AudienceRestriction>
                                        <saml:Audience>
                                                https://deleghedigitali.gov.it
                                        </saml:Audience>
                                </saml:AudienceRestriction>
                        </saml:Conditions>
                        <saml:AuthnStatement
                          AuthnInstant="2021-03-21T10:33:30Z"
```

```
                        SessionIndex="_30cdbc90-36a7-465d-807f-9238edd337a5">
                        <saml:AuthnContext>
                            <saml:AuthnContextClassRef>
                                https://www.spid.gov.it/SpidL3
                            </saml:AuthnContextClassRef>
                        </saml:AuthnContext>
                    </saml:AuthnStatement>
                    <saml:AttributeStatement>
                        <saml:Attribute
                          Name="fiscalNumber"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                            <saml:AttributeValue xsi:type="xs:string">
                                TINIT-RSSMROyyMddC999X
                            </saml:AttributeValue>
                        </saml:Attribute>
                    </saml:AttributeStatement>
                </saml:Assertion>
            </saml:Advice>
            <saml:AttributeStatement>
                <saml:Attribute Name="fiscalNumber" NameFormat="[……]">
                    <saml:AttributeValue [……]>TINIT-RSSMROyyMddC999Y</saml:AttributeValue>
                </saml:Attribute>
            </saml:AttributeStatement>
        </saml:Assertion>
        <saml:Assertion
          ID="del:delegator-1e64ee3d-2dfb-4676-b475-d1578f71a21d"
          IssueInstant="2021-03-21T10:34:00Z"
          Version="2.0">
            <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </samlp:Status>
            <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                https://deleghedigitali.gov.it
            </saml:Issuer>
            <saml:Subject>
                <saml:NameID
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                  NameQualifier="https://deleghedigitali.gov.it"
                  SPNameQualifier="del:https://www.SPdiesempio.it">
                    TINIT-RSSMROyyMddC999X
                </saml:NameID>
                <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                    <saml:SubjectConfirmationData
                      InResponseTo="del:attr-9R9FzkZ0h8JFRCRC4eGpuZii-6r52tJlpV7b5A9e"
                      NotOnOrAfter="2021-03-21T10:38:30Z"
                      Recipient="https://www.SPdiesempio.it/binding/http-post"/>
                    <del:Delegate
                      DelegationInstant="2021-03-21T10:33:30Z"
                      ConfirmationMethod="urn:oasis:[……]:2.0:ac:classes:PreviousSession">
                        <saml:NameID
                          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                          NameQualifier="https://deleghedigitali.gov.it"
                          SPNameQualifier="del:https://www.SPdiesempio.it"
                          SPProvidedID=">AAdzZWNyZXQx/cGt[……]rP0TASuN5FvymMCBzfA6IA6Ofps6">
                            AAdzZWNyZXQx/cGt[……]rP0TASuN5FvymMCBzfA6IA6Ofps6
                        </saml:NameID>
```

```
                        </del:Delegate>
                </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions
          NotBefore="2021-03-21T10:34:00Z"
          NotOnOrAfter="2021-03-21T10:39:0Z">
                <saml:OneTimeUse/>
                <saml:AudienceRestriction>
                        <saml:Audience>https://www.SPdiesempio.it</saml:Audience>
                </saml:AudienceRestriction>
                <saml:Condition>
                        <del:Delegate
                          DelegationInstant="2021-03-21T10:33:30Z"
                          ConfirmationMethod="urn:oasis:names:[……]:ac:classes:PreviousSession">
                                <saml:NameID
                                  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                                  NameQualifier="https://deleghedigitali.gov.it"
                                  SPNameQualifier="del:https://www.SPdiesempio.it"
                                  SPProvidedID="AAdzZWNyZXQx/cGt[……]rP0TASuN5FvymMCBzfA6IA6Ofps6">
                                        AAdzZWNyZXQx/cGt[……]rP0TASuN5FvymMCBzfA6IA6Ofps6
                                </saml:NameID>
                        </del:Delegate>
                </saml:Condition>
        </saml:Conditions>
        <saml:AttributeStatement>
                <saml:Attribute Name="delegatorName" NameFormat="[……]">
                        <saml:AttributeValue [……]>Verdi</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="delegatorFamilyName" NameFormat="[……]">
                        <saml:AttributeValue [……]>Anna</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="delegatorFiscalNumber" NameFormat="[……]">
                        <saml:AttributeValue [……]>TINIT-VRDNNA64T70G677R</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="delegatorMobilePhone" NameFormat="[……]">
                        <saml:AttributeValue [……]>+391234567890</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="delegatorEmail" NameFormat="[……]">
                        <saml:AttributeValue [……]>anna.verdi@email.it</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="delegation" NameFormat="[……]">
                        <saml:AttributeValue [……]>anna.verdi@email.it</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="soft:https://www.SPdiesempio.it?documentId" NameFormat="[……]">
                        <saml:AttributeValue [……]>REF 122547/39</saml:AttributeValue>
                </saml:Attribute>
                <saml:Attribute Name="soft:https://www.SPdiesempio.it?bookingDate" NameFormat="[……]">
                        <saml:AttributeValue [……]>2021-05-05</saml:AttributeValue>
                </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

5. Caratteristiche della delega digitale

La delega digitale, in base alla definizione data al punto *d)* del §2, è costituita da una serie di caratteristiche – alcune obbligatoriamente presenti in tutte le deleghe digitali, altre facoltative.

Le caratteristiche facoltative possono essere presenti in alcune deleghe digitali, ma non in altre.

Le caratteristiche di una delega digitale *possono* essere rappresentate da attributi-delega – legati o meno all'identità del delegante o del delegato, ovvero alla classe di servizi delegabili. Quando una caratteristica sia associata ad uno o più attributi-delega, il '*nome tecnico*' ed il '*nome discorsivo*' di ciascuno di essi sono definiti insieme alla caratteristica. Per 'nome tecnico' e 'nome discorsivo' dell'attributo-delega – al presente capitolo e nei successivi – si intendono i valori assunti rispettivamente dagli attributi `Name` (*obbligatorio*) e `FriendlyName` (*facoltativo*), usati nelle varie evidenze SAML – in particolar modo negli AtCS, così come negli elementi `<Attribute>` e `<RequestedAttribute>` nei metadata, richieste e risposte di autenticazione. Il nome tecnico è indicato con `questo carattere tipografico` e rispetta sempre le regole del *camel-casing*; il nome discorsivo è indicato semplicemente in **grassetto**. L'eventuale tipo dell'attributo-delega è indicato con la stringa XSD (*XML Schema*) corrispondente.

Caratteristiche aggiuntive delle deleghe digitali, così come mutamenti nel loro funzionamento rispetto ai con-partecipanti al sistema delle deleghe digitali – potranno essere introdotte tramite Avvisi, regolamentando in particolar modo le "estensioni" nei metadata SAML di cui al §6.

Ulteriori caratteristiche facoltative, *diverse* dagli attributi specifici di cui al §5.2, affinché possano essere adottate da un SP nelle proprie classi di servizi delegabili, DEVONO:

i. essere definite e normate nel presente Allegato Tecnico o in un successivo Avviso (cfr. §2);
ii. essere già espressamente indicate nel metadata del SGD (cfr. §6.3);
iii. venire indicare espressamente nel metadata-deleghe dell'SP (cfr. §6.2).

Le caratteristiche *obbligatorie* di una delega digitale sono:

1. ***Time-stamp* di creazione della delega** (`delegationCreationTime`, tipo `xsd:dateTime`) — marcatura temporale elettronica (ex [**eIDAS**]) relativa al momento in cui la delega digitale è creata presso il SGD. Questa caratteristica può essere utilizzata dal sistema delle deleghe digitali per gestire i cambiamenti negli attributi-delega come parte dell'attributo qualificato 'delega digitale.' In particolare, in ottica di protezione dei dati personali (cfr. [**GDPR**]), gli SP che accettano deleghe digitali DEVONO utilizzare tale attributo per gestire internamente la fruizione di servizi delegabili afferenti ad una classe di servizi, qualora tali associazioni siano avvenute, nel perimetro del SP, in data *successiva* alla creazione della delega per quella classe di servizi. Ciò POTREBBE costituire, infatti, un trattamento del dato personale del delegante non espressamente da questi autorizzato. Le modalità di creazione e modifica delle deleghe digitali non sono oggetto del presente Allegato Tecnico.
2. ***Time-stamp* di scadenza della delega** (`delegationExpirationTime`, tipo `xsd:dateTime`) — marcatura temporale elettronica relativa al momento nel tempo entro il quale la delega può rimanere valida.

Tra le caratteristiche *facoltative* di una delega digitale ci sono le seguenti:

3. ***Time-stamp* di rinnovo della delega** (`delegationRenewalTime`, tipo `xsd:dateTime`) — marcatura temporale elettronica (ex [**eIDAS**]) che, se presente, è relativa al momento in cui la delega digitale è stata rinnovata per l'ultima volta.
4. **Tipologia della delega** (`delegationType`, tipo `xsd:complexType`) — identificativo o identificativi della tipologia della delega (eventualmente separati fra loro da spazi), ciascuno selezionabile tra diversi valori, opportunamente estendibili tramite Avvisi. Per ulteriori dettagli, consultare il §6.2
5. **Numero di utilizzi della delega** (`delegationNumUses`, tipo `xsd:nonNegativeInteger`) — Numero di volte per le quali la delega digitale è stata fornita con successo ad un SP come attributo qualificato all'interno del suo periodo di validità.[16]
6. **Numero massimo di utilizzi della delega** (`delegationMaxUses`, tipo `xsd:positiveInteger`) — Numero di volte per le quali la delega digitale è utilizzabile da un SP sotto forma di attributo qualificato, all'interno del suo periodo di validità.
7. **Tipologia della delega** (`delegationType`, tipo `SGD:type:delegationType`) — Tipologia della delega, come definita in §5.1 e ulteriormente specificata al §6.2 punto 5.3.8.
8. **Modalità di creazione della delega** (`delegationCreationMode`, tipo `SGD:type:delegationMode`) — valorizzato con un identificativo che identifichi la modalità di creazione della delega. La valorizzazione di questo attributo, incluso il ricorso ad ulteriori attributi-delega, è al di fuori dell'ambito delle presenti regole tecniche.
9. **Identificativo univoco di un documento** (`soft:documentNo`, tipo `xsd:string`) — attributo specifico contenente un numero seriale, o altro identificativo univoco (UID) di uno specifico documento informatico richiesto (ad esempio: certificato tradizionale, attestato, referto).
10. **Data di prenotazione** (`soft:bookingDate`, tipo `xsd:date`) — attributo specifico contenente la data di prenotazione per un certo evento.
11. **Ora di prenotazione** (`soft:bookingDate`, tipo `xsd:time`) — attributo specifico contenente l'orario giornaliero di prenotazione per un certo evento.
12. ***Time-stamp* di prenotazione** (`soft:bookingDateTime`, tipo `xsd:dateTime`) — attributo specifico contenente la data e l'ora di prenotazione per un certo evento.
13. **Attributo X.509** (`urn:oid:`*`OID.number`*, tipologia variabile) — attributo associato, secondo quanto previsto dagli standard tecnici RFC-3061, ITU-T X.500, X.520, X.509, X.660, X.669 e loro derivati, a un arco di *object identifier* (OID). Riservato per applicazioni future ove sia presente o richiedibile anche come attributo X.509 all'interno di un certificato elettronico, qualificato o non qualificato (cfr. [**eIDAS**]).
14. **Identificativo univoco** (`urn:uuid:`*`UUID-number`*, tipologia variabile) — attributo associato ad un identificativo universalmente unico (UUID), secondo quanto previsto dagli standard tecnici RFC-4122, ITU-T X.660 e X.667.

5.1. Tipologia della delega digitale

Il funzionamento delle deleghe digitali dal punto di vista amministrativo è al di fuori dell'ambito del presente Allegato Tecnico, ivi inclusi gli aspetti che si differenziano a seconda della tipologia "organizzativo-amministrativa" della delega digitale. Dal punto di vista tecnico-implementativo, invece, una caratteristica obbligatoria della delega è la sua tiplogia "tecnica" e altre caratteristiche, attraverso le quali si declinano invece le tipologie organizzativo-amministrative. La suddetta tipologia tecnica (cd., semplicemente, **tipologia**) attualmente prevede la seguente classificazione:

[16] Ovdvero all'interno del periodo di validità dell'ultimo rinnovo, nel caso di deleghe digitali rinnovabili.

- delega **semplice** — per la cui creazione *non* sono necessari ulteriori tipi di controlli o adempimenti (ad es. di natura amministrativa) per l'associazione delle proprietà di cui ai punti da *a)* a *d)* del §2; una classe di servizi delegabili la cui tipologia non è espressamente definita nel metadata-deleghe del SP (cfr. §6.2) è da considerarsi 'semplice';

- delega **complessa** — per la cui creazione sono necessari alcuni adempimenti o controlli da parte del soggetto preposto (il SGD o suo incaricato); la natura e l'operatività di tali adempimenti è al di fuori degli scopi del presente documento;

Ulteriori tipologie di delega potranno essere introdotte o espanse tramite Avvisi.

5.2. Attributi specifici

Tra le caratteristiche facoltative di una delega digitali vi sono gli **attributi *specifici***, cioè dei dati forniti dal delegante al momento della creazione della delega digitale e conservati come parte integrante della stessa per il suo intero ciclo-vita. Anche nel caso in cui una delega sia modificata o rinnovata in seguito alla sua creazione (al di fuori dell'ambito delle presenti regole tecniche), né il delegante né il delegato possono modificare un attributo specifico.

Gli attributi specifici sono identificati da ciascun SP e indicati come tali in una o più AtCS del proprio metadata-deleghe (cfr. §6.2).

Gli attributi specifici DEVONO avere il nome tecnico che:

- comincia per "`soft:`" e, in tal caso:
- per gli attributi *specifici ma non globali* (cfr. §**Error! Reference source not found.**), PUÒ essere seguito da un *namespace* riconosciuto dall'SP o dagli SP che fanno uso di tale attributo – tipicamente coincidente con l'EntityID "globale" del SP (cfr. §6) – e, in tal caso, è seguito dal carattere "`:`";
- è seguito dal 'nome semplice' dell'attributo specifico che segue a sua volta le seguenti regole:
  - NON coincide col nome tecnico di nessun attributo identificativo di alcun IDP,
  - NON comincia con "`soft:`"
  - NON coincide con nessun nome di attributo-delega derivato da un attributo identificativo (cioè non comincia, a sua volta, con `delegator`).

5.3. Ambito della delega, ereditarietà, deleghe globali e generali

Come anticipato al §2 punto *c)*, ciascuna delega digitale è relativa ad una sola classe di servizi delegabile la quale, a sua volta, è ascrivibile ad uno specifico SP: si parla, in questo caso, di delega con *ambito* "**locale**."

Esistono tuttavia delle classi di servizi delegabili **globali** (opportunamente definite nel metadata del SGD, cfr. elemento `<GlobalServiceClasses>`, §5.3), cioè una delega digitale che, in base al suddetto punto *c)*, vi sia associata prende il nome di delega "globale" e può essere utilizzata presso qualunque SP che dichiari una classe di servizi delegabile con quello stesso identificativo univoco nel proprio metadata-deleghe (cfr. §6.2). A differenza delle classi di servizi delegabili **locali**, quelle globali possono essere associate ad insiemi di attributi-delega diversi a seconda dei diversi SP che specificano gli AtCS corrispondenti nel proprio metadata-deleghe.

Le classi di servizi delegabili possono inoltre essere inquadrate, nell'ambito di ciascun SP, in una o più gerarchie di classi di servizi. Le classi di servizio a un livello inferiore possono "ereditare" o meno la delegabilità dalle classi di

servizio superiori nella gerarchia. Questo significa che, nel caso un dato SP abbia una classe di servizi delegabili *a*, gerarchicamente posta al di sopra di una classe di servizi delegabili *b*, un delegato cui sia associata una delega digitale per la classe *a* PUÒ utilizzare o meno, per effetto di tale delega digitale, dei servizi associati alla classe *b* a seconda che il SP abbia dichiarato (nel proprio metadata-deleghe, cfr. §5.3.9.1) che la classe *b* eredita la delegabilità della classe *a* (cioè che con una delega assegnata alla classe a si può accedere anche ai servizi per la classe *b*.

Allo scopo di individuare gerarchie di classi di servizi delegabili, una classe di servizi non associata ad alcun AtCS non è utilizzabile direttamente nel contesto SAML, ma può essere indirettamente utilizzata dal SP come "contenitore" di più classi di servizio delegabili per le quali concedere congiuntamente un'unica delega digitale.

Tra le classi di servizio di quest'ultimo tipo, la presenza di una siffatta classe di servizio può agevolare la creazione di deleghe per tutti i servizi delegabili di un dato SP, qualora il SP *non* disponga di una AtCS, *unica* per tutti i propri servizi delegabili, cui associare deleghe digitali per tutti i servizi delegabili di quel SP.

Tra le classi di servizi delegabili globali, esiste una classe di servizi, individuata dal SGD, che ha come ambito *tutti* i servizi *delegabili* offerti da *tutti* i SP *pubblici*. Le deleghe globali create per tale classe di servizi delegabili prendono il nome di **deleghe generali**.

Circa l'utilizzo della delega digitale e l'utilizzo della stessa per uno specifico servizio delegabile afferente ad una classe di servizi delegabili, resta in capo al SP di controllare che il delegato possa effettivamente utilizzare tale servizio delegabile per conto del delegante; per questo motivo, la data di creazione della delega (cfr. §§5.1 e 5.4) è un importante caratteristica obbligatoria della delega, che può sempre essere richiesta, dal SP, allo scopo di discriminarne correttamente l'utilizzo.

5.4. Validità e rinnovabilità

La delega digitale ha sempre una validità finita nel tempo. Può inoltre essere facoltativamente specificato un numero massimo di utilizzi entro la sua validità. La delega digitale è VALIDA solo se utilizzata entro il periodo di validità e, qualora non sia stato superato il numero massimo di utilizzi, se previsto. Ciò è veicolato mediante alcune caratteristiche, obbligatorie o facoltative, della delega sopra introdotte (cfr. §5.1) e può essere ulteriormente regolato tramite Avvisi.

Le deleghe dotate di caratteristiche quali almeno una di quelle di cui ai punti 3 e 7, sono le cosiddette *deleghe rinnovabili*. Una delega rinnovabile sin dalla prima creazione PUÒ comunque presentare l'attributo di cui al punto 3, valorizzato – sino al primo rinnovo – con il medesimo *time-stamp* dell'attributo di cui al punto 1.

Affinché una delega digitale sia VALIDA, l'intervallo temporale assoluto tra i *time-stamp* di cui ai punti 1 e 2 non DOVREBBE essere superiore alla durata massima di validità associata alla classe di servizi delegabili della relativa delega, così come definita nel metadata-deleghe corrispondente mediante l'elemento `<MaxValidity>` (cfr. §0, punto 5.3.9). Qualora lo sia (cioè la durata calcolata per differenza tra i *time-stamp* di cui ai punti 2 e 1 è maggiore del valore del suddetto elemento `<MaxValidity>`), affinché l'attributo qualificato 'delega digitale' sia valido, DEVE essere verificato che:

- la delega contenga l'attributo facoltativo di cui al punto 3, valorizzato con un *time-stamp* strettamente compreso tra quelli di cui al punti 1 e 2, e
- la durata calcolata per differenza tra i *time-stamp* di cui ai punti 2 e 3 non sia maggiore del valore del suddetto elemento `<MaxValidity>`;

In ogni caso, tale durata (tra *time-stamp* ai punti 2 e 1 o, alternativamente, tra quelli ai punti 2 e 3) NON DEVE superare il limite massimo impostato dal SGD.

Se l'attributo-delega facoltativo di cui al punto 6 è presente, allora DEVE essere presente anche quello di cui al punto 4, con un valore non superiore di quello al punto 6; inoltre, la delega digitale è valida solo se:

- l'attributo di cui al punto 4 è strettamente *inferiore* di quello al punto 6.

6. Metadata SAML relativi alle deleghe digitali

I metadata di cui al presente Capitolo sono conformi a tutte le norme relative agli schemi di identificazione elettronica nazionali,[17] oltre allo standard tecnico [**samlMeta**]. Le convenzioni sintattiche relative all'XML sono le medesime definite al §4.

6.1. Struttura dei metadata tradizionali del SP

Il SP federato nel sistema delle deleghe digitali può avere uno o più metadata SAML a seconda di quanto previsto dalla normativa vigente degli schemi di identificazione elettronica nazionali (CIE o SPID). Ciascuno di questi metadata-SP è identificato da un "EntityID-SP" che rispetta anch'esso le *naming convention* dei relativi schemi. Tra tutti i metadata esiste tuttavia un metadata principale, il cui EntityID è denominato "globale." Le associazioni e i controlli incrociati di cui ai §§4 e **Error! Reference source not found.** POSSONO essere effettuati relativamente agli EntityID di pertinenza oppure, se effettuati rispetto agli EntityID "globali," saranno comunque considerati validi al *solo* fine di stabilire la validità di una delega digitale – ad esempio, controllare l'appartenenza di un determinato punto di ancoraggio (cfr. §**Error! Reference source not found.**) a un dato SP.

I metadata-SP DEVONO:

1. Includere nell'elemento `<md:AdditionalMetadataLocation>` la URL del registro delle AA ove è pubblicato il corrispondente metadata-deleghe del SP (cfr. §0).
2. Nell'elemento `<md:Extensions>` figlio dell'elemento-radice `<EntityDescriptor>`[18] sono presenti:
   2.1. un elemento `<sgd:EntityIDs>`, contenente:
      2.1.1. l'attributo `sgd:globalEntityID`, valorizzato con l'EntityID "globale" sopra definito,
      2.1.2. un solo elemento `<sgd:EntityID>`, contenente:
         2.1.2.1. l'attributo booleano `isDefault`, valorizzato positivamente,
         2.1.2.2. l'elemento valorizzato con il medesimo EntityID "globale" di cui al 2.1.1;
      2.1.3. uno o più elementi `<sgd:EntityID>`, ciascuno valorizzato con l'EntityID di un altro metadata associato al medesimo SP – l'elemento obbligatorio valorizzato con l'EntityID-delega (cfr. §0) e, se non già presente, quello contenente l'EntityID-SP dell'attuale metadata.
3. Adottare almeno un AtCS con il quale si richiede il codice fiscale del soggetto (che sarà utilizzato per richiedere all'IDP il codice fiscale del **delegato**, cfr. §0), cioè un elemento `<md:AttributeConsumingService>` contenete un elemento `<md:RequestedAttribute>` che si riferisca all'attibuto identificativo `fiscalNumber`.

[17] Per quanto riguarda i metadata SPID si faccia riferimento, ad esempio, agli Avvisi SPID №19/2020 e №29/2020 e ss.mm.ii.
[18] Da non confondersi con l'omonimo elemento facoltativamente figlio di `<SPSSODescriptor>` o suoi affini del tipo `RoleDescriptorType`.

Inoltre, si RACCOMANDA che:

4. Sia presente un solo elemento `<md:SPSSODescriptor>`.
5. Siano presenti gli elementi `<md:AdditionalMetadataLocation>` con le URL ove sono pubblicati *tutti* i metadata-SP associati a classi di servizio corrispondenti, nel metadata-deleghe, a classi di servizio delegabili.
6. Siano presenti due AtCS dedicati all'*eIDAS Minimum attribute set for physical persons* (indice 100) e all'*eIDAS Full attribute set for physical persons* (indice 101), per la compatibilità con lo schema di interoperabilità ai sensi di [**eIDAS**].
7. Per le classi di servizio delegabili associate a servizi fruibili anche senza delega digitale, sia adottata una chiara corrispondenza tra gli AtCS di queste ultime e quelli delle altre classi di servizio, inclusa la *naming convention* dei relativi attributi identificativi e attributi-delega (cfr. §6.2, punto 5.3.5). In particolare, questi AtCS contengono:
   7.1. Almeno il codice fiscale del delegato, richiedendo l'attributo.
8. Gli elementi `<Organization>` e `<ContactPerson>` siano adottati valorizzando con quanti più sotto-elementi facoltativi possibili.

Segue un esempio di metadata-SP per un SP pubblico utilizzabile sia per lo schema CIE che per quello SPID,[19] la cui implementazione è gestita da un partner tecnologico (nel contesto CIE) ovvero da un Aggregatore (nel contesto SPID)[20] privato. Si noti la presenza di sette classi di servizi (AtCS) distinte, di cui quello rilevante per la gestione delle deleghe digitali ha indice 40 (righe 49 e seguenti – cfr. punto 3 dal precedente elenco). Si notino anche i riferimenti al metadata-deleghe del SP e all'identificazione dell'EntityID del metadata-SP come quello "globale."

```
<md:EntityDescriptor
 entityID="https://www.SPdiesempio.it"
 validUntil="2026-01-01T00:00:00Z"
 ID="md-2abdd8d0-370e-4f76-b281-8eebb276faes"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 xmlns:ui="urn:oasis:names:tc:SAML:metadata:ui"
 xmlns:sgd="https://deleghedigitali.gov.it/saml-extensions"
 xmlns:spid="https://spid.gov.it/saml-extensions"
 xmlns:cie="https://www.cartaidentita.interno.gov.it/saml-extensions">
  <ds:Signature>  [……]  </ds:Signature>
  <md:Extensions>
          <sgd:EntityIDs SGD:globalEntityID="https://www.SPdiesempio.it">
                  <sgd:EntityID isDefault="true">https://www.SPdiesempio.it</sgd:EntityID>
                  <sgd:EntityID>del:https://www.SPdiesempio.it</sgd:EntityID>
          </sgd:EntityIDs>
          <spid:SignatureArt20>
                  <spid:FileTransferService Location="https://www.SPdiesempio.it/SPIDsignature/"/>
          </spid:SignatureArt20>
  </md:Extensions>
  <md:SPSSODescriptor
    AuthnRequestsSigned="true"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <md:Extensions>
                  <ui:UIInfo>
```

[19] Possono essere incluse anche estensioni specifiche dello schema, come la "firma con SPID" dell'esempio (righe 17-19 e seguenti).
[20] In merito ai soggetti aggregatori nella federazione SPID, si veda l'Avviso SPID №19/2020 e ss.mm.ii.

```
                        <ui:Logo height="800" width="800">http://www.SPdiesempio.it/SP.png</ui:Logo>
                </ui:UIInfo>
        </md:Extensions>
        <md:KeyDescriptor use="signing"> [……] </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption"> [……] </md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="[……]"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" [……]/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" [……]/>
        <md:AssertionConsumerService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
          Location="https://www.SPdiesempio.it/binding/post"
          index="0"
          isDefault="true"/>
        <md:AttributeConsumingService index="0"> [……] </md:AttributeConsumingService >
        <md:AttributeConsumingService index="1"> [……] </md:AttributeConsumingService >
        <md:AttributeConsumingService index="2">
                <md:ServiceName xml:lang="">urn:uuid:UUID_02</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Certificati anagrafici</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Anagraphics certificates</md:ServiceDescription>
                <md:RequestedAttribute Name="name" [……]/>
                <md:RequestedAttribute Name="familyName" [……]/>
                <md:RequestedAttribute Name="fiscalNumber" [……]/>
                <md:RequestedAttribute Name="mobilePhone" [……]/>
                <md:RequestedAttribute Name="email" [……]/>
        </md:AttributeConsumingService >
        <md:AttributeConsumingService index="40">
                <md:ServiceName xml:lang="">urn:uuid:UUID_40</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Identità del delegato</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Delegate person Id</md:ServiceDescription>
                <md:RequestedAttribute
                  Name="fiscalNumber"
                  FriendlyName="codice fiscale del delegato"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
        </md:AttributeConsumingService >
        <md:AttributeConsumingService index="77">
                <md:ServiceName xml:lang="">urn:uuid:UUID_77</md:ServiceName>
                <md:ServiceName xml:lang="it">Sottoscrizione elettronica ex art.20 CAD</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Firma con SPID</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">“SPID” e-Signing</md:ServiceDescription>
        </md:AttributeConsumingService >
        <md:AttributeConsumingService index="100"> [……] </md:AttributeConsumingService >
        <md:AttributeConsumingService index="101"> [……] </md:AttributeConsumingService >
</md:SPSSODescriptor>
<md:Organization>
        <md:OrganizationName xml:lang="it">Istituto Service Provider di Esempio</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">ISPE</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">https://www.SPdiesempio.it/it-IT/</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="technical other" spid:entityType="spid:aggregator">
        <md:Extensions>
                <spid:VATNumber>IT01234567890</spid:VATNumber>
                <spid:FiscalCode>9753108642</spid:FiscalCode>
                <cie:Private/>
                <spid:PublicServicesFullAggregator/>
                <cie:NACE2Code>codiceATECO_referenteTecnico</cie:NACE2Code>
                <cie:Country>IT</cie:Country>
```

```
                    <cie:Municipality>codiceISTAT_referenteTecnico</cie:Municipality>
            </md:Extensions>
            <md:Company>Partner Tecnologico per Soluzioni di Identità Federata s.r.l.</md:Company>
            <md:EmailAddress>info.eid@partnertecnologicoidfederata.com</md:EmailAddress>
            <md:TelephoneNumber>+390999135792</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson contactType="administrative other" spid:entityType="spid:aggregated">
            <md:Extensions>
                    <spid:IPACode>codiceIPA_soggetto</spid:IPACode>
                    <spid:FiscalCode>2468013579</spid:FiscalCode>
                    <cie:Public/>
                    <spid:Public/>
                    <cie:IPACategory>categoriaIPA_SP</cie:IPACategory>
                    <cie:Country>IT</cie:Country>
                    <cie:Province>sigla_provincia_SP</cie:Province>
                    <cie:Municipality>codiceISTAT_comune_SP</cie:Municipality>
            </md:Extensions>
            <md:Company>Istituto Service Provider di Esempio</md:Company>
            <md:EmailAddress>info@spesempio.gov.it</md:EmailAddress>
            <md:TelephoneNumber>+390011223344</md:TelephoneNumber>
    </md:ContactPerson>
    <md:AdditionalMetadataLocation>
            https://registry.spid.gov.it/metadata/sp/codiceIPA_soggetto__IT01234567890.xml
    </md:AdditionalMetadataLocation>
</md:EntityDescriptor>
```

6.2. Struttura dei metadata-delega del SP

Il SP federato nel sistema delle deleghe digitali possiede l'ulteriore metadata-deleghe, dedicato al SGD (quando questi agisce nel ruolo di un "IDP tecnico" nei confronti del SP) e identificato da un "EntityID-deleghe."

I metadata-deleghe DEVONO avere le seguenti caratteristiche:

1. L'EntityID-deleghe valorizza l'attributo `entityID` dell'elemento `<md:EntityDescriptor>` e deve cominciare con il prefisso "`del:`". Qualora il SP abbia *un solo* metadata-SP, l'EntityID-deleghe è derivato dall'EntityID-SP aggiungendovi tale prefisso.
2. C'è un unico elemento `<md:SPSSODescriptor>` e nessun altro `RoleDescriptor`; al suo interno:
3. Almeno un elemento `<md:KeyDescriptor>` con l'attributo `use` valorizzato come `signing`, utilizzato da norma per contenere il certificato di sigillo elettronico cui afferisce la chiave privata con cui sono sigillare elettronicamente tutte le evidenze informatiche generate dal SP verso il SGD.
4. Sono presenti tanti elementi `<md:AttributeConsumingService>` (AtCS) quante sono tutte e sole le classi di servizio delegabili; per *ciascuno* di essi:
   4.1. È *obbligatoria* la presenza di un elemento `<md:ServiceName>`, con localizzazione "aspecifica" (attributo `xmlns:lang` pari alla stringa vuota), recante un identificativo univoco della classe di servizio in formato UUID versione 4 (e quindi valorizzato con una stringa con prefisso `urn:uuid:`).
   4.2. Se presenti altre istanze *facoltative* dell'elemento `<md:ServiceName>`, tutte *localizzate*, una di esse DEVE esserlo in lingua italiana. Questi elementi sono relativi al funzionamento SAML del SP; ai fini del funzionamento del SGD, invece, sono *ignorati* mentre sono significativi gli omonimi di cui al punto 5.3.6.

4.3. Possono essere presenti una o più istanze dell'elemento <md:ServiceDescription>, tutte localizzate ma soltanto nelle lingue in cui sono presenti istanze di elementi <ServiceName> per la medesima classe di servizi. Questi elementi sono relativi al funzionamento SAML del SP; ai fini del funzionamento del SGD, invece, sono *ignorati* mentre sono significativi gli omonimi di cui al punto 5.3.7.

4.4. Uno o più elementi-vuoti <md:RequestedAttribute>, ciascuno con i seguenti attributi:

4.4.1. `Name` (*obbligatorio*) — identificativo univoco dell'attributo nell'ambito dell'elemento <ServiceClasses> del medesimo metadata, cfr. §5.3.1;

4.4.2. `FriendlyName` (*facoltativo*) — stringa contenente un nome comprensibile dell'attributo;

4.4.3. `NameFormat` (*obbligatorio*) — descrizione del tipo di dato veicolato dall'attributo; DEVE essere un tipo noto negli ambiti dei *namespace* SAML o di quello proprio del SGD.

5. Nell'elemento <md:Extensions> figlio dell'elemento-radice <EntityDescriptor>:[21]

5.1. Un elemento <sgd:EntityIDs>, contenente:

5.1.1. L'attributo sgd:**globalEntityID**, valorizzato con l'EntityID "globale" sopra definito.

5.1.2. Un solo elemento <sgd:EntityID>, contenente:

5.1.2.1. l'attributo **isDefault**, pari a true;

5.1.2.2. l'elemento valorizzato con il medesimo EntityID "globale" di cui al 5.1.1.

5.1.3. Uno o più elementi <sgd:EntityID>, ciascuno valorizzato con l'EntityID di un altro metadata associato al medesimo SP – l'elemento obbligatorio valorizzato con l'EntityID-delega (cfr. §0) e, se non già presente, quello contenente l'EntityID-SP dell'attuale metadata.

5.2. Uno o più elementi *facoltativi* <md:KeyDescriptor>, ciascuno contenente un certificato elettronico utilizzato per altre funzionalità specifiche del sistema delle deleghe digitali. Ogni occorrenza contiene un elemento <ds:KeyInfo> conforme con lo standard [**xmlDSig**] (nella versione adottata dallo standard SAML in uso): il certificato è sempre accluso e può essere opzionalmente presente un identificativo della chiave crittografica adottata (mediante elemento <ds:KeyName>). L'utilizzo per ciascuna occorrenza è regolato dal valore del suo attributo use:

5.2.1. sgd:**webaccess** — usato per certificati di autenticazione di siti web, eventualmente qualificati (cfr. [**eIDAS**]), da utilizzarsi per l'omonimo riconoscimento tra il SGD e ulteriori sistemi client o server (fuori dall'ambito del presente documento);

5.2.2. sgd:**policysealing** — da usarsi per cifrare i documenti informatici, esterni al metadata, referenziati negli elementi-vuoti <sgd:Agreement> dotati di attributo `Location` (cfr. punto 5.5.4.2);

5.3. Un elemento <sgd:ServiceClasses> contenente una **gerarchia**, NON VUOTA di elementi-figli <sgd:ServiceClass>; ciascun ramo della gerarchia può essere costituita da un minimo di 1 ad un massimo di 5 livelli, purché i livelli dell'intera gerarchia non siano superiori a **sei**. Ciascun elemento <ServiceClass> contiene i seguenti attributi ed elementi e segue le seguenti regole:

5.3.1. `AttributeConsumingServiceIndex` (*facoltativo*) — valorizzato con l'indice di un AtCS definito, nell'ambito del medesimo metadata-deleghe, in un elemento di cui al punto 2 (<md:AttributeConsumingService>); i sotto-alberi la cui radice è costituita da un elemento <ServiceClass>:

5.3.1.1. *dotato* di un tale attributo, sono considerati **pieni** e costituiscono perciò una classe di servizi delegabili (cfr. §2);

[21] Da non confondersi con l'omonimo elemento facoltativamente figlio di <SPSSODescriptor> o suoi affini del tipo XML RoleDescriptorType.

5.3.1.2. *non dotato* di un tale attributo, sono considerati un mero contenitore logico di classi di servizi, il cui funzionamento riguarda solo la presentazione all'utente del SGD (p.es. il delegante) di una gerarchia di servizi o classi di servizio, ricadendo ciò al di fuori dell'ambito delle presenti regole tecniche;

5.3.2. `id` (*facoltativo*) — Se presente, è valorizzato con il valore di un particolare elemento `<md:ServiceName>` con localizzazione "aspecifica" – cfr. punto 5.3.1.1, già collegato tramite attributo `AttributeConsumingServiceIndex`.

5.3.3. `sgd:hierarchy` (*facoltativo*) — Valorizzato con uno o più identificatori *senza spazi* (fra di loro, se più di uno, separati da un carattere `0x20` di spazio), ciascuno associante la classe di servizio afferente all'elemento con una o più gerarchie diverse, che ne rappresentino il collocamento all'interno di altrettante tassonomie di servizi digitali. Ad esempio, un indicatore che afferisce a una gerarchia di servizi di ambito "globale," indipendente dal singolo SP e, contemporaneamente, un secondo indicatore che afferisce ai servizi digitali specifici del SP cui il metadata-deleghe afferisce). Si raccomanda di rappresentare tali identificatori mediante OID (secondo la norma RFC-3061), valorizzati come stringhe che cominciano per `urn:oid:`.

5.3.4. `sgd:hered` (*facoltativo*) — booleano che, se presente e valorizzato affermativamente, conferma che tale classe di servizio **eredita** deleghe digitali ammissibili per la classe di servizio superiore nella gerarchia dell'elemento-padre `<ServiceClass>` (mentre la sua assenza è equivalente ad una valorizzazione negativa).

5.3.5. `sgd:nonDelegateAtCSIndex` (*facoltativo*) — Nel caso in cui sia opportuno collegare la classe di servizio ad una classe di servizio non delegabile presente in un metadata del SP, è possibile utilizzare questo attributo, valorizzandolo con il valore di un attributo `AttributeConsumingServiceIndex` presente in un metadata-SP; in caso vi siano più metadata-SP, l'attributo può essere ottenuto separando con un carattere di spazio l'EntityID-SP del metadata cui ci si riferisce dal valore dell'indice del'AtCS.

5.3.6. `<md:ServiceName>` (*uno* o più) — Valorizzato come da propria norma [**samlMeta**], gli elementi posizionati in questo punto sono rilevanti e ad esclusivo utilizzo da parte del SGD e contengono il nome della classe di servizio, localizzata in una lingua specifica; deve essere presente almeno la localizzazione in lingua italiana e, facoltativamente in altre lingue, con la prima lingua facoltativa che deve essere l'inglese. Inoltre, tutti gli elementi `<sgd:ServiceClass>` devono avere lo stesso numero e lingue di localizzazione, adottato anche per gli elementi `<md:ServiceDescription>` e `<md:Agreements>`; per gli elementi-figli all'interno di `<md:Organization>` e, se qualora adottati all'interno del metadata, per gli elementi localizzati definiti in [**samlUI**].

5.3.7. `<md:ServiceDescription>` (zero o più) — Valorizzato come da propria norma [**samlMeta**], gli elementi posizionati in questo punto sono rilevanti e ad esclusivo utilizzo da parte del SGD e contengono una descrizione testuale, localizzata in una lingua specifica. Tutti gli elementi `<sgd:ServiceDescription>` devono avere lo stesso numero e lingue di localizzazione, adottato anche per gli elementi `<md:ServiceClass>` e `<md:Agreements>`.

5.3.8. `<sgd:ServiceClassType>` (*facoltativo*) — Valorizzato con la tipologia (o le tipologie, se separate da uno spazio) di deleghe creabili associate alla relativa classe di servizio delegabile (cfr. §5.1). I valori ammissibili sono:

5.3.8.1. `sgd:type:simple` — delega **semplice** (tipologia di default quando `<sgd:Type>` è mancante);

5.3.8.2. `sgd:type:complex` — delega **complessa**.

5.3.9. `<sgd:MaxValidity>` — Valorizzato con la durata *massima* di una delega digitale per la relativa classe di servizi (cfr. §5.4, nonché il punto 5.3.9.2 per la sua sintassi); contiene i seguenti attributi:

5.3.9.1. `sgd:hered` (*facoltativo*) — booleano che, se presente e valorizzato affermativamente, conferma che tale limite massimo è **ereditato** da tutte le classi di servizio contenute nel sotto-albero afferente all'elemento-padre `<ServiceClass>` (mentre la sua assenza è equivalente ad una valorizzazione negativa) – a meno che un sotto-albero di classi di servizio non contenga un nuovo elemento `<MaxValidity>`: in tal caso, l'istanza locale dell'elemento ha precedenza su quella ereditata;

5.3.9.2. `xsi:type` (*obbligatorio*) — valorizzato come `xsd:duration` .

5.3.10. `<sgd:AgreementRef>` — Elemento contenente l'identificativo univoco (attributo `agreementId`, punto 5.5.1) di uno specifico accordo che è normativamente cogente per i servizi digitali associati all'elemento-padre `<ServiceClass>`;

5.3.10.1. `index` (*facoltativo*) — valorizzato con un numero intero non negativo che stabilisce l'ordine con cui sono presentati gli accordi di cui al punto 5.4; è *facoltativo* qualora le classi di servizio in ambito siano associate ad un solo accordo (cioè è presente *un solo* elemento `<AgreementRef>`); altrimenti, tale attributo DEVE essere presente in *tutti* gli elementi `<AgreementRef>` ed essere valorizzato con numeri differenti;

5.3.10.2. `sgd:hered` (*facoltativo*) — booleano che, se presente e valorizzato affermativamente, conferma che il relativo accordo è **ereditato** da tutte le classi di servizio contenute nel sotto-albero afferente all'elemento-padre `<ServiceClass>` (mentre la sua assenza è equivalente ad una valorizzazione negativa), con eventuali accordi specificati nei figli `<ServiceClass>` in *aggiunta* a quelli vigenti; inoltre, qualora un medesimo accordo venga associato più volte ad una classe di servizi, conta una sola volta e l'ordine più alto (associato al più basso valore dell'attributo `index`) ha la precedenza; in caso di sovrapposizioni di accordi provenienti da diversi livelli (ereditati) di gerarchia, gli accordi associati a livelli più alti sono sempre presentati prima.

5.4. `<sgd:SoftAttributes>` — *facoltativo* e comunque presente solo in caso vi sia almeno un AtCS associato ad uno o più attributi specifici (o "*soft*," cfr. §5.2). Rappresenta un elenco di elementi `<sgd:SoftAttribute>` , ciascuno con informazioni facoltative circa un attributo, particolarmente untili per il delegante in fase di creazione di una delega digitale per le classi di servizio associate a tali attributi:

5.4.1. `Name` (*obbligatorio*) — associato al nome unico dell'attributo, così come è chiamato nell'AtCS o negli AtCS del medesimo metadata e che segue la naming convention di cui al §5.2.

5.4.2. `xmlns:lang` (*obbligatorio*) — specifica la lingua in cui sono declinate le informazioni contenute nel presente elemento `<SoftAttribute>`. Un medesimo attributo specifico può essere associato a più istanze di questo elemento – con il medesimo attributo `Name` ma ciascuna con un attributo valorizzati differentemente. Deve essere presente almeno un'istanza per la lingua italiana e, se presente più di un'istanza, deve essere presente almeno quella in lingua inglese. Infine, tutti gli attributi specifici sono associati ad istanze per le medesime lingue all'interno di uno stesso metadata-deleghe.

5.4.3. `FriendlyName` (*facoltativo*) — contiene un nome colloquiale dell'attributo specifico, eventualmente utilizzato dal SGD in fase di creazione, di modifica o di utilizzo della delega per visualizzare l'attributo al delegante o al delegato. Può essere omesso se le informazioni relative agli attributi specifiche sono declinate solo in una lingua (l'italiano): in tal caso, fa fede l'attributo `FriendlyName` nell'elemento `<RequestedAttribute>` dell'AtCS corrispondente.

5.4.4. `sgd:HelperText` (*facoltativo*) — Contiene un testo che descrive ancora più approfonditamente l'attributo e come il delegante deve operativamente valorizzarlo in fase di creazione della delega. Ad esempio: potrebbe spiegare la sintassi del testo da riempire (p.es. numero di targa automobilistica); avvertire di non usare caratteri diversi da quelli alfanumerici; ovvero come selezionare una data precisa da un calendario virtuale; ecc..

5.5. `<sgd:Agreements>` — *obbligatorio* se è presente un elemento `<AgreementRef>` come figlio di almeno un `<ServiceClass>` ovvero `<ServiceClasses>`. Rappresenta un catalogo di tutti i tipi di **accordi** previsti dal SP (che richiedono, cioè, un'interazione preventiva con persone fisiche), normativamente associati all'utilizzo delle deleghe digitali – da presentare al delegante, in fase di creazione della delega digitale, o al delegato, in fase di utilizzo della medesima. Il funzionamento e l'interattività con tali accordi è demandato ai manuali operativi del SGD o ad altri Avvisi. Tale elemento è costituito da un elenco di uno o più elementi `<sgd:Agreement>` (ciascuno associato ad un simile accordo), *tutti* dotati dei seguenti attributi ed elementi:

5.5.1. `sgd:agreeementId` — identificativo (UID) dell'accordo, unico nell'ambito del metadata-deleghe; si raccomanda di riferirsi a identificativi *machine-readable* – come ad esempio degli UUID versione 4 (valorizzati con una stringa con prefisso `urn:uuid:`) ovvero degli OID esistenti in un elenco-directory (ITU-T X.500) o riusandoli da certificazioni elettroniche esistenti (X.509/RFC-5280 e X.520 – valorizzati con una stringa con prefisso `urn:oid:` – cfr. RFC-3061).

5.5.2. `xmlns:lang` (*obbligatorio*) — localizza ciascun accordo in una data lingua, secondo le seguenti regole:

5.5.2.1. la lingua valorizzante l'attributo è indicata mediante la codifica ISO 639-1;

5.5.2.2. un medesimo accordo DEVE essere declinato almeno in lingua italiana;

5.5.2.3. un medesimo accordo PUÒ essere declinato in più lingue aggiuntive e, in questo caso, DEVE essere declinato almeno in lingua inglese;

5.5.2.4. tutti gli accordi nel metadata DEVONO essere declinati nelle medesime lingue;

5.5.2.5. le versioni localizzate del medesimo accordo hanno la comune valorizzazione dell'attributo `id` e diverse valorizzazioni dell'attributo `lang`;

5.5.2.6. le differenti localizzazioni di uno stesso accordo devono avere la medesima struttura dei sotto-elementi (incluso l'utilizzo degli stessi elementi XML, loro attributi e valori degli attributi), differendo quindi solo per la lingua dei testi liberi.

5.5.3. `sgd:agreementType` (*obbligatorio*) — tipologia giuridica dell'accordo, a scelta tra il seguente elenco di stringhe, ulteriormente estendibile tramite Avvisi:

5.5.3.1. `sgd:legal:infopolicy` — informativa circa il trattamento dei dati personali,

5.5.3.2. `sgd:legal:privacypolicy` — consenso al trattamento dei dati personali (*privacy policy*),

5.5.3.3. `sgd:legal:NDA` — accordo di riservatezza (*non-disclosure agreement*, o NDA),

5.5.3.4. `sgd:legal:CP` — *certificate policy* (o CP) inerente l'utilizzo di certificati elettronici;

5.5.3.5. `sgd:legal:CPS` — *certificate practice statement* (o CPS) inerente l'emissione di suddetti certificati,

5.5.3.6. `sgd:legal:TC` — altro accordo di natura commerciale,

5.5.3.7. `sgd:legal:notice` — altra notifica,

5.5.3.8. `sgd:legal:policy` — altro tipo di politica, non afferente alle precedenti tipologie,

5.5.3.9. `sgd:other` — altro tipo di avviso, anche non normativo.

5.5.4. `md:Location` (*facoltativo*) — Se presente, il corrispondente elemento `<sgd:Agreement>` è *vuoto*, non ha altri attributi e l'accordo corrispondente è:

5.5.4.1. referenziato da un documento informatico in formato XML, esternalizzato al metadata-delega e reso disponibile al SGD mediante URL in HTTPS valorizzante l'attributo `Location`;

5.5.4.2. sigillato elettronicamente, mediante lo standard [**xmlDSig**], utilizzando la chiave privata afferente a uno dei certificati elettronici presenti nello stesso metadata-delega, all'interno di un elemento `<KeyDescriptor>`, figlio di `<Extensions>` e con attributo `use` valorizzato con `sgd:policysealing`, come da punto 5.2.2;

5.5.4.3. la cui radice è costituita da un elemento `<sgd:Agreement>`, con *namsepace* localmente ri-definito, che segue la sintassi di cui al punto 5.4 e seguenti, ma *senza* contenere l'attributo `Location`.5.5.5

5.5.5. `<sgd:Clause>` (uno o più, ma *nessuno* se il padre sia dotato dell'attributo `Location` – cfr. punto 5.5.4) — singola clausola dell'accordo di cui è elemento-figlio, dotato dei seguenti attributi e valorizzato con una sequenza non vuota dei seguenti elementi:

5.5.5.1. `sgd:interaction` (*facoltativo*) — modalità di interazione richiesta, a scelta tra il seguente elenco di stringhe, ulteriormente estendibile tramite Avvisi:

5.5.5.1.1. `sgd:legal:check` — richiesta di presa visione (o "consenso implicito"): l'utente DEVE spuntare o de-spuntare un *flag* per confermare di aver visionato il documento;

5.5.5.1.2. `sgd:legal:consent` — richiesta di consenso: l'utente DEVE prestare o negare un consenso "esplicito,"

5.5.5.1.3. `sgd:legal:subscription` — richiesta di sottoscrizione; l'utente DEVE prestare un consenso rappresentato sotto forma di sottoscrizione elettronica – la cui implementazione esula dalle finalità del presente Allegato Tecnico;

5.5.5.2. `<sgd:choice>` (zero o più) — contiene il testo di una possibile scelta per l'utente relativamente alla clausola; l'obbligatorietà o il numero di ripetizioni di questo elemento esula dallo scopo delle presenti Linee Guida; è valorizzato con il testo associato alla scelta (declinato nella lingua indicata con l'attributo `lang` dell'elemento-padre di cui al punto **Error! Reference source not found.**) ed è dotato degli attributi al seguente elenco; è valorizzato con un breve periodo inerente alla scelta (p.es. «accetto», «non acconsento», «ho letto», «firmato») e sono ammessi all'interno i seguenti *tag* [**html5**]: `<abbr>`, `<acronym>`, `<b>`, `<blockquote>`, `<cite>`, `<code>`, `<dfn>` (che può riferirsi a definizioni nell'ambito del medesimo elemento `<Agreement>`), `<em>`, `<q>`, `<strong>`, `<sub>`, `<sup>`.

5.5.5.2.1. `index` (*obbligatorio*) — valorizzato con un numero intero positivo che stabilisce l'ordine delle scelte di interazione per la clausola cui l'elemento appartiene; i numeri DEVONO cominciate da `1` ed essere consecutivi; PUÒ essere omesso solo se l'accordo è composto da una singola clausola.

5.5.5.2.2. `md:isDefault` (*facoltativo*) — booleano che indica quale scelta sia quella predefinita per la clausola; qualora sia assente, si assume che la relativa scelta non sia quella predefinita; un elemento `<choice>` DEVE avere questo attributo valorizzato affermativamente, a meno che la tipologia di clausola (di cui al punto 5.5.5.1) *non* preveda alcuna scelta predefinita, ma al di fuori dell'ambito del presente documento);

5.5.5.3. `<p>` (uno o più) — *non* vuoto, rappresenta un singolo paragrafo della clausola e contiene del testo libero (declinato nella lingua indicata con l'attributo `lang` dell'elemento-padre di cui al punto **Error! Reference source not found.**); ammesso l'utilizzo dei seguenti *tag* dello standard [**html5**]: `<abbr>`, `<acronym>`, `<b>`, `<blockquote>`, `<cite>`, `<code>`, `<dfn>` (che può riferirsi a definizioni nell'ambito del medesimo elemento `<Agreement>`), `<dl>` (contenente uno o più `<dd>`), `<em>`, `<ol>` (contenente uno o più `<li>`), `<q>`, `<strong>`, `<sub>`, `<sup>`, `<th>`

(ammessi i suoi sotto-elementi standard), `<time>`, `<ol>` (contenente uno o più `<li>`); NÉ `<p>` NÉ i suoi figli, però, possono avere alcun attributo;

5.5.5.4. `<title>` (zero o più) — rappresenta il titolo facoltativo della clausola e, se presente, è il primo figlio della clausola, senza altri caratteri prima; NON sono ammessi attributi;

5.5.5.5. `<hn>` (con *n* da 1 a 6; zero o più) — usato per i titoli facoltativi relativi a paragrafi diversi; NON sono ammessi attributi.

5.6. `<EndServices>` (*facoltativo*) — Se presente, indica che la classe di servizi cui appartiene è associata ad un elenco *di nomi* di servizi digitali offerti dal SP. Il SGD può così elencare o presentare tali servizi anche se questi non sono funzionalmente distinguibili fra di loro: la massima granularità in tal senso è ottenuta dalla classe di servizi (elemento `<sgd:AttributeConsumingService>`). È costituito da un elenco di uno o più nomi di servizi, rappresentati da elementi `<md:ServiceName>`, ciascuno contenente:

5.6.1. `index` (*obbligatorio*) — valorizzato con un numero intero positivo che stabilisce l'ordine formale con cui i nomi di servizi digitali sono presentati. Più istanze di `<ServiceName>` possono avere il medesimo valore di questo attributo qualora rappresentino il nome dello stesso servizio ma declinato in lingue differenti;

5.6.2. `xmlns:lang` (*obbligatorio*) — specifica la lingua di localizzazione per il nome del servizio digitale, codificata secondo lo standard ISO 639-1; per ciascun nome DEVE essere presente almeno la lingua italiana.

5.7. Allo scopo di consentire al SGD di personalizzare visivamente il SP cui afferiscono i servizi delegabili in tutte le pagine e i documenti presentati all'utente (delegante o delegato) – inclusi gli eventuali accordi di cui al punto 5.4 – DEVE essere presente *almeno* un elemento `<mdui:Logo>` (all'interno di `<mdui:UIInfo>`, dentro `<Extensions>`, dentro `<SPSSODescriptor>`), come previsto in [**samlUI**]; ciascun logo DEVE:

5.7.1. essere referenziato tramite un URL con schema HTTPS ad un'immagine in formato PNG, cfr. [**eDoc**];

5.7.2. essere di dimensioni non inferiori a 1000 punti (pixel) per lato;

5.7.3. avere le trasparenze sufficienti ad essere sovrapposto a sfondi di diversi colori chiari e trame.

5.8. NON sono adottati i riferimenti a URL esterni per le informative o le privacy policy del SP, come sarebbe previsto dallo standard [**samlUI**], in quanto il SGD utilizza il proprio sistema degli 'accordi' di cui al punto 5.4.

6. Gli elementi figli di `<md:Organization>` sono declinati nelle medesime lingue utilizzate per gli elementi di cui ai punti 4 e 5.3.

7. È presente almeno un'occorrenza di elemento `<md:ContactPerson>`; tutte le sue occorrenze sono comunque conformi con quanto previsto dagli schemi di identificazione elettronica nazionale per i metadata sia degli SP che degli IDP.

8. All'interno dell'elemento `<md:Extensions>` di *ciascuna* occorrenza dell'elemento `<ContactPerson>`, sono presenti *almeno* le seguenti estensioni (valorizzate in base a quanto previsto dalle normative degli schemi di identificazione elettronica di riferimento):

8.1. la provincia (`<cie:Province>`) ove è situata la sede legale cui l'antenato si riferisce (se il soggetto è situato in Italia), ovvero

8.2. il codice-paese (`<cie:Country>`) ove è situata la sede legale cui l'antenato si riferisce (se il soggetto è situato all'estero);

8.3. il codice IPA (`<spid:IPACode>`) e la categoria IPA (`<cie:IPACategory>`), qualora l'antenato si riferisca ad una pubblica amministrazione (PA) o a un gestore di pubblico servizio;

8.4. il numero di partita IVA (`<spid:VATNumber>`) e/o il codice fiscale (`<spid:FiscalNumber>`), insieme a uno o più codici ATECO/NACE2 (`<cie:NACE2Code>`), qualora l'antenato si riferisca ad un soggetto di diritto privato o a un gestore di pubblico servizio.

Gli AtCS delle classi di servizio delegabili di cui al precedente punto 4 DEVONO essere composte da un *ensemble* di: attributi identificativi (riferiti al **delegato**), ed eventualmente altre *caratteristiche* della delega (come definite al punto *d)* del §2, cfr. seguente punto **Error! Reference source not found.**), valorizzandone opportunamente i nomi-attributi (cfr. precedente punto 4.4), come specificato al seguente elenco:

i. Almeno l'attributo identificativo `fiscalNumber`, riferito al **delegato**, trattato nel metadata-deleghe del SGD (cfr. §6.3), come "IDP tecnico" al punto 2.5.1, e come "SP tecnico" al punto 3.5.1;
ii. uno o più attributi-delega riferiti al **delegante**, i cui nomi cominciano con il suffisso `delegator`, trattati nel metadata-deleghe del SGD (§6.3) solamente nel ruolo di "IDP tecnico" al punto 2.5.2;
iii. zero o più attributi specifici, il cui nome comincia per `soft:` – introdotti al §5;
iv. zero o più ulteriori caratteristiche (cfr. punto *d)* del §2), veicolate tramite attributi, il cui nome comincia per `delegation` – anch'essi introdotte al §5.

Gli elementi e attributi di cui ai punti 4.2 (`<ServiceName>`), 4.3 (`<ServiceDescription>`) e 4.4.2 (`FriendlyName`) non sono utilizzati nel sistema delle deleghe digitali: sono mantenuti per compatibilità con lo standard [**samlMeta**].

Inoltre, si RACCOMANDA che:

9. Siano presenti gli elementi `<md:AdditionalMetadataLocation>` con le URL ove sono pubblicati – o resi disponibili al SGS – *tutti* i metadata-SP associati a classi di servizio corrispondenti, nel metadata-deleghe, a classi di servizio delegabili.
10. Siano presenti due AtCS dedicati all'*eIDAS Minimum attribute set for physical persons* (indice 100) e all'*eIDAS Full attribute set for physical persons* (indice 101).
11. Per le classi di servizio delegabili associate a servizi fruibili anche senza delega digitale, sia adottata una chiara corrispondenza tra gli AtCS di queste ultime e quelli delle altre classi di servizio, inclusa la *naming convention* dei relativi attributi identificativi e attributi-delega.
12. In caso di classi di servizio delegabili con attributi specifici, si utilizzi l'attributo `FriendlyName` per
13. Gli elementi `<md:Organization>` e `<md:ContactPerson>` sono adottati, valorizzando quanti più elementi discendenti possibili (in base anche alle normative degli schemi di identificazione elettronica adottati).

Come specificato al §2, ulteriori regole tecniche di pertinenza dei metadata-deleghe sono pubblicate mediante Avvisi.

Segue un esempio di metadata-deleghe relativo al medesimo SP di cui al §6.1. Si noti la presenza di sole cinque classi di servizio delegabili (e relativi AtCS, di cui una solo relativa a deleghe 'complesse'), la gerarchizzazione di queste classi di servizio con le informazioni di pertinenza del SGD, i riferimenti al metadata-SP del SP, all'identificazione dell'EntityID di quest'ultimo come quello "globale" e all'inclusione del riferimento URL ad un logotipo del SP.

Infine, incrociando i dati del metadata-deleghe del SP con quelli del metadata dell'SGD (cfr. esempio al §6.3), si evince che la classe di servizi con AtCS 1 (descritta come 'servizi anagrafici'), definita nel primo metadata come appartenente a due gerarchie contemporaneamente (basate su archi OID distinti) è definita nel secondo metadata come associabile a deleghe globali – quando queste sono create relativamente all'oid definito nel secondo metadata (quello che termina con `.15.44.926`). Non potranno invece essere create deleghe globali per i servizi di cui alla classe associata all'AtCS

2 (descritta come 'ritiro di certificati anagrafici') poiché, nonostante questa classe di servizi delegabili sia una sotto-classe della precedente, tale classe di servizi ha una tipologia complessa che (per quanto definito al §5.3, cioè per via di ulteriori adempimenti necessari – probabilmente a carico del SP – in fase di creazione della delega) non può essere associata a deleghe globali.

```
<md:EntityDescriptor
 entityID="del:https://www.SPdiesempio.it"
 validUntil="2022-01-01T00:00:00Z"
 ID="md-225a4c23-be5a-4dc5-9a5a-bb3be889e2d1"
 xmlns:html="http://www.w3.org/TR/"
 xmlns:ds="urn:oasis:names:tc:www.w3.org/2000/09/xmldsig#"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
 xmlns:sgd="https://deleghedigitali.gov.it/saml-extensions"
 xmlns:spid="https://spid.gov.it/saml-extensions"
 xmlns:cie="https://www.cartaidentita.interno.gov.it/saml-extensions"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ds:Signature>  [……]  </ds:Signature>
  <md:Extensions>
          <sgd:EntityIDs SGD:globalEntityID="https://www.SPdiesempio.it">
                  <sgd:EntityID isDefault="true">https://www.SPdiesempio.it</sgd:EntityID>
                  <sgd:EntityID>del:https://www.SPdiesempio.it</sgd:EntityID>
          </sgd:EntityIDs>
          <sgd:ServiceClasses>
                  <sgd:ServiceClass sgd:hierarchy="urn:oid:[……].6.15.129">
                          <md:ServiceDescription xmlns:lang="it">Servizi civici</md:ServiceDescription>
                          <md:ServiceDescription xmlns:lang="en">Citizenship</md:ServiceDescription>
                          <sgd:MaxValidity hered="true" xsi:type="xsd:duration">P2Y</sgd:MaxValidity>
                          <sgd:AgreementRef hered="true">urn:uuid[…]UUID_infopolicy</sgd:AgreementRef>
                          <sgd:ServiceClass
                            md:AttributeConsumingServiceIndex="1"
                            id="urn:uuid:UUID_del.01"
                            sgd:hierarchy="urn:oid:[……].6.15.129.1  urn:oid:[……].15.44.926"
                            sgd:hered="true"
                            sgf:nonDelegateAtCSIndex="urn:uuid:UUID_01">
                                  <md:ServiceDescription lang="it">Anagrafici</md:ServiceDescription>
                                  <md:ServiceDescription lang="en">Anagraphics</md:ServiceDescription>
                                  <sgd:EndServices>
                                      <md:ServiceName index="1" lang="it">servizio 1</md:ServiceName>
                                      <md:ServiceName index="2" lang="it">servizio 2</md:ServiceName>
                                      [……]
                                      <md:ServiceName index="n" lang="it">servizio n</md:ServiceName>
                                  </sgd:EndServices>
                                  <sgd:ServiceClass
                                    md:AttributeConsumingServiceIndex="2"
                                    id="urn:uuid:UUID_del.02"
                                    sgd:hierarchy="
                                          urn:oid:[……].6.15.129.2
                                          urn:oid:[……].4342.3.43.424.23"
                                    sgd:hered="false"
                                    sgd:nonDelegateAtCSIndex="urn:uuid:UUID_02"/>
                                          <md:ServiceDescription lang="it">
                                                  Ritiro di certificati anagrafici
                                          </md:ServiceDescription>
```

```
                                        <md:ServiceDescription lang="it">
                                                Pickup of anagraphic certificates
                                        </md:ServiceDescription>
                                        <sgd:ServiceClassType>
                                                SGD:type:complex
                                        </sgd:ServiceClassType>
                                        <sgd:MaxValidity type="duration">P30D</sgd:MaxValidity>
                                        <sgd:AgreementRef>
                                                urn:oid:[……].4342.3.43.424.23
                                        </sgd:AgreementRef>
                                        <sgd:EndServices>
                                                <md:ServiceName index="1">[…]</md:ServiceName>
                                                <md:ServiceName index="2">[…]</md:ServiceName>
                                                [……]
                                        </sgd:EndServices>
                                        <md:RequestedAttribute
                                          Name="https://www.SPdiesempio.it?documentId"
                                          FirendlyName="Id documento"
                                          sgd:soft="true"
                                          xsi:type="xsd:string"/>
                                        <md:RequestedAttribute
                                          Name="https://www.SPdiesempio.it?bookingTime"
                                          FriendlyName="data e ora di ritiro"
                                          sgd:soft="true"
                                          xsi:type="xsd:dateTime"/>
                                </sgd:ServiceClass>
                        </sgd:ServiceClass>
                </sgd:ServiceClass>
                <sgd:ServiceClass
                  SGD:hierarchy="urn:oid:[……].6.15.30"/>
                        <md:ServiceDescription lang="it">CIE e eIDAS</md:ServiceDescription>
                        <md:ServiceDescription lang="en">CIE & other eID's</md:ServiceDescription>
                        <sgd:MaxValidity
                          sgd:hered="true"
                          xsi:type="xsd:duration">P60D</sgd:MaxValidity>
                        <sgd:AgreementRef index="1" sgd:hered="true">
                                urn:uuid:UUID_infopolicy
                        </sgd:AgreementRef>
                        <sgd:AgreementRef index="2" sgd:hered="false">
                                urn:uuid:UUID_privacypolicy
                        </sgd:AgreementRef>
                        <sgd:ServiceClass
                          md:AttributeConsumingServiceIndex="100"
                          id="urn:uuid:UUID_del.100"
                          sgd:hierarchy="urn:oid:[……].6.15.129.30.100"
                          sgd:nonDelegateAtCSIndex="urn:uuid:UUID_100"/>
                                <md:ServiceDescription lang="it">eIDAS Min.</md:ServiceDescription>
                                <md:ServiceDescription lang="en">eIDAS Full</md:ServiceDescription>
                                <sgd:EndServices>  […]  </sgd:EndServices>
                        </sgd:ServiceClass>
                        <sgd:ServiceClass
                          md:AttributeConsumingServiceIndex="101"
                          id="urn:uuid:UUID_del.100"
                          sgd:hierarchy="urn:oid:[……].6.15.129.30.101"
                          sgd:nonDelegateAtCSIndex="urn:uuid:UUID_101"/>
                                <md:ServiceDescription lang="it">eIDAS full</md:ServiceDescription>
```

```
                                    <md:ServiceDescription lang="en">eIDAS full</md:ServiceDescription>
                                    <sgd:AgreementRef>urn:uuid:UUID_eidas-policy</sgd:AgreementRef>
                            </sgd:ServiceClass>
                    </sgd:ServiceClass>
            </sgd:ServiceClasses>
            <sgd:SoftAttributes>
                    <sgd:SoftAttribute
                      xmlns:lang="it-IT"
                      Name="soft:https://www.SPdiesempio.it?documentId"
                      FriendlyName="Identificativo unico del documento"
                      HelperText="Digitare il numero seriale del documento da scaricare, avendo cura di
controllarne l'esattezza (pena l'impossibilità di fruire della delega digitale. Sono ignorati i caratteri
di spaziatura e di interpunzione, mentre è importante la distinzione tra maiuscole e minuscole."/>
                    <sgd:SoftAttribute
                      xmlns:lang="en-GB"
                      Name="soft:https://www.SPdiesempio.it?documentId"
                      FriendlyName="Document unique identifier"
                      HelperText="Enter the case-insensitive serial number of the document to download,
taking care of its exactness. Whitespaces and other symbols are irrelevant."/>
                    <sgd:SoftAttribute
                      xmlns:lang="it"
                      Name="soft:https://www.SPdiesempio.it?bookingTime"
                      FriendlyName="Data e ora della prenotazione"
                      HelperText="Selezionare una data e un orario dai box sotto"/>
                    <sgd:SoftAttribute
                      xmlns:lang="en"
                      Name="soft:https://www.SPdiesempio.it?bookingTime"
                      FriendlyName="Booking date and time"
                      HelperText="Please choose a date and time from the selection boxes below"/>
            </sgd:SoftAttributes>
            <sgd:Agreements xmlns="http://www.w3.org/TR/">
                    <sgd:Agreement
                      sgd:agreementID="urn:uuid:UUID_infopolicy"
                      sgd:agreementType="sgd:legal:infopolicy"
                      xmlns:lang="it">
                            <sgd:Clause sgd:interaction="sgd:legal:check">
                                    <title>Informativa ai sensi del Reg. (UE) 679/2016 "RGPD"</title>
                                    <p>Lorem ipsum dolor sit amet [...]</p>
                                    <sgd:choice isDefault="false">Ho letto</sgd:choice>
                            </sgd:Clause>
                    </sgd:Agreement>
                    <sgd:Agreement
                      sgd:agreementID="urn:uuid:UUID_privacypolicy"
                      sgd:agreementType="SGD:legal:privacypolicy"
                      xmlns:lang="it">
                            <sgd:Clause sgd:interaction="sgd:legal:consent">
                                    <title>Consenso al trattamento dei dati personali</title>
                                    <p>Lorem ipsum dolor sit amet, consectetur <em>elit</em> [...].</p>
                                    <p> [...] </p>
                                    <sgd:choice index="1" isDefault="false">Acconsento</sgd:choice>
                                    <sgd:choice index="2" isDefault="true"><em>Nego</em></sgd:choice>
                            </sgd:Clause>
                            <sgd:Clause sgd:interaction="sgd:legal:consent">
                                    <p>Excepteur sint [...] <ol>
                                            <li>Ut enim ad minim [...];</li>
                                            <li>Duis aute irure dolor [...].</li>
```

```
                                    </ol></p>
                                    <sgd:choice index="1" isDefault="false">Acconsento</sgd:choice>
                                    <sgd:choice index="2" isDefault="true">Non acconsento</sgd:choice>
                            </sgd:Clause>
                    </sgd:Agreement>
                    <sgd:Agreement
                      sgd:agreementID="urn:uuid:UUID_privacypolicy"
                      sgd:agreementType="sgd:legal:privacypolicy"
                      xmlns:lang="it">
                            <sgd:Clause SGD:interaction="sgd:legal:consent">
                                    <title>Consenso al trattamento dei dati personali</title>
                                    <p>Lorem ipsum [...].</p><p> [...] </p>
                                    <sgd:choice index="1" isDefault="false">I agree</sgd:choice>
                                    <sgd:choice index="2" isDefault="true">I do not agree</sgd:choice>
                            </sgd:Clause>
                            <sgd:Clause sgd:interaction="sgd:legal:consent">
                                    <p>Excepteur [...] <ol><li> [...] </li><li> [...] </li></ol></p>
                                    <sgd:choice index="1" isDefault="false"> [...] </sgd:choice>
                                    <sgd:choice index="2" isDefault="true"> [...] </sgd:choice>
                            </sgd:Clause>
                    </sgd:Agreement>
                    <sgd:Agreement
                      sgd:agreementID="urn:oid:[……].4342.3.43.424.23"
                      sgd:agreementType="sgd:legal:CP"
                      xmlns:lang="it"
                      Location="https://www.SPdiesempio.it/ca/CPS_IT.html"/>
                    <sgd:Agreement
                      sgd:agreementID="urn:oid:[……].4342.3.43.424.23"
                      sgd:agreementType="sgd:legal:CP"
                      xmlns:lang="en"
                      Location="https://www.SPdiesempio.it/ca/CPS_EN.html"/>
                    <sgd:Agreement
                      sgd:agreementID="urn:uuid:UUID_eidas-generic-policy"
                      sgd:agreementType="sgd:legal:policy"
                      xmlns:lang="it"
                      Location="https://www.SPdiesempio.it/legal/it/infoPolicy_eidasFull.html"/>
                    <sgd:Agreement
                      sgd:agreementID="urn:uuid:UUID_eidas-generic-policy"
                      sgd:agreementType="sgd:legal:policy"
                      xmlns:lang="en"
                      Location="https://www.SPdiesempio.it/legal/it/infoPolicy_eidasFull.html"/>
            </sgd:Agreements>
            <md:KeyDescriptor use="SGDsgdwebaccess"> [……] </md:KeyDescriptor>
            <md:KeyDescriptor use="sgd:policysealing"> [……] </md:KeyDescriptor>
    </md:Extensions>
    <md:SPSSODescriptor
      AuthnRequestsSigned="true"
      WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:Extensions>
                    <mdui:UIInfo>
                            <mdui:DisplayName xml:lang="it">ISPE - servizi delegabili</mdui:DisplayName>
                            <mdui:Description xml:lang="it"> [……] </mdui:Description>
                            <mdui:Keywords xml:lang="it"> [……] </mdui:Keywords>
                            <mdui:Logo height="1920" width="1080">
                                    https://www.SPdiesempio.it/SP-delegate-logo.png
```

```
                        </mdui:Logo>
                </mdui:UIInfo>
        </md:Extensions>
        <md:KeyDescriptor use="signing">  [……]  </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">  [……]  </md:KeyDescriptor>
        <md:SingleLogoutService Binding="[……]:SOAP" Location="[……]"/>
        <md:SingleLogoutService Binding="[……]:HTTP-POST" Location="[……]"/>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
        <md:AssertionConsumerService Binding="[……]:bindings:HTTP-POST" Location="[……]"/>
        <md:AssertionConsumerService  Binding="[……]:bindings:HTTP-Redirect" Location="[……]"/>
        <md:AttributeConsumingService index="1">
                <md:ServiceName xml:lang="">urn:uuid:UID_del.01</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Servizi anagrafici</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Anagraphics</md:ServiceDescription>
                <md:RequestedAttribute Name="fiscalNumber" FriendlyName="[……]" NameFormat="[……]"/>
                <md:RequestedAttribute Name="delegatorName" [……] />
                <md:RequestedAttribute Name="delegatorFamilyName" [……] />
                <md:RequestedAttribute Name="delegatorFiscalNumber" [……] />
                <md:RequestedAttribute Name="delegationCreationTime" [……] NameFormat="xsd:dateTime"/>
        </md:AttributeConsumingService>
        <md:AttributeConsumingService index="2">
                <md:ServiceName xml:lang="">urn:uuid:UUID_del.02</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Certificati anagrafici</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Anagraphic certificates</md:ServiceDescription>
                <md:RequestedAttribute Name="fiscalNumber" [……] />
                <md:RequestedAttribute Name="delegatorName" [……] />
                <md:RequestedAttribute Name="delegatorFamilyName" [……] />
                <md:RequestedAttribute Name="delegatorFiscalNumber" [……] />
                <md:RequestedAttribute Name="delegatorMobilePhone" [……] />
                <md:RequestedAttribute Name="delegatorEmail" [……] />
                <md:RequestedAttribute Name="delegationCreationTime" [……] />
                <md:RequestedAttribute Name="soft:https://www.SPdiesempio.it?documentId" [……] />
                <md:RequestedAttribute Name="soft:https://www.SPdiesempio.it?bookingTime" [……] />
        </md:AttributeConsumingService>
        <md:AttributeConsumingService index="40">
                <md:ServiceName xml:lang="">urn:uuid:UUID_del.40</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Identificazione delegato</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Delegate person Id</md:ServiceDescription>
                <md:RequestedAttribute Name="fiscalNumber" [……] />
                <md:RequestedAttribute Name="delegatorFiscalNumber" [……] />
                <md:RequestedAttribute Name="delegationCreationTime" [……] />
        </md:AttributeConsumingService>
        <md:AttributeConsumingService index="100">
                <md:ServiceName xml:lang="">urn:uuid:UUID_del.100</md:ServiceName>
                [……]
        </md:AttributeConsumingService>
        <md:AttributeConsumingService index="101">
                <md:ServiceName xml:lang="">urn:uuid:UUID_del.101</md:ServiceName>
                [……]
        </md:AttributeConsumingService>
</md:SPSSODescriptor>
<md:Organization>
        <md:OrganizationName xml:lang="it">Istituto Service Provider di Esempio</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">ISPE</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">https://www.SPdiesempio.it/it-IT/</md:OrganizationURL>
</md:Organization>
```

```
  <md:ContactPerson contactType="technical other" spid:entityType="spid:aggregator">
          <md:Extensions>
                  <spid:VATNumber>IT01234567890</spid:VATNumber>
                  <spid:FiscalCode>9753108642</spid:FiscalCode>
                  <cie:Private/>
                  <spid:PublicServicesFullAggregator/>
                  <cie:NACE2Code>codiceATECO_aggregatore</cie:NACE2Code>
                  <cie:Country>IT</cie:Country>
                  <cie:Municipality>codiceISTAT_aggregatore</cie:Municipality>
          </md:Extensions>
          <md:Company>Partner Tecnologico per Soluzioni di Identità Federata s.r.l.</md:Company>
          <md:EmailAddress>info.deleghe@partnertecnologico.com</md:EmailAddress>
          <md:TelephoneNumber>+390123456789</md:TelephoneNumber>
  </md:ContactPerson>
  <md:ContactPerson contactType="other" spid:entityType="spid:aggregated">
          <md:Extensions>
                  <spid:IPACode>codiceIPA_soggetto</spid:IPACode>
                  <spid:FiscalCode>2468013579</spid:FiscalCode>
                  <cie:Public/>
                  <spid:Public/>
                  <cie:IPACategory>categoriaIPA_SP</cie:IPACategory>
                  <cie:Country>IT</cie:Country>
                  <cie:Province>sigla_provincia_SP</cie:Province>
                  <cie:Municipality>codiceISTAT_comune_SP</cie:Municipality>
          </md:Extensions>
          <md:Company>Istituto Service Provider di Esempio</md:Company>
          <md:EmailAddress>info@spesempio.gov.it</md:EmailAddress>
          <md:TelephoneNumber>+390011223344</md:TelephoneNumber>
  </md:ContactPerson>
  <md:AdditionalMetadataLocation>
          https://registry.spid.gov.it/metadata/sp/codiceIPA_soggetto__IT01234567890.xml
  </md:AdditionalMetadataLocation>
</md:EntityDescriptor>
```

6.3. Struttura del metadata del SGD

Il SGD è un gestore di attributi qualificati (qAA), conforme con le Linee Guida di cui questo allegato tecnico è parte integrante. Pertanto, nell'ambito SAML, esiste un meccanismo di doppia federazione "tecnica": quella che comprende gli SP e gli IDP di tutti gli schemi di identificazione elettronica nazionale (della quale il SGD fa parte nel ruolo tecnico di SP) e quella denominata *sistema delle deleghe digitali*, che comprende i SP e il SGD (della quale quest'ultimo fa parte nel ruolo tecnico di IDP unico). Le due federazioni fanno parte dell'unico *ecosistema* delle identità digitali nazionali, che comprende tutti gli SP, tutti gli IDP e tutte le AA – e nel quale il SGD svolge, appunto, il ruolo di un qAA. Le due federazioni sono tecnicamente legate fra di loro mediante il meccanismo di "delega SAML" o '*proxying*' come definito in [**samlDel**] e [**samlCore**] e il legame virtuale tra questi due ruoli svolti dal SGD è istituito, a livello logico, presentando il SGD ad entrambe le federazioni mediante un *unico* metadata SAML.

Il metadata del SGD è perciò conforme con quanto previsto – per i rispettivi ruoli – nei regolamenti degli schemi di identificazione elettronica nazionale e ha inoltre le seguenti caratteristiche:

1. Almeno *due* certificati elettronici, ciascuno contenuto – come da standard [**samlMeta**] – all'interno di un elemento `<md:KeyDescriptor>` nei rispettivi elementi di tipo `RoleDescriptor`; afferenti a chiavi crittografiche

utilizzate una per sigillare elettronicamente e l'altra per la cifratura *opzionale* delle evidenze informatiche scambiate con le altre entità tecniche.

2. È presente un solo elemento `<md:IDPSSODescriptor>`, conforme con le specifiche del metadata di un IDP secondo le normative vigenti degli schemi di identificazione elettronica nazionale e, in più, contenente:
   2.1. L'attributo `WantAssertionsSigned`, valorizzato con `true`.
   2.2. L'attributo `protocolSupportEnumeration`, valorizzato con `urn:oasis:names:tc:SAML:2.0:protocol`.
   2.3. Nell'elemento `<md:Extensions>` PUÒ essere presente un elemento `<sgd:GlobalServiceClasses>`, valorizzato come l'elemento `<sgd:ServiceClasses>` del metadata-deleghe (cfr. §6.2 punto 5.3 e seguenti), relativamente alla definizione di classi di servizi delegabili per deleghe "globali" (cfr. §5.3), con le seguenti *differenze*:
      2.3.1. gli elementi `<sgd:ServiceClass>` non ammettono né gli attributi `sgd:nonDelegateAtCSIndex`, né l'elemento `<sgd:EndServices>`;
      2.3.2. gli eventuali 'accordi' definiti sostituiscono interamente gli accordi efficaci specificati nel metadata-deleghe dell'SP che ammette la medesima classe di servizi delegabili.
   2.4. Tanti elementi `<md:SingleLogoutService>` *almeno* per ciascun *binding* previsto dagli schemi di identificazione elettronica nazionali – e almeno per l'HTTP POST.
   2.5. Almeno i seguenti elementi `<md:Attribute>`:
      2.5.1. uno per ciascun attributo identificativo *minimo* del **delegato** persona fisica — come da successivo punto 3.5.1 e mantenendo il nome degli attributi invariati;
      2.5.2. uno per ciascun attributo-delega del **delegante** persona fisica — derivati dagli attributi identificativi *completi* del delegato persona fisica, aggiungendo al nome il prefisso `delegator` (e mantenendo il *camel-casing*) – si veda il successivo punto 3.5.2 come riferimento;[22]
      2.5.3. uno o più attributi specifici della delega
      2.5.4. allo scopo di impedire le deleghe ricorsive, il SGD non tratta mai attributi con il nome che comincia con una desinenza `delegator` *multipla* (ad esempio: `delegatordelegator*`)
3. È presente un solo elemento `<md:SPSSODescriptor>`, conforme con le specifiche del metadata di un SP secondo le normative vigenti degli schemi di identificazione elettronica nazionale e, in più, contenente:
   3.1. Gli attributi `AuthnRequestsSigned` e `WantAssertionsSigned`, entrambe valorizzati con `true`.
   3.2. L'attributo `protocolSupportEnumeration`, valorizzato con `urn:oasis:names:tc:SAML:2.0protocol`.
   3.3. L'elemento `<md:SingleLogoutService>`, contenente le seguenti estensioni:
      3.3.1. `<sgd:SPScope>` (*facoltativo*) — Valorizzato con l'ambito della classe di servizio delegabile (cfr. §5.3).
   3.4. Tanti elementi `<md:SingleLogoutService>` e `<md:AssertionConsumerService>` *almeno* per ciascun *binding* previsto dagli schemi di identificazione elettronica nazionali – e almeno per l'HTTP POST.
   3.5. Almeno i seguenti elementi `<md:AttributeConsumingService>`:
      3.5.1. un AtCS dedicato agli attributi identificativi *minimi* del **delegato** persona fisica (con indice 0) — `fiscalNumber`;
      3.5.2. un AtCS dedicato agli attributi identificativi *completi* del **delegato** persona fisica (indice 1) — `name`, `familyName`, `gender`, `placeOfBirth`, `countryOfBirth`, `dateOfBirth`, `address`,

[22] Ad esempio, l'attributo-delega del delegante `delegatorFamilyName` è derivato dall'attributo identificativo del delegato `familyName`.

`mobilePhone`, `email`, `fiscalNumber`, `ivaCode`, `digitalAddress`, `idCard`, `expirationDate`, `domicileAddress`, `domicilePostalCode`, `domicileMunicipality`, `domicileProvince` e infine `domicileNation`;

3.5.3. un AtCS dedicato agli attributi identificativi *minimi* del **delegato** persona giuridica (indice 2) — `companyFiscalNumber` e `digitalAddress`;

3.5.4. un AtCS dedicato agli attributi identificativi *completi* del **delegato** persona giuridica (indice 3) — `companyName`, `ivaCode`, `companyFiscalNumber`, `digitalAddress`, `registeredOffice`;

3.5.5. un AtCS dedicato agli attributi identificativi *completi* del **delegato** persona fisica professionista (indice 4) — unione di tutti gli attributi identificativi *completi* per la persona fisica E la persona giuridica;

3.5.6. quattro AtCS dedicati (con indici da 100 a 103) agli attributi identificativi previsti da [**eIDAS**] per la persona fisica (minimi e completi) e per la persona giuridica (minimi e completi).

4. Nell'elemento `<md:Extensions>` *sia* dentro `<IDPSSODescriptor>` *che* dentro `<SPSSODescriptor>` è presente l'elemento `<mdui:UIInfo>`, valorizzato secondo quanto previsto in [**samlUI**] e contenente *almeno un* logo del SGD, che soddisfa le regole tecniche di cui al §6.2, punti 5.7 e seguenti.

Segue un esempio di metadata del SGD su cui sono basati anche gli esempi nei §§4 e 6. Incrociando il metadata con il metadata-delega di un SP di esempio (cfr. §6.2) è possibile identificare le classi di servizio associabili a deleghe globali, nonché il nome di tutti gli attributi-delega (non specifici) che il SGD è in grado di gestire – inclusi gli attributi che veicolano caratteristiche obbligatorie e alcune caratteristiche facoltative delle deleghe digitali (tipologia, rinnovabilità).

```
<md:EntityDescriptor
 entityID="https://deleghedigitali.gov.it"
 validUntil="2031-01-01T00:00:00Z"
 ID="md-2a94899a-b906-4d48-a811-52b47ac09af8"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:profiles"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
 xmlns:mdsess="urn:oasis:names:tc:SAML:2.0:profiles:session:metadata"
 xmlns:sgd="https://deleghedigitali.gov.it/saml-extensions"
 xmlns:cie="https://www.cartaidentita.interno.gov.it/saml-extensions"
 xmlns:spid="https://spid.gov.it/saml-extensions"
 xmlns:eidas="http://eidas.europa.eu/attributes"
 xmlns:lp="http://eidas.europa.eu/attributes/legalperson/"
 xmlns:np="http://eidas.europa.eu/attributes/naturalperson/" >
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ds:Signature>  [……]  </ds:Signature>
  <md:IDPSSODescriptor
    WantAuthnRequestsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <md:Extensions>
                  <mdui:UIInfo>
                          <mdui:Description xml:lang="it">  [……]  </mdui:Description>
                          <mdui:Description xml:lang="en">  [……]  </mdui:Description>
                          <mdui:Keywords xml:lang="it">  [……]  </mdui:Keywords>
                          <mdui:Keywords xml:lang="en">  [……]  </mdui:Keywords>
                          <mdui:Logo height="2048" width="1556">
                                  https://deleghedigitali.gov.it/img/SGD_logo.png
                          </mdui:Logo>
```

```
            </mdui:UIInfo>
        </md:Extensions>
        <md:KeyDescriptor use="signing"> […] </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption"> […] </md:KeyDescriptor>
        <md:SingleLogoutService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
          Location="https://deleghedigitali.gov.it/saml-idp/slos/post"
          ResponseLocation="https://deleghe.ipzs.it/saml-idp/slor/post"/>
        <md:SingleLogoutService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
          Location="https://deleghedigitali.gov.it/saml-idp/slos/redirect"
          ResponseLocation="https://deleghedigitali.gov.it/saml-idp/slor/redirect"/>
        <md:SingleLogoutService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-SOAP"
          Location="https://deleghedigitali.gov.it/saml-idp/slos/soap"
          ResponseLocation="https://deleghe.ipzs.it/saml-idp/slor/soap"/>
        <md:SingleSignOnService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
          Location="https://deleghedigitali.gov.it/saml-idp/slos/post"/>
        <md:SingleSignOnService
          Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
          Location="https://deleghedigitali.gov.it/saml-idp/slos/post"/>
        <md:Attribute
          Name="fiscalNumber"
          FriendlyName="codice fiscale del delegato"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
        <md:Attribute Name="email" FriendlyName="indirizzo email del delegato" […] />
        <md:Attribute Name="delegatorName" FriendlyName="nome del delegante" […] />
        <md:Attribute Name="delegatorFamilyName" […] />
        <md:Attribute Name="delegatorGender" […] />
        <md:Attribute Name="delegatorPlaceOfBirth" […] />
        <md:Attribute Name="delegatorCountyOfBirth" […] />
        <md:Attribute Name="delegatorDateOfBirth" […] />
        <md:Attribute Name="delegatorAddress" […] />
        <md:Attribute Name="delegatorMobilePhone" […] />
        <md:Attribute Name="delegatorEmail" […] />
        <md:Attribute
          Name="delegatorFiscalNumber"
          FriendlyName="codice fiscale del delegante"
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
        <md:Attribute Name="delegatorIvaCode" […] />
        <md:Attribute Name="delegatorDigitalAddress" […] />
        <md:Attribute Name="delegatorIdCard" […] />
        <md:Attribute Name="delegatorExpirationDate" […] />
        <md:Attribute Name="delegatorCompanyName" […] />
        <md:Attribute Name="delegatorRegisteredOffice" […] />
        <md:Attribute Name="delegatorCompanyFiscalNumber" […] />
        <md:Attribute Name="delegatorSPIDCode" FriendlyName" […] />
        <md:Attribute Name="delegatorDomicileStreetAddress" […] />
        <md:Attribute Name="delegatorDomicilePostalCode" […] />
        <md:Attribute Name="delegatorDomicileMunicipality" […] />
        <md:Attribute Name="delegatorDomicileProvince" […] />
        <md:Attribute Name="delegatorDomicileNation" […] />
        <md:Attribute Name="delegationCreationTime" […] />
        <md:Attribute Name="delegationExpirationTime" " FriendlyName="scadenza della delega" […] />
        <md:Attribute Name="delegationRenewalTime" […] />
```

```
        <md:Attribute Name="delegationType" FriendlyName="tipologia della delega" [……] />
        <md:Attribute Name="delegationNumUses" [……] />
        <md:Attribute Name="delegationMaxUses" [……] />
        <md:Attribute Name="delegationCreationMode" [……] />
</md:IDPSSODescriptor>
<md:SPSSODescriptor
  AuthnRequestsSigned="true"
  WantAssertionsSigned="true"
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:Extensions>
                <mdui:UIInfo>
                        <mdui:Description xml:lang="it">  [……]  </mdui:Description>
                        <mdui:Description xml:lang="en">  [……]  </mdui:Description>
                        <mdui:Keywords xml:lang="it">  [……]  </mdui:Keywords>
                        <mdui:Keywords xml:lang="en">  [……]  </mdui:Keywords>
                        <mdui:Logo height="2048" width="1556">
                                https://deleghedigitali.gov.it/img/SGD_logo.png
                        </mdui:Logo>
                </mdui:UIInfo>
                <sgd:GlobalServiceClasses>
                        <sgd:ServiceClass
                          id="urn:uuid:UUID_del.01"
                          SGD:hierarchy="urn:oid:[……].15.44.926">
                                <md:ServiceDescription lang="it">Anagrafici</md:ServiceDescription>
                                <md:ServiceDescription lang="en">Anagraphics</md:ServiceDescription>
                                <sgd:AgreementRef>urn:uuid[…]globalInfoPolicy</sgd:AgreementRef>
                        </sgd:ServiceClass>
                        <sgd:Agreements>
                                <sgd:Agreement
                                  SGD:agreementID="urn:uuid:globalInfoPolicy"
                                  SGD:agreementType="SGD:legal:infopolicy"
                                  xmlns:lang="it">
                                        <sgd:Clause SGD:interaction="SGD:legal:check">
                                                <title>InfoPolicy pursuant to GDPR</title>
                                                <p> [...] </p>
                                                <sgd:choice isDefault="false"/>
                                        </sgd:Clause>
                                </sgd:Agreement>
                                <sgd:Agreement […] xmlns:lang="en">  [……]  </sgd:Agreement>
                        </sgd:Agreements>
                </sgd:GlobalServiceClasses>
        </md:Extensions>
        <md:KeyDescriptor use="signing">  [……]  </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">  [……]  </md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" [……] />
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" [……] />
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" [……] />
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" [……] />
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"[…]/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" [……] />
        <md:AttributeConsumingService index="0" isDefault="true">
                <md:ServiceName xml:lang="">urn:uuid:UUID0</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Set minimo persona fisica</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Natural person minimum set<md:ServiceDescription>
                <md:RequestedAttribute Name="fiscalNumber" FriendlyName="codice fiscale" […] />
        </md:AttributeConsumingService>
```

```
        [……]
        <md:AttributeConsumingService index="100" isDefault="false">
                <md:ServiceName xml:lang="">urn:uuid:UUID_100</md:ServiceName>
                <md:ServiceDescription xml:lang="it">Set minimo attributi eIDAS</md:ServiceDescription>
                <md:ServiceDescription xml:lang="en">Minimum eIDAS data set<md:ServiceDescription>
                <md:RequestedAttribute Name="eidas:/naturalperson/GivenName" [……] />
                <md:RequestedAttribute Name="eidas:/naturalperson/FamilyName" [……] />
                <md:RequestedAttribute Name="eidas:/naturalperson/DateOfBirth" [……] />
                <md:RequestedAttribute Name="eidas:/naturalperson/PersonIdentifier" [……] />
        </md:AttributeConsumingService>
        [……]
</md:SPSSODescriptor>
<md:Organization>
        <md:OrganizationName xml:lang="it">
                        Sistema di gestione delle deleghe digitali
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">SGD</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">https://deleghedigitali.gov.it/it</md:OrganizationURL>
        <md:OrganizationName xml:lang="en">Digital Delegates Management System</md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="en">SGD</md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="en">https://deleghedigitali.gov.it/en</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="other administrative">
        <md:Extensions>
                <spid:FiscalCode> [……] </spid:FiscalCode>
                [……]
                <cie:Country>IT</cie:Country>
                <cie:Province> [……] </cie:Province>
                <cie:Municipality> [……] </cie:Municipality>
        </md:Extensions>
        <md:Company>Sistema di gestione delle deleghe digitali</md:Company>
        <md:EmailAddress>email@deleghedigitali.gov.it</md:EmailAddress>
        <md:TelephoneNumber> [……] </md:TelephoneNumber>
</md:ContactPerson>
<md:AdditionalMetadataLocation>
        https://registry.spid.gov.it/metadata/sp/[……].xml
</md:AdditionalMetadataLocation>
</md:EntityDescriptor>
```

7. Messaggi di errore

Il mancato utilizzo di una delega digitale a causa di un errore (imputabile ad un qualunque soggetto tecnico della federazione) o a un diniego del SGD nel fornirla, è considerata un'**anomalia** al pari di quelle definite dagli schemi di identificazione elettronica nazionali; pertanto, viene gestita ottemperando alle condizioni di anomalia già previste per l'utilizzo delle identità digitali.

Le anomalie relative alle deleghe digitali DEVONO essere sempre presentate all'utente in maniera *accessibile* e preservando la UX offerta durante la normale navigazione dello stesso presso il servizio di ciascun ente federato. In particolare, presso il servizio del SP, le anomalie sono presentate con un'interfaccia grafica (*UI*) che consenta il riconoscimento del SP (per mantenere la UX in base a quanto sopra richiesto) e dalla quale sia possibile tornare indietro nella navigazione. Presentando le anomalie all'utente, POSSONO essere incluse *anche* informazioni di carattere tecnico, valutando

attentamente i rischi di sicurezza dovuti all'esposizione di tali informazioni.

I messaggi di errori con le relative codifiche di cui al presente Capitolo fanno riferimento all'esito dell'`<AuthnRequest>`-**2** e riguardano le seguenti categorie:

- anomalie di sistema;
- anomalie di protocollo;
- anomalie utente.

Laddove possibile, gli errori sono veicolati, all'interno della `<AuthnResponse>`-**2**, nell'elemento `<StatusCode>` figlio dell'elemento `<Status>`, sotto forma di un SAML Status Code. La notifica dell'errore può essere veicolata anche mediante il sottostante protocollo HTTP, a seconda del tipo di *binding* utilizzato per il trasporto dei messaggi. Nei seguenti sotto-capitoli sono riportate le tabelle, per ciascuna categoria di errori, con i SAML Status Code, i relativi HTTP Status Code (ove applicabili) e il codice numerico associato a ciascun errore.

7.1. Anomalie di sistema

Scenario di riferimento	*Binding*	SAML/HTTP Status Code	error code
Indisponibilità del sistema	HTTP POST	—	102
Errore di sistema	HTTP Redirect	HTTP 500	103

7.2. Anomalie di protocollo

Scenario di riferimento	SAML/HTTP Status Code	error code
Formato di *binding* non corretto	HTTP 403	104
Errata corrispondenza tra *binding* ed *entrypoint* HTTP	HTTP 403	105
Sigillo elettronico del SP assente o non valido	HTTP 403	106
Formato della richiesta non conforme alle specifiche SAML (o a quelle XML)	`urn:oasis:names:tc:SAML:2.0:status:Requester`	107
Parametro `Version` non presente, malformato o diverso da `2.0`	`urn:oasis:names:tc:SAML:2.0:status:VersionMismatch`	108
`<Issuer>` non presente, malformato o non corrispondente all'entità che sigilla l'evidenza	HTTP 403	109
`ID` (identificativo unico dell'evidenza) non presente, malformato o non conforme a	`urn:oasis:names:tc:SAML:2.0:status:Requester`	110

quanto atteso		
Contesto di autenticazione non presente, malformato, non riconosciuto o non conforme con quanto atteso (p.es. LoA insufficiente)	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext	111
`IssueInstant` non presente, malformato o non conforme con le tempistiche attese	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied	112
`Destination` non presente, malformata o non corrispondente all'entità attesa	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	113
Errata rappresentazione degli attributi `ForceAuthn` e/o `isPassive`	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive	114
`AssertionConsumerServiceIndex` o `<AssertionConsumerService>` non presente o non correttamente valorizzato	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	115
`Format` del `<NameIDPolicy>` non presente o non correttamente valorizzato	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	116
`AttributeConsumingServiceIndex` non presente o non correttamente valorizzato	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	117
Sigillo elettronico dell'IDP (nell'`<Evidence>`) assente o invalido	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	118
Autenticazione pregressa del delegato non valida: `<Assertion>` imbustata dentro `<Evidence>` assente o invalida	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	119
IDP non comunicato, comunicato erroneamente tramite elemento `<IDPList>` o non coincidente con l'IDP atteso	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAvailableIDP	120
Numero di re-indirizzamenti invalido (p.es. `ProxyCount` omesso o non valido)	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded	121
Sigillo elettronico dell'IDP (nell'`<Assertion>` imbustata dentro `<Evidence>`) assente o invalido	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	122
Impossibile riutilizzare la sessione di autenticazione pre-esistente (o nessuna sessione di autenticazione valida)	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	123

Uno o più attributi identificativi del delegato non inviati al SP durante la precedente sessione di autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	124
Uno o più attributi identificativi del delegante non inviati al SP durante la precedente sessione di autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal	125
Almeno una caratteristica della delega richiesta dal SP non presente nella delega digitale.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	126
Almeno una caratteristica della delega richiesta dal SP valorizzata in modo errato.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	127

7.3. Anomalie utente

Le anomalie utente DEVONO essere presentate, presso il servizio offerto *dal SP*, mediante un testo chiaramente visibile, identico o simile a quanto riportato nella colonna 'Scenario di riferimento' della seguente tabella. *Solo* nel caso i contenuti del SP siano presentati, in condizioni normali, già localizzati nella lingua dell'utente diversa dall'italiano, il suddetto testo DEVE essere tradotto anch'esso nella corrispondente lingua.

Salvo ove espressamente indicato

Scenario di riferimento	SAML/HTTP Status Code	error code
Time-out durante l'autenticazione del delegato	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	123
Il delegato nega il consenso all'invio della delega digital al SP in caso di sessione vigente	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	124
Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate)	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	125
Delegato privo di credenziali compatibili con il livello richiesto dal SP	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	126
Delegato privo di credenziali compatibili con il livello richiesto dal sistema di gestione delle deleghe digitali	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	127
Mancata corrispondenza del delegato attraverso la doppia autenticazione	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	128

Delegato con identità sospesa/revocata o con credenziali bloccate	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	
Processo di autenticazione annullato dal delegato	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	