Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

REGOLAMENTO

RECANTE LE MODALITÀ ATTUATIVE PER LA REALIZZAZIONE DELLO SPID

(articolo 4, comma 2, DPCM 24 ottobre 2014)

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale, e, in particolare, l'articolo 64 che prevede l'istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (di seguito: SPID);

Visto il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 che definisce le caratteristiche di SPID, nonché i tempi e le modalità di adozione dello stesso da parte delle pubbliche amministrazioni e delle imprese, e, in particolare, l'articolo 4, comma 2;

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

Visto il Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta ufficiale dell'Unione europea serie L 257 del 28 agosto 2014;

Sentito il Garante per la protezione dei dati personali;

l'Agenzia per l'Italia Digitale emana il seguente Regolamento.

CAPO I
Disposizioni generali

Art. 1
(Oggetto)

1. Ai fini della realizzazione di SPID, il presente regolamento individua le modalità attuative:

a) con cui i soggetti aderiscono al sistema, previo accreditamento e stipula di convenzioni;

b) di rilascio dell'identità digitale, previa verifica dell'identità del soggetto richiedente e rilascio delle credenziali;

c) di gestione del ciclo di vita dell'identità digitale, ivi compresa la sospensione e la revoca;

d) di autenticazione del soggetto che richiede il servizio;

e) di monitoraggio da parte dell'Agid.

Art. 2
(Il sistema pubblico per la gestione dell'identità digitale)

SPID prevede diversi soggetti:

a) l'utente, che potrà disporre di uno o più identità digitali, che contengono alcune informazioni identificative obbligatorie, come il codice fiscale, il nome, il cognome, il luogo di nascita, la data di nascita e il sesso;

b) il gestore dell'identità digitale. Si tratta di un soggetto, che dovrà essere accreditato dall'Agenzia per l'Italia Digitale e che avrà il ruolo di creare e gestire le identità digitali;

c) il gestore di attributi qualificati che, in base alle norme vigenti, può certificare attributi qualificati, come il possesso di un titolo di studio, l'appartenenza ad un ordine professionale;

d) il fornitore di Servizi – soggetto pubblico o privato – che eroga servizi on-line, previo riconoscimento dell'utente da parte del gestore dell'identità digitale.

Il Sistema SPID si conforma al principio di necessità nel trattamento dei dati di cui all'articolo 3 del decreto legislativo 30 giugno 2003, n. 196, in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. I trattamenti dei dati personali in applicazione del presente regolamento sono effettuati esclusivamente per le finalità previste dall'articolo 64 del CAD e dall'articolo 2, comma2, del DPCM 24 ottobre 2014 e con le modalità individuate dal presente regolamento, nel rispetto delle garanzie previste dal medesimo decreto legislativo n. 196 del 2003.

Il sistema SPID è basato su tre livelli di sicurezza di autenticazione informatica.

Il processo di autenticazione informatica è diretto alla verifica dell'identità digitale associata a un soggetto ai fini della erogazione di un servizio fornito in rete. A tale verifica di identità è associato un livello di sicurezza o di garanzia (*level of assurance - LoA*) progressivamente crescente in termini di sicurezza.

Il livello di sicurezza è il risultato dell'intero procedimento che sottende all'attività di autenticazione. Tale processo va dalla preliminare associazione tra un soggetto e un'identità digitale che lo rappresenta in rete, con annessa attribuzione di credenziali in grado di comprovare tale associazione, ai meccanismi che realizzano il protocollo di autenticazione al momento della richiesta di un servizio in rete.

In SPID sono definiti tre livelli di sicurezza, corrispondenti ad altrettanti livelli specificati nella ISO-IEC 29115, rispetto al rischio di uso abusivo o alterazione di identità. In particolare:

a) livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115): è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche , norme e procedure dello strumento di identificazione elettronica tali da ridurre il rischio di uso abusivo o di alterazione di identità.~~.~~ A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato applicabile nei casi in cui il danno causato, da un utilizzo indebito dell'identità digitale, ha un basso impatto per le attività del cittadino/impresa/amministrazione;

b) livello 2 (corrispondente al LoA3 dell'ISO-IEC 29115): è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche, norme e procedure dello strumento di identificazione elettronica tali da ridurre significativamente il rischio di uso abusivo o di alterazione di identità . A tale livello è associato un rischio notevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell' identità digitale può provocare un danno consistente;

c) livello 3 (corrispondente al LoA4 dell'ISO-IEC 29115): è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche , norme e procedure dello strumento di identificazione elettronica il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità e garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell' Allegato II del Regolamento 910/2014; questo è il livello di garanzia più elevato e da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell' identità digitale può provocare un danno serio e grave.

Ai sensi dell'articolo 6, commi 4 e 5, del DPCM 24 ottobre 2014 (di seguito: "DPCM"), i fornitori di servizi scelgono il livello di sicurezza SPID necessario per accedere ai propri servizi e non possono discriminare l'accesso ai propri servizi sulla base del gestore di identità che l'ha fornita.

Nell'Appendice A è riportata, a titolo esemplificativo, una metodologia da adottare allo scopo.

Art. 3
(Adesione a SPID)

Possono aderire a SPID:

a) i gestori dell'identità digitale e i gestori di attributi qualificati, previo accreditamento e stipula di apposite convenzioni con Agid secondo le modalità definite con regolamento adottato ai sensi dell'articolo 4, comma 3, del DPCM 24 ottobre 2014; i gestori dell'identità digitale sono tenuti inoltre ad aderire alle apposite convenzioni che l'Agenzia stipula con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità;

b) i fornitori dei servizi stipulando una convenzione con l'Agenzia. Ai fini della stipula, i fornitori dei servizi indicano all'Agenzia i servizi erogati e, per ciascuno di questi servizi, motivano le scelte in relazione ai livelli di sicurezza adottati e alla necessità di informazioni richieste relative ad attributi identificativi, non identificativi e qualificati. Per i servizi qualificati, i predetti soggetti motivano le circostanze per cui le informazioni sono necessarie e non eccedenti per l'erogazione dei singoli servizi.

Aderiscono a SPID le pubbliche amministrazioni di cui all'articolo 2, comma 2, del CAD, entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale.

L'Agenzia vigila sull'operato dei soggetti che partecipano a SPID.

Art. 4
(Rilascio e gestione delle identità digitali SPID)

Il rilascio dell'identità digitale SPID e la gestione del ciclo di vita della stessa da parte dei gestori dell'identità digitale sono così articolati:

1) Il rilascio delle identità digitali si articola nei seguenti processi:

a) richiesta dell'identità digitale e identificazione del richiedente;
b) esame e verifica dell'identità del richiedente;
c) conservazione e registrazione dei documenti;
d) emissione dell'identità digitale;
e) creazione e consegna delle credenziali.

2) La gestione del ciclo di vita dell'identità digitale si articola nei seguenti processi:

a) gestione degli attributi;
b) sospensione e revoca dell'identità;
c) gestione del ciclo di vita delle credenziali che si articola in:
    1) conservazione;

2) sospensione e revoca;
3) rinnovo e sostituzione.

CAPO II
Rilascio delle identità digitali

Art. 5
(Richiesta dell'identità digitale)

Le identità digitali sono rilasciate dal gestore dell'identità digitale, su richiesta di un soggetto interessato secondo quanto previsto dall'art. 7 del DPCM mediante presentazione di un modulo di *richiesta di adesione* che contiene tutte le informazioni necessarie per l'identificazione del soggetto richiedente.

Il modulo di *richiesta di adesione* contiene:

a) i dati identificativi del richiedente, che costituiscono gli attributi identificativi dell'identità digitale;

b) le informazioni che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali e il richiedente dell' identità digitale, che costituiscono gli attributi secondari dell'identità digitale;

Per le persone fisiche sono obbligatorie le seguenti informazioni:

a) cognome e nome;
b) sesso, data e luogo di nascita;
c) codice fiscale;
d) estremi di un valido documento di identità
e) gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM .

Per le persone giuridiche sono obbligatorie le seguenti informazioni:

a) denominazione/ragione sociale;

b) codice fiscale o P.IVA (se uguale al codice fiscale);

c) sede legale;

d) visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale);

e) estremi del documento di identità utilizzato dal rappresentante legale;

f) gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM .

Per gli attributi secondari, sono forniti almeno un indirizzo di posta elettronica e un recapito di telefonia mobile, entrambi verificati dal gestore di identità digitale nel corso del processo di identificazione, inviando

un messaggio di posta all'indirizzo dichiarato, contenente una URL per la verifica e un SMS al numero di cellulare con un codice numerico di controllo che deve essere riportato in risposta. Inoltre, per quanto riguarda l'indirizzo di posta elettronica, i gestori dovranno accertarsi, che lo stesso sia un indirizzo corrispondente a una reale casella di posta.

Nel modulo, il soggetto richiedente sottoscrive l'apposita dichiarazione con cui si assume la responsabilità, ai sensi dell'articolo 76 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, della veridicità delle informazioni fornite.

Art. 6
(Identificazione del soggetto richiedente)

Al ricevimento della richiesta, il gestore dell'identità digitale procede all'identificazione del soggetto richiedente, che consiste nell'accertamento delle informazioni sufficienti a identificare il soggetto richiedente sulla base di documenti forniti dallo stesso. Tale processo è effettuato da personale qualificato e opportunamente formato.

Le modalità di consegna della richiesta e il supporto utilizzato (cartaceo o digitale) dipendono da quale modalità, tra quelle previste dall'art. 7 del DPCM il gestore dell'identità digitale adotta per operare il processo di identificazione.

Il gestore dell'identità digitale, per una corretta e sicura attuazione del processo,

a) fornisce l'informativa sul trattamento dei dati (articolo 13 del D.lgs. 196 del 2003);

b) si assicura che il richiedente sia consapevole dei termini e delle condizioni associati all'utilizzo del servizio di identità digitale;

c) si assicura che il richiedente sia consapevole delle raccomandazioni e delle precauzioni da adottare per l'uso delle identità digitale e propone l'attivazione del servizio di segnalazione di cui all'art. 18;

d) acquisisce i dati necessari alla dimostrazione di identità.

Art. 7
(Identificazione a vista del soggetto richiedente)

Nel caso di identificazione a vista del soggetto richiedente presso le sedi allo scopo individuatesi procede con l'acquisizione del modulo di *richiesta di adesione* in formato cartaceo compilato e sottoscritto dall'utente e con l'esibizione di un valido documento di identità.

Nel caso in cui il soggetto richiedente sia una persona giuridica, deve essere fornita la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che sottoscrive e presenta l'istanza. Il rappresentante legale dovrà a sua volta essere identificato tramite un valido documento d'identità.

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

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

Art. 8
(Identificazione a vista da remoto)

L'identificazione a vista della persona fisica richiedente un'identità SPID da parte del gestore dell'identità può essere effettuata dai gestori dell'identità digitale anche in digitale da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196.

Il gestore deve implementare un sistema che garantisca, preliminarmente all'instaurazione della sessione audio/video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente. Inoltre deve garantire l'utilizzo di applicativi orientati all'usabilità e all'accessibilità da parte dell'utente.

L'identificazione da remoto deve avvenire in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte dell'utente nel rispetto delle seguenti condizioni:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;

b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi.

c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

Il gestore è responsabile della valutazione in merito alla sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del soggetto.

L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso, rilasciato da un'Amministrazione dello Stato e verifica il codice fiscale tramite la tessera sanitaria in corso di validità.

L’operatore che effettua l’identificazione può escludere l’ammissibilità della sessione audio/video per qualunque ragione, inclusa l’eventuale inadeguatezza del documento presentato dal richiedente (ad esempio perché logoro o carente delle caratteristiche elencate).

La sessione audio/video è interamente registrata e conservata per venti anni decorrenti dalla scadenza o dalla revoca dell’identità digitale con modalità crittografiche atte a garantirne l’accesso esclusivamente dietro richiesta dell’autorità giudiziaria, dell’Agenzia nel corso delle attività di vigilanza, dell’utente e dell’autorità giudiziaria in caso di disconoscimento della stessa.

Nel caso l'identificazione a vista da remoto sia solo una delle modalità predisposte per la verifica dell'identità del richiedente, il gestore dell’identità deve richiedere il consenso al trattamento dei dati personali contenuti nelle riprese audio-video, specificando tale aspetto nell’informativa da rendere all'interessato ai sensi dell'articolo 13 del Codice. Nel caso in cui l'identificazione a vista da remoto sia l’unica modalità disponibile per la verifica dell'identità del richiedente, ciò deve essere messo in specifica evidenza, oltre che nelle condizioni e termini del contratto, anche nell’informativa da rendere all'interessato ai sensi dell'articolo 13 del Codice. (punto b)

La sessione audio/video deve essere condotta seguendo una procedura scritta e formalizzate dal gestore che prevede almeno le seguenti attività:

a) l’acquisizione del consenso, **qualora necessario**, alla videoregistrazione e alla sua conservazione per 20 anni come previsto dalla normativa vigente in materia. L’operatore informa che la videoregistrazione sarà conservata in modalità protetta;

b) l’operatore dichiara i propri dati identificativi;

c) il soggetto conferma le proprie generalità;

d) il soggetto conferma la data e l’ora della registrazione;

e) il soggetto conferma di volersi dotare di un’identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;

f) il soggetto conferma il proprio numero di telefonia mobile e l’indirizzo mail;

g) l’operatore invia un sms che il soggetto richiedente è tenuto a esporre al dispositivo di ripresa e una mail all’indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;

h) l’operatore chiede e ottiene conferma dal soggetto circa la conoscenza delle tipologie di credenziali di cui disporrà per l’accesso ai servizi in rete;

i) l’operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le

informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);

j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;

k) il soggetto conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;

l) l'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;

m) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati in base all'articolo 7, commi 8 e 9 del DPCM.

Per la conservazione dei dati di registrazione si applica quanto stabilito all'articolo 13.

Art. 9
(Identificazione informatica tramite documenti digitali di identità)

Nel caso di identificazione informatica tramite documenti digitali di identità di cui all'art. 64 del Dlgs. n.82/2005, l'identificazione avviene tramite verifica dei documenti digitali che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi.

Il gestore dell'identità digitale deve garantire che la richiesta di rilascio dell'identità digitale sia riconducibile all'utilizzo degli strumenti di cui al presente articolo.

Art. 10
(Identificazione informatica tramite altre identità SPID)

Nel caso di identificazione informatica tramite altre identità SPID si procede con l' acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto elettronicamente (ad esempio con firme qualificate valide solo per la sessione in corso o per un periodo limitato).L'identificazione avviene attraverso l'accesso, utilizzando credenziali SPID di livello di sicurezza pari o superiore a quella oggetto della richiesta, a un servizio reso disponibile allo scopo da parte dal gestore dell'identità digitale. Questa modalità di identificazione è applicabile quando la richiesta di una nuova identità è effettuata presso lo stesso gestore che ha rilasciato l'identità SPID utilizzata per la richiesta.

Art. 11
(Identificazione informatica tramite firma elettronica qualificata o firma digitale)

Nel caso di identificazione informatica tramite firma elettronica qualificata o firma digitale si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto con firma elettronica qualificata o con firma digitale. L'identificazione avviene tramite la verifica della firma elettronica qualificata o firma digitale apposta sulla richiesta. Anche in questo caso il gestore delle identità digitali, considera che la fase di identificazione sia stata correttamente espletata dal fornitore di firma elettronica qualificata o digitale.

Art. 12
(Verifica dell'identità dichiarata)

La verifica dell'identità consiste nel rafforzamento del livello di attendibilità degli attributi di identità, raccolti in fase di identificazione, compiuta attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti.

L'accesso alle fonti autoritative da parte dei gestori dell'identità ai fini dell'attività di verifica è effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445.

I gestori dell'identità digitale e i gestori degli attributi qualificati usufruiscono del servizio di verifica del codice fiscale e dei dati anagrafici ad esso strettamente correlati fornito dall'Agenzia delle Entrate.

Sia il processo di identificazione che il processo di verifica sono eseguiti allo scopo di ottenere un adeguato grado di affidabilità, tenuto conto anche dello specifico livello di sicurezza di SPID.

Le tabelle seguenti rappresentano i requisiti relativi alla verifica di identità in relazione al livello di sicurezza nel caso di persona fisica e di persona giuridica.

Livello di sicurezza	Requisiti
Per tutti i livelli SPID	1) Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata.

	2) I documenti sono autentici e validi sulla base di quanto risulta da soggetti istituzionali competenti (articolo 4, comma 1, lettera c del DPCM o, in assenza di convenzioni con l'Agenzia, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445). Il richiedente viene identificato usando le informazioni ottenute da soggetti istituzionali competenti con i quali l'Agenzia stipulerà apposite convenzioni..

Requisiti da soddisfare/Livelli di sicurezza SPID (persona fisica)

Livello di garanzia	Requisiti
Per tutti i livelli SPID	1) L'esistenza della persona giuridica è basata su evidenze riconosciute dal sistema delle imprese in ambito nazionale. 2) Le evidenze sono tutte valide e autentici sulla base di quanto risulta da soggetti istituzionali competenti. 3) Effettuata l'associazione amministratore o rappresentante legale, all'impresa-persona giuridica, si procede alla verifica - come persona fisica - dell'amministratore o del legale rappresentante, come indicato nella tabella precedente per l'identificazione di una persona fisica.

Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)

In merito alle possibili minacce associabili al processo di verifica dell'identità, si veda l'Appendice B al presente documento.

Art. 13
(Conservazione e registrazione dei documenti)

Il processo di registrazione dei documenti completa la fase di rilascio di un'identità SPID a un soggetto. La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione.

I gestori dell'identità digitale, al fine di poter documentare la corretta esecuzione dei precedenti processi relativi all'attività di rilascio e di una identità, conservano i riscontri relativi ai processi di identificazione e verifica.

In merito al processo di richiesta e identificazione del richiedente devono essere conservati:

1) nel caso di identificazione tramite esibizione a vista:

    a) identificazione "de visu": copia per immagine di tutta la documentazione esibita (documento d'identità e codice fiscale per persone fisiche, procura per persone giuridiche) e modulo di richiesta su supporto cartaceo sottoscritto in modalità autografa;

    b) identificazione remota con strumenti audio/video: i dati di registrazione, nonché l'esplicita volontà del soggetto di dotarsi di identità digitale memorizzati in file audio-video, immagini e metadati strutturati in formato elettronico;

2) nel caso di identificazione informatica:

    a) log della transazione contestualizzato alla specifica richiesta di rilascio dell'identità SPID;

3) nel caso di firma elettronica qualificata o digitale:

    a) modulo di *richiesta di adesione* allo SPID in formato digitale sottoscritto digitalmente;

    b) tutti i documenti e dati utilizzati per l'associazione e la verifica degli attributi.

In merito al processo di verifica devono essere conservati i riscontri ottenuti a seguito degli accessi alle fonti autoritative.

Tutta la documentazione inerente alla creazione e al rilascio di una identità digitale deve essere conservata ai sensi dell'articolo 7, commi 8 e 9, del DPCM.

Al fine della conservazione, il gestore predispone e formalizza un processo di conservazione atto a garantire l'integrità, la disponibilità e la protezione delle informazioni conservate, siano esse analogiche o digitali. Tale processo deve garantire che l'accesso alle informazioni conservate sia limitato esclusivamente a soggetti appositamente designati, per la gestione di motivate richieste da parte dell'utente ovvero per le attività svolte in sede di vigilanza o da parte dell'autorità giudiziaria. Ogni accesso deve essere rilevato, riscontrabile nel tempo, consentire di accertare quando e quali soggetti hanno acceduto alla specifica informazione e la causale dell'accesso. In sede di vigilanza l'Agenzia valuta l'adeguatezza del processo e ne verifica l'effettiva applicazione.

Art. 14
(Emissione dell'identità digitale)

Espletate con successo tutte le attività previste dai processi precedenti, l'identità digitale viene creata e rilasciata dal gestore. L'identità digitale è costituita da un insieme di attributi:

a) attributi identificativi, come specificato dalla lettera c) del comma 1 dell'articolo 1 del DPCM;

b) attributi secondari, come specificato dalla lettera d) del comma 1 dell'articolo 1 del DPCM;

c) codice identificativo, come specificato dalla lettera g) del comma 1 dell'articolo 1 del DPCM;

Il *codice identificativo* è assegnato dal gestore dell'identità digitale, deve essere univoco in ambito SPID. Tale *codice identificativo* è definito dalla seguente regola:

<*codice Identificativo*> = <*cod_IdP*><*numero unico*>

Dove:

a) < *cod_IdP* >: è un codice composto da 4 lettere;

b) <*numero unico*>: è un codice alfanumerico composto da 10 caratteri univoco nel dominio del gestore.

Al fine di supportare anche i caratteri diacritici la codifica degli attributi, primari e secondari di SPID, deve essere effettuata utilizzando lo standard UTF-8 (RFC 3629).

Sezione IV
Rilascio e consegna delle credenziali SPID

Art. 15
(Creazione delle credenziali)

1. Il processo di creazione delle credenziali comprende le attività necessarie a dare origine ad una credenziale o ai mezzi per la sua produzione.

2. In alcuni casi le credenziali, o i mezzi usati per la loro produzione, richiedono una fase di pre-elaborazione prima della loro emissione, ad esempio personalizzazioni sulla base dell'identità a cui esse vengono rilasciate. In questi casi la personalizzazione può avvenire secondo diverse modalità in relazione alla tipologia di credenziale da emettere (ad esempio la personalizzazione di un dispositivo (card, token) che contiene le credenziali può includere la stampa (all'esterno del dispositivo) o la scrittura (sul chip del dispositivo) del nome del soggetto per cui le credenziali saranno emesse). Ovviamente alcune tipologie di credenziali, ad esempio la password, non richiedono alcun intervento di personalizzazione.

Segue l'attività di inizializzazione delle credenziali operata al fine di assicurare che tutti i mezzi usati per la loro produzione siano successivamente idonei a supportare tutte le funzionalità attese. Per esempio, potrebbe essere richiesto che il chip della smart card calcoli la coppia di chiavi crittografiche. Analogamente, una smart card potrebbe essere emessa in uno stato "bloccato" e richiedere un PIN nel successivo processo di attivazione. Deve essere pure definita un'associazione fra una credenziale, o i mezzi usati per la sua produzione, e il soggetto per la quale viene emessa.

Le modalità con cui viene operata tale associazione e il legame instaurato tra le credenziali e l'utente a cui afferiscono, dipendono anche dal livello di sicurezza SPID per il quale le stesse credenziali sono rilasciate.

livello 1 SPID

Per il livello 1 SPID (corrispondente al LoA2 dell'ISO-IEC 29115) sono accettabili credenziali composte da un singolo fattore (ad es. password).

In particolare, in relazione al tipo della password, si raccomanda di adottare regole per ottenere password complesse e difficilmente attaccabili rispettando almeno i seguenti accorgimenti:

a) lunghezza minima di otto caratteri;

b) uso di caratteri maiuscoli e minuscoli;

c) inclusione di uno o più caratteri numerici;

d) non deve contenere più di due caratteri identici consecutivi.

e) inclusione di almeno un carattere speciale ad es #, $,% ecc.

Si raccomanda poi di vietare l'uso di informazioni non segrete riconducibili all'utente (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).

Le password devono avere una durata massima non superiore a 180 giorni e non possono essere riusate, o avere elementi di similitudine, prima di cinque variazioni e comunque non prima di 15 mesi: in questa materia resta valida la normativa prevista dal Codice in materia di protezione dei dati personali (Artt. da 33 a 36) e, in particolare, dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Codice privacy) aggiornato periodicamente in relazione all'evoluzione tecnica e all'esperienza maturata nel settore. Il Gestore dell'Identità adotta una procedura di sollecito con la quale invita l'utente a modificare la Password.)

livello 2 SPID

Per il livello 2 SPID (corrispondente al LoA3 dell'ISO-IEC 29115), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori, non necessariamente basati su certificati digitali.

In questo caso è accettabile l'utilizzo di una password (come sopra descritto) e l'adozione di una OTP generata, a titolo esemplificativo, con l'ausilio di un dispositivo fisico, l'invio di un SMS, liste-tabelle predefinite o applicazioni mobile per smartphone *o tablet collegati in rete*; resta chiaro che, trattandosi di un OTP, la sua validità è limitata solo ad una transazione nell'ambito della sessione applicativa e per un tempo limitato e dipendente dal contesto del servizio richiesto.

livello 3 SPID

Per il livello 3 SPID (corrispondente al LoA4 dell'ISO-IEC 29115), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori, basati su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato II del Regolamento 910/2014.

In merito alle possibili minacce che possono essere associabili alle varie tipologie di token, si veda l'Appendice B al presente documento. In appendice D è inoltre riportata una tassonomia dei tipi di token.

Art. 16
(Consegna delle credenziali)

Anche in questo caso, la complessità del processo dipende dal livello di sicurezza di autenticazione informatica SPID associato alla determinata credenziale. La consegna delle credenziali deve essere operata con modalità e strumenti che assicurino che la stessa sia effettuata al legittimo destinatario con adeguati criteri di riservatezza che salvaguardino il contenuto.

Per alti livelli di sicurezza deve essere prevista una consegna con attestazione dell'effettivo ricevimento delle credenziali; per dispositivi software ciò può essere fatto attraverso sessioni protette per la spedizione in modalità elettronica che assicurino la verifica della corrispondenza tra richiedente dell'identità e destinatario delle credenziali. Per livelli più bassi può essere sufficiente inviare una password o un PIN direttamente all'indirizzo fisico, ad esempio con posta raccomandata, al domicilio elettronico, tramite posta elettronica o PEC, oppure tramite comunicazioni inviate al dispositivo mobile del titolare (smartphone, tablet, cellulare, ecc.)

Il gestore delle identità digitali nella consegna delle credenziali garantisce:

a) che il richiedente sia espressamente informato in modo compiuto e chiaro riguardo:

    1) agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali;

    2) sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;

b) la rispondenza del proprio sistema di sicurezza dei dati alle misure di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196.

Art. 17
(Attivazione delle credenziali)

L'attivazione delle credenziali è il processo durante il quale le credenziali o i mezzi usati per produrle, sono rese effettivamente operative e pronte all'utilizzo.

Il processo di attivazione dipende direttamente dalla tipologia di credenziali adottate, ad esempio in alcuni casi le credenziali sono definite in uno stato di blocco quando sono inizializzate e restano in questo stato

fino alla consegna al soggetto richiedente, in modo da prevenire qualsiasi abuso. In altri casi può essere prevista una password o codice iniziale per lo sblocco delle credenziali. Si consideri pure che le credenziali possono essere attivate anche successivamente ad una sospensione, quando ad esempio la loro validità sia stata temporaneamente annullata.

Art. 18
(Segnalazioni sull'utilizzo delle credenziali)

Il gestore dell'identità digitale, su richiesta dell'utente, segnala via email o via sms, rispettivamente alla casella di posta o sul riferimento telefonico indicato dall'utente ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi di utilizzo della credenziale (data, ora, fornitore del servizio) ad uno degli attributi secondari a tale scopo indicato dall'utente.

CAPO III
Gestione del ciclo di vita dell'identità digitale

Art. 19
(Gestione attributi)

L'utente è tenuto a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del gestore, i contenuti degli attributi identificativi di seguito elencati.

a) Per le persone fisiche:
    1. estremi del documento di riconoscimento e relativa scadenza;
    2. gli attributi secondari così come definiti all'articolo 1, comma d) del DPCM;
b) Per le persone giuridiche:
    1. indirizzo sede legale
    2. codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
    3. rappresentante legale della società
    4. attributi secondari così come definiti all'articolo 1, comma d) del DPCM

L'utente, in caso di dichiarazioni non fedeli o mendaci, si assume le responsabilità previste dalla legislazione vigente:

Le modalità operative per gli aggiornamenti devono essere rese possibili attraverso un'area web dedicata del gestore delle identità digitali, accessibile mediante le credenziali SPID, di livello massimo tra quelle fornite all'utente dal gestore dell'identità digitale.

4. Il gestore dell'identità digitale deve inoltre prevedere un servizio di help desk tramite mail o compilando un form on-line sul sito web. Inoltre potrà essere previsto un sistema attraverso il quale l'utente potrà effettuare autonomamente alcune operazioni.

Ad ogni variazione da operare sugli attributi relativi ad una identità, il gestore dell' identità digitale, prima di aggiornare i dati registrati, deve eseguire le fasi di esame e verifica in relazione al livello SPID associato all'identità digitale La richiesta di aggiornamento e aggiornamento devono essere notificati all'utente utilizzando un attributo secondario funzionale alle comunicazioni (ad es. l'indirizzo di posta elettronica se non è stato modificato durante la sessione di aggiornamento).

Futuri sviluppi potranno includere aggiornamenti automatici sulla base di modifiche degli attributi identificativi o secondari effettuati da pubbliche amministrazioni (ad es. ANPR, comuni, motorizzazione ecc.).

Art. 20
(Sospensione e revoca dell'identità digitale)

Ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il gestore revoca l'identità digitale nei casi seguenti:

1) risulta non attiva per un periodo superiore a 24 mesi;
2) per decesso della persona fisica;
3) per estinzione della persona giuridica;
4) per uso illecito dell'identità digitale;
5) per richiesta dell' utente;
6) per scadenza contrattuale;
7) per scadenza documento identità;

Nel caso previsto dai punti 1 e 6, il gestore dell'identità digitale revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca al utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Nei casi previsti dai punti 2 e 3, il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

Nel caso previsto dal punto 7, il gestore dell'identità digitale sospende di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della sospensione al utente, utilizzando

l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Nel caso previsto dal punto 4, ovvero nel caso in cui il utente ritenga che la propria identità digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione con una delle seguenti modalità:

a) richiesta al gestore inviata via PEC;

b) richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica, inviata tramite la casella di posta appositamente predisposta dal gestore.

Il gestore deve fornire esplicita evidenza al utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
Contestualmente il utente potrà richiedere al fornitore dei servizi presso il quale ritiene che la propria identità sia stata utilizzata fraudolentemente il blocco all'accesso della propria identità inviando una richiesta in tal senso con le stesse modalità sopra previste ad una casella di posta appositamente predisposta dal fornitore di servizi.
Trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione. In caso contrario l'identità digitale viene ripristinata.
Nel caso previsto dal punto 5, l'utente può chiedere al gestore dell'identità digitale, , in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità analoghe a quelle previste dal precedente punto 4, ovvero attraverso:

c) richiesta al gestore inviata via PEC;

d) richiesta inviata tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale o elettronica;

Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.
La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.
I gestori dell'identità digitale conservano la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale

Art. 21
(Gestione del ciclo di vita delle credenziali)

La gestione del ciclo di vita delle credenziali può comprendere i seguenti processi:

a) creazione delle credenziali;
b) consegna delle credenziali o dei mezzi usati per la loro produzione;
c) attivazione delle credenziali o dei mezzi usati per la loro produzione;

d) conservazione delle credenziali;
e) sospensione e revoca delle credenziali o mezzi usati per la loro produzione;
f) rinnovo e sostituzione delle credenziali o mezzi usati per la loro produzione;

Alcuni dei processi sopra elencati possono essere influenzati dal fatto che le credenziali siano rese operative attraverso l'ausilio di un dispositivo hardware.

In merito alle possibili minacce associate al processo di emissione delle credenziali, si veda l'Appendice B al presente documento.

Adeguata documentazione deve essere conservata per tutto il ciclo di vita di una credenziale. Come condizione minima, la documentazione dovrà essere mantenuta per avere traccia delle seguenti informazioni:

a) la creazione della credenziale

b) l'identificativo della credenziale;

c) il soggetto per il quale è stata emessa;

d) lo stato della credenziale.

Opportuna documentazione sarà conservata per ogni sottoprocesso (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) del processo di gestione delle credenziali, nel pieno rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Dovranno essere conservate almeno le informazioni relative alla data di creazione della credenziale, allo stato della stessa, alle date di consegna, di attivazione (se prevista) e di eventuale sospensione, revoca o cancellazione.

Art. 22
(Conservazione delle credenziali)

Questo processo riguarda la conservazione delle credenziali o dei mezzi usati per loro produzione, in modo da garantirne la protezione contro abusi ed usi non autorizzati.

A livello 1 SPID, i file delle credenziali devono essere protetti da un sistema di controllo in modo da limitare l'accesso agli amministratori e alle applicazioni autorizzate.

Questi file non devono mai contenere le password in chiaro; allo scopo possono essere usate tecniche, come da standard internazionali e approvate dall'Agenzia, di crittografia o algoritmi di salt e hashing. A livello 2 e 3 SPID, vale quanto indicato a livello 1 con i necessari allineamenti e conformità agli standard e alla normativa vigente per i moduli crittografici e di sicurezza software/hardware, avendo cura di approntare misure adeguate a mitigare gli specifici rischi derivanti dalla particolare tecnologia adottata.

Art. 23
(Sospensione e revoca delle credenziali)

La revoca è il processo che annulla definitivamente la validità delle credenziali. Diversamente, la sospensione è associata ad un processo di annullamento temporaneo.

La revoca è disposta nei seguenti casi:

1) smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria);

2) utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto;

3) emissione di una nuova credenziale in sostituzione di una già in possesso dell'utente; emissione di una nuova credenziale in sostituzione di una scaduta.

Nel caso previsto dal numero 1, l'utente deve effettuare immediata richiesta di sospensione delle credenziali. Se la richiesta dell'utente non viene effettuata tramite posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il gestore dell'identità digitale deve verificare, anche attraverso uno o più attributi secondari, la provenienza della richiesta di sospensione da parte del soggetto utente.

Il gestore dell'identità digitale sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Durante questo periodo può accadere che:

a) il richiedente annulla la richiesta di sospensione (ad es. per ritrovamento) e quindi l'identità digitale viene ripristinata;

b) il richiedente formalizza la richiesta presentando copia della denuncia presentata all'autorità giudiziaria, quindi l'identità digitale viene revocata.

In assenza di quanto indicato nelle lettere a) o b), l'identità digitale sarà automaticamente ripristinata scaduto il periodo di 30 giorni dalla data della richiesta.

Nel caso previsto dal numero 2, anche a seguito di segnalazioni ai sensi dell'articolo 8, comma 4 del DPCM, l'utente richiede la sospensione immediata dell'identità digitale al gestore del servizio. Si veda il paragrafo sulla sospensione e revoca dell'identità digitale.

Art. 24
(Rinnovo e sostituzione delle credenziali)

Alcune tipologie di credenziali prevedono una scadenza temporale per l'uso. In questo caso il gestore dovrà provvedere tempestivamente alla creazione di una nuova credenziale da consegnare all'utente in sostituzione della vecchia scaduta. Situazione analoga è quella della sostituzione di una credenziale a seguito di guasto o per upgrade tecnologico (ad esempio nel caso di credenziali di livello 3 passaggio da

chiavi da 128 bit a quelle da 256). Il gestore dell'identità, nel primo caso su richiesta dell'utente, nel secondo su sua iniziativa, emette la nuova credenziale e revoca automaticamente la vecchia.
In entrambi i casi devono essere previsti meccanismi con i quali il gestore comunica la revoca all' utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Si noti che, per alcune tipologie di credenziali, come ad es. quelle contenute su un dispositivo, può essere prevista (successivamente alla sua revoca) anche la distruzione fisica.

CAPO IV
Utilizzo di SPID

Art. 25
(Autenticazione)

L'autenticazione è il processo in cui l'utente, usando le proprie credenziali SPID, dimostra la propria identità al gestore dell'identità digitale al fine di accedere a servizi disponibili in rete. Per la realizzazione del processo di autenticazione, SPID adotta il modello federato delle identità digitali definito dalle specifiche SAML emesse dal consorzio OASIS (cfr *Regole Tecniche SPID).*

Le relazioni tra i soggetti coinvolti nel processo (*l'utente, il gestore dell'identità digitale, il fornitore di servizi* ed, eventualmente, *il gestore di attributi qualificati*) si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata dal soggetto titolare di una identità digitale, portano all'autorizzazione o al diniego della fruizione di un servizio erogato da un fornitore di servizi. Tali interazioni determinano la produzione di certificazioni (Asserzioni nella nomenclatura SAML) da parte dei *gestori delle Identità digitali* ed, eventualmente, dei *gestori di attributi qualificati*, e l'utilizzo delle stesse da parte dei *fornitori di servizi*.

I passaggi previsti sono i seguenti:

1) il *titolare dell'identità digitale* richiede l'accesso ad un servizio collegandosi telematicamente al portale del *fornitore di servizi*;

Il *fornitore dei servizi,* per poter procedere, deve individuare il *gestore dell'Identità digitale* in grado di autenticare il soggetto richiedente. Per far ciò il *fornitore dei servizi* chiede indicazioni allo stesso utente, ad esempio, facendo scegliere il proprio gestore dell'identità digitale da un elenco riportante tutti i gestori di identità aderenti a SPID;

2) il *fornitore dei servizi* indirizza il soggetto *titolare dell'identità digitale* presso il *gestore dell'identità digitale,* individuato al passaggio precedente, richiedendo l'autenticazione con il livello SPID associato al servizio richiesto e l'eventuale attestazione di attributi necessari per l'autorizzazione all'accesso;

3) *il gestore dell'identità digitale* verifica l'identità del soggetto sulla base di credenziali fornite dallo stesso. Se tale verifica ha esito positivo viene emessa, ad uso del *fornitore dei servizi*, una asserzione di autenticazione SAML attestante gli attributi eventualmente richiesti; Le modalità per la richiesta e l'impiego degli attributi deve avvenire secondo quanto specificato al successivo art.27

4) il *titolare dell'identità digitale* viene quindi reindirizzato, portando con sé l'asserzione prodotta, verso il *fornitore dei servizi*;

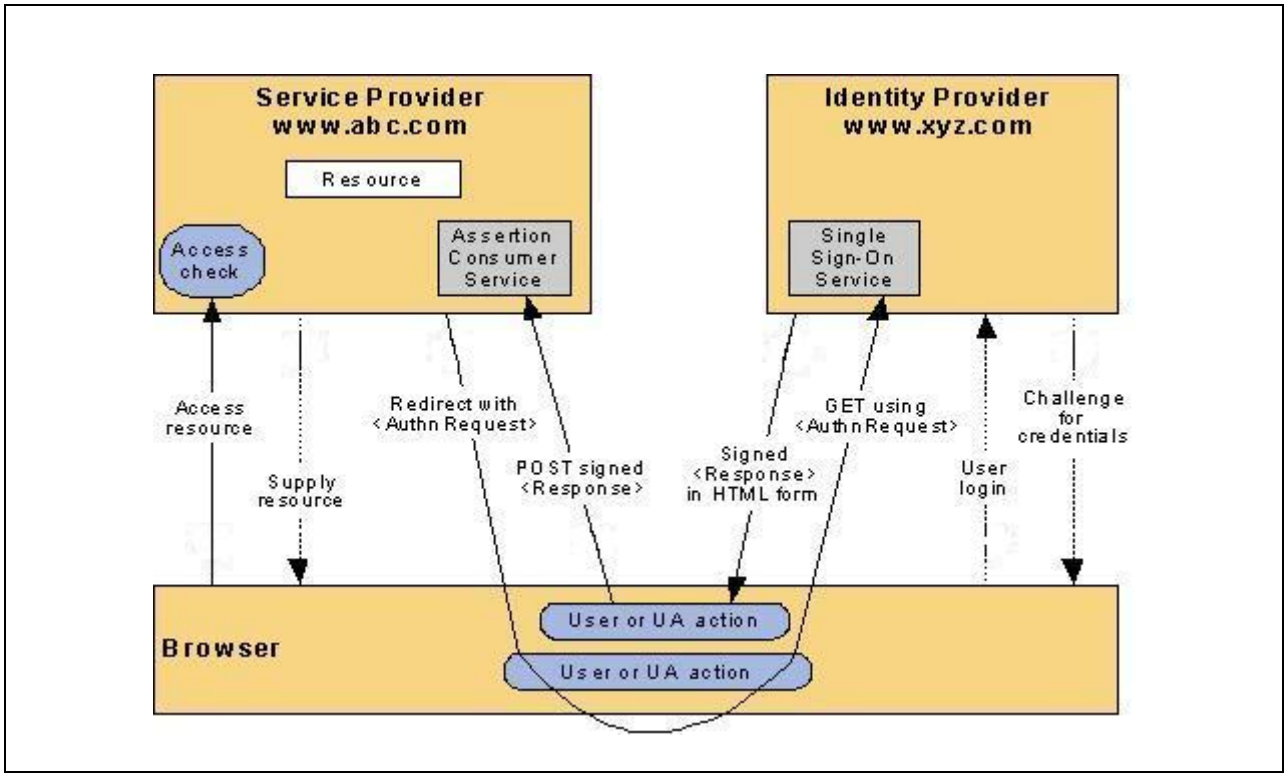
5) il *fornitore dei servizi* può, a questo punto, avere la necessità di verificare attributi qualificati riferibili all'utente qualora questi fossero richiesti dalle policy di sicurezza che regolano l'accesso al servizio.

   In questo caso:

   a) individuati, per il tramite del registro SPID, i gestori di attributi qualificati in grado di certificare gli attributi necessari, inoltra agli stessi una richiesta di attestazione presentando i riferimenti dell'identità digitale per la quale si richiede la verifica;

   b) il risultato della richiesta è l'emissione, da parte del gestore di attributi qualificati, di una asserzione SAML;

6) il fornitore dei servizi, raccolte tutte le necessarie asserzioni SAML, verifica le policy di accesso al servizio richiesto e decide se accettare o rigettare la richiesta.



SSO SP-Initiated Redirect/POST binding

Il protocollo descritto viene realizzato secondo il profilo "*Web Browser SSO*" dello standard SAML, nella modalità cosiddetta "*SP-Initiated" e* nelle versioni "*Redirect/POST binding*" e "*POST/POST binding*". Tale modalità prevede che il processo di autenticazione sia innescato dalla richiesta operata dall'utente, tramite il suo web browser, presso il sito del *fornitore di servizi*, il quale, a sua volta, si rivolge al gestore dell'identità inoltrando una richiesta di autenticazione SAML basata sul costrutto <AuthnRequest> e usando il binding HTTP Redirect o il binding HTTP POST.

La relativa risposta SAML, basata sul costrutto <Response>, veicolante una asserzione di autenticazione, viene restituita al richiedente tramite il binding HTTP POST.

Art. 26
(Registro SPID)

Il Registro SPID contiene le informazioni relative ai soggetti che hanno in corso un'apposita convenzione con AgID per operare nell'ambito dello SPID ed assolve la funzione di registro di federazione, certificando la relazione di fiducia stabilita tra i soggetti appartenenti a SPID. Tale relazione di fiducia si fonda nella condivisione dei criteri di sicurezza e delle regole di interoperabilità previste da SPID.

Art. 27
(Uso degli attributi SPID)

I fornitori di servizi, per verificare le policy di sicurezza relativi all'accesso ai servizi da essi erogati potrebbero avere necessità di informazioni relative ad attributi riferibili ai soggetti richiedenti. Tali policy dovranno essere concepite in modo da richiedere per la verifica il set minimo di attributi pertinenti e non eccedenti le necessità effettive del servizio offerto e mantenuti per il tempo strettamente necessario alla verifica stessa, come previsto dall'articolo 11 del decreto legislativo n. 196 del 2003.

I fornitori di servizio dovranno segnalare ai gestori delle identità quali attributi identificativi e secondari dovranno essere attestati con l'asserzione emessa a seguito dell'autenticazione dei soggetti richiedenti i servizi. I gestori dell'identità, al momento dell'autenticazione e prima di emettere l'asserzione, devono ottemperare all'obbligo di informativa di cui all'articolo 13 del decreto legislativo n. 196 del 2003.
Nel caso in cui per l'applicazione delle policy di accesso relative al servizio invocato si rendesse necessaria la verifica di attributi qualificati riferibili al richiedente, i fornitori di servizio si rivolgeranno ai gestori degli attributi qualificati in grado di certificare tali attributi, individuabili attraverso il registro SPID. Per far ciò, prima di procedere, ai sensi del comma 2 dell'articolo 13 del DPCM, danno evidenza all'utente degli attributi qualificati necessari in ottemperanza all'obbligo di informativa di cui all'articolo 13 del decreto legislativo n. 196 del 2003.

Art. 28
(Gestione delle sessioni di autenticazione)

Il modello di gestione delle sessioni di autenticazione in SPID si differenzia a seconda del livello SPID con il quale viene instaurato un contesto di autenticazione. Inoltre per la sicurezza del canale di comunicazione tra utente e gestore è necessario che il gestore IdP

· garantisca la cifratura mediante l'adozione di meccanismi standard e protocolli aggiornati alle versioni più recenti

· renda possibile l'utilizzo delle funzionalità di accesso web mediante le tipologie di browser più diffuse ma con limitazioni per le versioni più obsolete indicando le versioni minime necessarie per accedere al servizio SPID nel Manuale Operativo e nella Guida Utente.

Per particolari esigenze, può essere temporaneamente consentito l'uso di versioni precedenti di meccanismi e protocolli se preventivamente autorizzati dalla Agenzia e nei termini da questa indicati.

A) Gestione delle sessioni per il livello 1 SPID

Per il livello 1 SPID è ammessa l'instaurazione di una sessione di autenticazione, associata ad un determinato utente titolare di identità digitale, mantenuta dal gestore dell'identità digitale e condivisa da tutti i fornitori di servizio che nel corso di vita della sessione stessa erogano servizi per quel determinato utente.

Per ogni nuovo fornitore di servizi che si aggiunge al contesto di autenticazione, il gestore dell'identità digitale dovrà dare informativa all'utente ai sensi dell'articolo 13 del decreto legislativo n. 196 del 2003

Il fornitore di servizi che condivide una sessione di autenticazione di un dato gestore di identità digitale, può instaurare con l'utente una sessione finalizzata al solo accesso al servizio richiesto e per questa sessione

deve fornire meccanismi espliciti per il logout dell'utente.

Per la chiusura della sessione comune è previsto un meccanismo logout globale secondo il *single logout profile* di SAML (cfr par. 4.4 del documento *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*)

B) Gestione delle sessioni per i livelli 2 e 3 SPID

Per i livelli 2 e 3 SPID, allo scopo di garantire la massima sicurezza e stabilità del sistema, non si prevede la possibilità di mantenimento di sessioni condivise di autenticazione.

Pertanto:

1) il gestore dell'identità digitale non deve mantenere alcuna sessione di autenticazione con l'utente;
2) ogni fornitore di servizi deve gestire per proprio conto l'eventuale sessione con l'utente. Per la chiusura dovranno essere forniti meccanismi espliciti per il logout.

Art.29
(Tracciatura e conservazione della documentazione di riscontro)

Il comma 2 dell'articolo 13 del DPCM obbliga i fornitori di servizi alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi. Tali informazioni saranno costituite da registrazioni composte dal messaggio SAML di richiesta di autenticazione e della relativa asserzione emessa dal gestore delle identità. Tali messaggi riportano identificativi e date di emissione e sono firmati, rispettivamente, dallo stesso *fornitore di servizi* e dal *gestore dell'identità digitale;* quest'ultima caratteristica fornisce le necessarie garanzie di integrità e non ripudio.

L'insieme delle Registrazioni costituisce il Registro delle transazioni del fornitore del servizio. Le tracciature devono avere caratteristiche di riservatezza, inalterabilità e integrità e sono conservate adottando idonee misure di sicurezza ai sensi dell'articolo 31 del decreto legislativo 30 giugno 2003, n. 196, sotto la responsabilità del titolare del trattamento; l'accesso ai dati è riservato a personale espressamente autorizzato e incaricato del trattamento dei dati personali. Devono essere utilizzati meccanismi di cifratura.

Analogo registro dovrà essere tenuto dal gestore delle identità digitali, secondo modalità definite nelle regole tecniche di cui all'articolo 4, comma 3 del DPCM.

Nel caso in cui uno stesso soggetto sia, allo stesso tempo, gestore dell'identità digitale e fornitore di servizi devono essere mantenuti separati i registri di tracciatura delle transazioni così come le banche dati relative alla gestione delle identità digitali. Tale vincolo di separazione deve essere applicato anche nei confronti degli accessi degli operatori di help desk e nella gestione di cruscotti di self-caring.

Sezione V
Monitoraggio e convenzioni

Art. 30
(Monitoraggio di AGID sul sistema SPID)

L'Agenzia svolge funzioni di monitoraggio, anche sulla base delle segnalazioni fatte dai cittadini, allo scopo di valutare e garantire usabilità, accessibilità e corretto utilizzo degli elementi identificativi SPID e

indica le migliori pratiche da adottare. Ai fini dell'attività di vigilanza, i gestori di identità digitali rendono disponibili all'Agenzia:

1) gli incidenti di sicurezza rilevati;

2) le informazioni circa il livello di soddisfazione dei propri clienti;

3) le caratteristiche di eventuali servizi aggiuntivi offerti;

4) le informazioni relative a disservizi, secondo la classificazione e le modalità riportate nella tabella seguente.

Classificazione dei disservizi in relazione agli effetti prodotti e relativi codici identificativi
1. Comportamento anomalo e non circoscritto: comportamento difforme dalle regole tecniche per il quale non è circoscritto il potenziale impatto (codice 1A, se rilevato dal gestore; codice 1B, se rilevato da terzi).
2. Comportamento anomalo circoscritto: comportamento difforme dalle regole tecniche per il quale è circoscritto il potenziale impatto (codice 2A, se rilevato dal gestore; codice 2B, se rilevato da terzi).
3. Malfunzionamento bloccante: tipologia di malfunzionamento a causa del quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, non possono essere utilizzate in tutto o in parte consistente dagli utenti (codice 3A, se rilevato dal gestore; codice 3B, se rilevato da terzi).
4. Malfunzionamento grave: tipologia di malfunzionamento a causa del quale in alcune circostanze le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, possono essere utilizzate parzialmente dagli utenti (codice 4A, se rilevato dal gestore; codice 4B, se rilevato da terzi).
5. Malfunzionamento: situazione a causa della quale le funzionalità del sistema del gestore delle identità digitali, come definite nelle regole tecniche, in tutto o in parte, risultano degradate ovvero il sistema ha un comportamento anomalo in situazioni circoscritte e per funzionalità secondarie (codice 5A, se rilevato dal gestore; codice 5B, se rilevato da terzi).

Classificazione dei disservizi

I gestori dell'identità digitale hanno l'obbligo di comunicare all'Agenzia, entro trenta minuti dalla rilevazione dell'evento stesso, i disservizi contraddistinti da uno dei seguenti codici: 1A, 1B, 2A, 2B, 3A, 3B ed entro due ore i disservizi contraddistinti dai codici 4A, 4B, 5A e 5B.

La comunicazione deve fornire anche una prima valutazione dell'incidente, le eventuali misure adottate al riguardo e la tempistica prevista per il ripristino della normale operatività.

A seguito delle risultanze dell'attività di monitoraggio e della rilevanza/frequenza dei disservizi, nell'ipotesi di inosservanza di uno o più degli obblighi posti a carico del gestore delle identità digitali, l'Agenzia in esito all'accertamento contesta le violazioni disponendo l'eventuale sospensione, prescrivendo le attività da porre in essere per l'adeguamento da parte del gestore, indicando nel contempo il termine entro il quale il gestore stesso deve conformarsi agli obblighi previsti. Qualora il gestore non provveda in tal senso nei tempi indicati, l'Agenzia, con provvedimento motivato notificato all'interessato, adotta, nei casi più gravi, un provvedimento di revoca dell'accreditamento ai sensi dell'articolo 12, comma 4 del DPCM.

I gestori delle identità digitali inviano all'Agenzia, con cadenza almeno bimestrale, i dati statistici relativi all'utilizzo del sistema, le metriche quantitative e qualitative che saranno definite e concordate a valle dello *start up* di SPID.

Art. 30-bis
(Collaborazione fra AGID ed il Garante per la protezione dei dati personali)

Nell'ambito dell'attività di vigilanza di cui all'articolo 4, comma 1, lett. b), del DPCM sull'operato dei soggetti che partecipano a SPID, l'AGID ove riscontri casi in cui sussistano elementi per ritenere la violazione della normativa in materia di protezione dei dati personali, ne informa tempestivamente il garante per la protezione dei dati personali.

Il Garante, anche sulla base delle informazioni di cui sopra o di quelle concernenti violazioni di dati personali di cui all'articolo 4, comma 3 lett.g-bis, del decreto legislativo 30 giugno 2003 n. 196, eventualmente ricevute ai sensi dell'art. 11, comma 1, lett. o) del DPCM, sottopone a un audit di sicurezza, anche a campione, i soggetti partecipanti allo SPID di cui all'articolo 3, comma 1, lett. a), b) e c) del DPCM, tenuto conto delle diverse categorie dei soggetti interessati. I risultati dell'audit sono inseriti nella relazione annuale del Garante.

I gestori dell'identità digitale comunicano al garante, e per conoscenza all'AGID, la violazione dei dati personali di cui sopra entro 24 ore dell'avvenuta conoscenza della violazione per la prima sommaria comunicazione ed entro 3 giorni dalla stessa per una comunicazione dettagliata. La comunicazione è effettuata mediante apposito modello predisposto dal garante e disponibile on line sul sito dell'autorità. Qualora si verifichi una violazione di dati personali e dalla stessa possa derivare un pregiudizio ai dati personali o alla riservatezza di un utente o di altre persone, ossia dei soggetti cui si riferiscono i dati violati , oltre alla comunicazione al Garante i gestori sono tenuti a comunicare l'avvenuta violazione, senza ritardo, anche a tali soggetti, utilizzando il modello predisposto da Garante. Si applicano, in quanto compatibili, le disposizioni di cui al provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*) adottato dal Garante il 4 aprile 2013 e pubblicato sulla gazzetta ufficiale n.97 del 4 aprile 2013.

Il Garante e l'AGID stipulano un protocollo di intesa per l'attuazione delle disposizioni del presente articolo nel rispetto delle rispettive competenze.

Art. 31
(Convenzioni)

Gli schemi di convenzione per i gestori dell'identità digitale e per le pubbliche amministrazioni in qualità di fornitori di servizi sono definiti nell'ambito di specifici regolamenti emanati dall'Agenzia .

Gli schemi di convenzione per i gestori degli attributi qualificati e per i fornitori di servizi privati sono definiti nell'ambito di specifici regolamenti emanati dall'Agenzia.

Appendice A – Criteri per l'attribuzione dei i livelli di sicurezza dei servizi

Il sistema SPID è basato su tre livelli di sicurezza di autenticazione informatica, con il livello 1 associato a quello più basso ed il livello 3 a quello più elevato. Ai sensi dell'articolo 6, comma 5 del DPCM, l'erogatore del servizio deve scegliere il livello di sicurezza da associare all'accesso del servizio stesso.

La scelta del livello di sicurezza (LoA) deve essere fondamentalmente basata sulle conseguenze derivanti da un accesso improprio a sistemi o applicazioni determinato dalla probabilità di errore che si può commettere nel processo di autenticazione; livelli di sicurezza (LoA) più alti saranno associati a servizi per i quali un accesso improprio comporta conseguenze e impatti più significativi (come sistemi che trattano dati sensibili o dati relativi a reddito o patrimonio) mentre richieste a carattere informativo possono essere associate a livelli più bassi.

E' importante evidenziare il fatto che la scelta dei livelli di sicurezza è operata a tutela degli interessi reciproci degli utenti fruitori che degli erogatori dei servizi. Ad evidenziare ciò basta riferirsi a servizi relativi a operazioni dispositive, come bonifici on line effettuati attraverso servizi di home banking. E' chiaro che se la banca, erogatrice dei servizio, ha interesse a tutelarsi contro i furti on-line operati, ad esempio, attraverso furti di identità, questo interesse coincide con quello del titolare del conto corrente on-line dal quale vengono fraudolentemente sottratti i fondi.

La metodologia suggerita dall'Agenzia prevede l'identificazione dei rischi per ogni specifico servizio e la conseguente assegnazione dei livelli di sicurezza previsti in ambito SPID; ovviamente la misura dello impatto potenziale di questi rischi individuati dipende dallo specifico contesto e dalle entità coinvolte da impropria autenticazione.

La tabella seguente fornisce sinteticamente una serie di possibili associazioni

	Impatto potenziale massimo di eventi per ogni livello di sicurezza SPID		
Impatto causato da un accesso improprio	**Livello 1**	**Livello 2**	**Livello 3**
	Sistema di autenticazione a singolo fattore, discreta sicurezza sulla fedeltà/esattezza dell'identità asserita	Sistema di autenticazione a doppio fattore, alta sicurezza sulla fedeltà/esattezza dell'identità asserita	Sistema di autenticazione a doppio fattore basato su certificati digitali, elevatissima sicurezza sulla fedeltà/esattezza dell'identità asserita
Potenziale danno di reputazione	Basso	Moderato	Alto
Potenziali danni finanziari del l'utente e dell'erogatore del servizio	Basso	Moderato	Alto

Potenziale danno per rilascio di informazioni sensibili del l'utente	N/A	Basso	Moderato/Alto
Potenziale danno per violazioni di carattere civile, ad es. non conformità a regolamenti, norme ecc.	N/A	Basso/Moderato	Alto
Potenziali danni a programmi di interesse pubblico	Basso	Moderato	Alto
Impatto potenziale per la sicurezza personale del l'utente e dell'erogatore del servizio	N/A	Basso	Moderato/Alto

Impatto Potenziale/Livello di Sicurezza SPID

Dove per il valore (basso, moderato, alto) assegnato ai potenziali impatti è stato scelto la definizione normalmente adottata nell' ISO/IEC 27001 framework e FIPS 199.

Valore Impatto	
Basso	La perdita di confidenzialità, integrità e disponibilità ha un effetto negativo limitato per l'operatività delle organizzazioni, per i beni e per le persone.
Moderato	La perdita di confidenzialità, integrità e disponibilità potrebbe avere un serio effetto negativo per l'operatività delle organizzazioni, per i beni e per le persone.
Alto	La perdita di confidenzialità, integrità e disponibilità potrebbe avere un severo o catastrofico effetto negativo per l'operatività delle organizzazioni, per i beni e per le persone.

Definizione valore impatto

Ulteriori considerazioni possono essere fatte in relazione alla classificazione dei dati secondo lo schema riportato in tabella, fermo restando la facoltà della singola Amministrazione di definire criteri diversi in base alle diverse modalità di erogazione dei servizi e ai dati resi disponibili :

Livello	Classificazione del dato	Tipo di accesso	Esempi
nessuno	Pubblico	Non è richiesto nessun livello di autenticazione.	Esempio area informativa del sito www.agid.gov.it; www.comune.milano.it
1	Pubblico/Interno	Livello 1 è adeguato per utenti sono iscritti ad un sito ma senza la possibilità di eseguire operazioni dispositive.	Esempio 1. area cittadini ma non dispositiva del comune di Roma https://www.comune.roma.it/wps/myportal
2	Interno	Livello 2 è adeguato per utenti che accedono ad informazioni che hanno creato, o per utenti che per motivazioni professionali possono ad trattare informazioni di soggetti terzi.	Esempio area riservata dei comuni per il pagamento di tasse e tributi, inoltro di richieste/domande, interrogazioni, aggiornamenti e cancellazioni che non riguardano dati sensibili.
3	Riservato	Livello 3 è necessario per utenti che sulla base di ruoli/responsabilità possono accedere ad informazioni di tipo riservato.	Esempio siti che trattano dati sensibili, specifiche transazioni che includono trasferimento di fondi, accesso a documenti riservati o rilevanti per le amministrazioni e le imprese.

Classificazione dato/Tipo di accesso

L'Agenzia, al fine di rendere omogenei i LoA associati ai servizi su tutto il territorio nazionale, promuove e pubblica, nella sezione SPID del proprio sito istituzionale il LoA da associare alle categorie di servizi che presentano carattere di omogeneità.

Appendice B – Minacce associate alla gestione del ciclo di vita delle identità digitali
Minacce per il processo verifica dell'identità dichiarata in fase di registrazione.

In generale sussistono due categorie di minacce nel processo di registrazione:

a) furto/usurpazione di identità

b) compromissione o uso non corretto della infrastruttura associata ai servizi erogati dal gestore delle identità digitali. Questa problematica rientra in quella generale relativa ai controlli di sicurezza (separazione dei compiti, conservazione della documentazione, audit indipendenti)

La tabella A elenca le minacce correlate al processo di registrazione.

Attività	**Minaccia/Attacco**	**Esempio**
Registrazione	Furto/usurpazione di identità	Un richiedente dichiara una identità non corretta ad es. usando un documento d'identità contraffatto
	Ripudio/disconoscimento della registrazione	Un cittadino/impresa nega la registrazione affermando che non ha mai richiesto la registrazione

Minacce nel processo di registrazione

Le minacce di registrazione possono essere impedite, o almeno dissuase, rendendo più complessa la possibilità di effettuare un furto di identità e aumentando la probabilità di rilevazione di queste evenienze.

A qualsiasi livello devono essere utilizzati dei metodi (1) per verificare l'esistenza di una persona con l'identità dichiarata, (2) che il richiedente sia effettivamente l'utente titolare dell'identità dichiarata e (3) che lo stesso non può successivamente disconoscere la registrazione.

Minacce associate al processo di emissione delle credenziali

Le minacce nel processo di emissione riguardano attacchi causati da furti/usurpazione di identità e da meccanismi di trasporto per l'emissione delle credenziali.

La tabella elenca le minacce ed esempi di possibile strategia di mitigazione correlate al processo di emissione.

Attività	Minaccia/Attacco	Esempio	Strategia di mitigazione
Emissione	Divulgazione/rivelazione	Una chiave generata dal gestore delle identità digitali è copiata da un aggressore informatico.	Emissione delle credenziali di persona, spedizione in buste sigillate con posta raccomandata, uso di una sessione protetta per la spedizione in modalità elettronica
	Manomissione	Una nuova password generata dal sottoscrittore viene modificata da un aggressore informatico.	Emissione delle credenziali di persona, spedizione in buste sigillate con posta raccomandata, uso di protocolli di comunicazione che proteggono la sessione dati.
	Emissione non autorizzata	Rilascio delle credenziale ad una persona che afferma di essere il sottoscrittore (e in effetti non lo è)	Definizione di una procedura che assicura che la persona destinataria delle credenziali sia la stessa persona che ha partecipato nel processo di registrazione

Minacce/Processo di emissione

Minacce associate ai token

Un potenziale aggressore malevolo può prendere il controllo di un token e fingere di essere il legittimo proprietario del token. Le minacce associate ai token sono classificate in base alla tipologia dei token:

Tipo token	**Esempi di minacce**
Qualcosa che abbiamo	Può essere perso, danneggiato, rubato o clonato. Ad esempio un aggressore malevolo potrebbe prendere possesso del computer e copiare un token software. Analogamente un token hardware potrebbe essere rubato, manomesso o duplicato.
Qualcosa che conosciamo	L'aggressore potrebbe provare ad indovinare la password o il PIN o installare del software maligno (ad es. keyboard logger) per catturare la password, in alternativa possono essere adottate catture del traffic dalla rete o attraverso tecniche di social engineering
Qualcosa che siamo	Può essere replicato, ad esempio un aggressore potrebbe ottenere una copia delle impronte digitali e costruirne una replica assumendo che il sistema biometrico non utilizzi robuste, e consigliate, tecniche di rilevazione.

Tipo token

La tabella che segue illustra le minacce/attacchi più comuni:

Minaccia/Attacco token	**Descrizione**	**Esempi**
Furto	Un token fisico viene rubato	Furto di un cellulare, dispositivo fisico ecc.
Scoperta	Le risposte a domande di suggerimento per riconoscere l'utente sono facilmente deducibili o ricavabili da diverse sorgenti disponibili.	Ad es. la domanda "Quale liceo hai frequentato ?" è facilmente ottenibile dai siti web di tipo social.
Duplicazione	Il token è stato copiato senza , o con, l’assenso dell'utente.	Password scritta su post-it o memorizzato su un file che viene successivamente copiato da un aggressore.
Intercettazione	Il token viene rilevato nel momento dell'immissione.	La password viene dedotta osservando l'immissione da tastiera, o con l'ausilio di keylogger software.

Offline cracking	Sono usate tecniche analitiche offline ed esterne ai meccanismi di autenticazione.	Una chiave viene estratta utilizzando tecniche di analisi differenziale su token hardware rubati. Un token software PKI può essere soggetto ad attacchi da dizionario per identificare la password corretta da usare per decifrare la chiave privata.
Phishing o pharming	L'utente viene ingannato e crede che l'aggressore sia il fornitore di servizi o di identità (sito civetta).	DNS re-routing. Una password viene rivelata ad un sito civetta che simula l'originale.
Ingegneria sociale	L'aggressore stabilisce un livello di sicurezza con l'utente in modo da convincerlo a rivelargli il contenuto del token.	Una password viene rivelata durante una telefonata ad un aggressore che finge di essere l'amministratore di sistema.
Provare a indovinare (online)	L'aggressore si connette al sito del gestore di identità online e prova ad indovinare il token valido.	Attacchi online basati su dizionari o password note.

Minacce/Tipo token

E le strategie di mitigazione delle minacce sono indicate nella tabella.

Minaccia/Attacco token	**Tecnica di mitigazione della minaccia**
Furto	usare token multi-fattore che devono essere attivati attraverso un PIN o elementi biometrici.
Scoperta	Usare metodologie tali da rendere complessa la deduzione di una risposta
Duplicazione	Usare token difficilmente duplicabili come token crittografici hardware.
Intercettazione	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.

Offline cracking	Usare token con elevata entropia. Usare token che causino il blocco dopo un numero limitato di tentativi.
Phishing o pharming	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.
Ingegneria sociale	Usare tecniche di autenticazione dinamica tali che la conoscenza di una parola non fornisca alcuna informazione in successive autenticazioni.
Provare a indovinare (online)	Usare token con elevata entropia. Usare token che causino il blocco dopo un numero limitato di tentativi.

Tipo minaccia/Tecnica di mitigazione

A queste tecniche possono essere applicate strategie addizionali come l'uso di fattori multipli, meccanismi di sicurezza fisica, regole di complessità sulle password, sistematici controlli di sicurezza sulla rete e sui sistemi, tecniche out of band per la verifica del possesso di dispositivi registrati, addestramento periodico e informazione preventiva su potenziali minacce.

Appendice C - Tipi di token e loro Tassonomia

Per le credenziali a doppio fattore viene normalmente utilizzato un token di tipo hardware o di tipo software.

- Token di tipo hardware: sotto forma di dispositivo elettronico portatile di piccole dimensioni, alimentato a batteria con autonomia nell'ordine di qualche anno, dotato di uno schermo e talvolta di una tastiera numerica (alcuni token possono essere collegati ad un computer tramite una porta USB per facilitare lo scambio di dati).
- Token di tipo software: le informazioni necessarie risiedono direttamente nell'apparato dell'utente (PC, tablet, ecc.), e non in un oggetto esterno.

In particolare nei token crittografici multi-fattore, una chiave crittografica viene direttamente contenuta nel dispositivo hardware o viene immagazzinata su un disco, o equivalente media "soft", nel caso di token software ne viene richiesta l'attivazione attraverso un secondo fattore di autenticazione. L'autenticazione, in questo caso, è ottenuta provando sia il possesso che il controllo della chiave. Il convalidatore del token dipende strettamente dallo specifico protocollo crittografico, generalmente basato su qualche tipo di messaggio firmato, ad esempio, nel caso del protocollo TLS, è previsto il messaggio di "certificate verify".

I token del tipo one-time password (OTP) multi-fattore, sono dispositivi hardware che generano una password valida una sola volta nella fase di attivazione e che richiedono l'attivazione attraverso un secondo fattore di autenticazione. Il secondo fattore di autenticazione può essere ottenuto attraverso "qualcosa che conosciamo" ad es. un PIN o "qualcosa che siamo" ad esempio attraverso la lettura di elementi biometrici (impronte digitali). La password one-time viene normalmente visualizzata sul dispositivo e deve essere digitata manualmente (in alcuni casi può essere prevista la lettura diretta dal computer attraverso, ad esempio, l'interfaccia USB).

Per completezza, i processi di autenticazione multi-stadio nel quale viene utilizzato un token a singolo fattore per ottenere un secondo token non costituiscono una vera autenticazione multi-fattore, in questo caso il livello di sicurezza dell'autenticazione della soluzione combinata è pari a quello del token più debole. Ad esempio, alcune soluzioni in mobilità si basano su chiavi crittografiche complete o parziali memorizzate su un server online e scaricate sul computer locale del richiedente dopo una prima autenticazione basata sull'uso di password. Successivamente, il richiedente può usare il token crittografico precedentemente scaricato per autenticarsi con un gestore di identità remoto; questo tipo di soluzione deve essere considerata dello stesso livello di sicurezza della password usata dal richiedente per ottenere il token crittografico.

In alcuni casi può essere preferibile elevare il livello di sicurezza dell'autenticazione durante una sessione applicativa, ciò può essere considerato un caso speciale di autenticazione multi-token dove un primo token (ad es. la password) viene utilizzato per stabilire una sessione sicura ed un secondo token (ad es. un out of band token) viene utilizzato per attivare una particolare transazione durante la sessione. Anche se i due token sono usati in fasi differenti, viene normalmente riconosciuto questo risultato come uno schema di autenticazione multi-token che può elevare il livello globale di sicurezza dell'autenticazione se i due token appartengono a due tipologie ("che abbiamo", "che conosciamo", "che siamo") differenti.

Di seguito si descrivono i principali tipi di token utilizzabili per l'autenticazione informatica:

- **Token con segreto memorizzato**: tipicamente è composto da una stringa di caratteri (password) o una sequenza di cifre (PIN); nel caso SPID per essere considerato a livello 1 di sicurezza di autenticazione informatica devono essere rispettate le caratteristiche, policy e regole di complessità delle password indicate al paragrafo relativo alla creazione delle credenziali.

- **Token con conoscenza pre-registrata**: normalmente una serie di richieste o indicazioni (prompt o challenge) che vengono stabilite tra l'utente e il gestore delle identità digitali durante la fase di registrazione (ad es. una risposta del tipo "il nome di tua da nubile ?").

- **Token con tabella dei codici/segreti**: un token fisico o elettronico che contiene una tabella di codici riservati, all'utente può essere richiesto di rispondere con il codice/segreto corrispondente ad una specifica posizione della tabella.

- **Token out of band**: un token fisico indirizzabile in modo univoco che può ricevere un codice/segreto selezionato dal gestore dell'identità per essere usato una sola volta durante la sessione di servizio (ad esempio un codice inviato via SMS ad un numero di cellulare certificato).

- **Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP)**: un dispositivo hardware che supporta la generazione automatica di una OTP (ad es. un codice composto da sei caratteri).

- **Dispositivo Crittografico a singolo fattore (SF)**: un dispositivo hardware che esegue operazioni crittografiche su un input al dispositivo. Il dispositivo non richiede l'attivazione attraverso un secondo fattore di autenticazione. Questo dispositivo usa chiavi crittografiche asimmetriche o simmetriche embedded (integrate nel dispositivo stesso).

- **Token crittografico software multi-fattore (MF)**: una chiave crittografica è memorizzata su un disco o un altro "media" e richiede l'attivazione attraverso un secondo fattore di autenticazione. L'autenticazione viene quindi ottenuta provando il possesso e il controllo della chiave. Questo sistema è basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato II del Regolamento 910/2014

- **Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP)**: un dispositivo hardware che genera una one-time password per l'uso durante l'autenticazione e che richiede l'attivazione attraverso un secondo fattore di autenticazione (ad es. un dato biometrico, un dato digitato su un pad integrato ecc.)
- **Dispositivo Crittografico multi-fattore (MF)**: un dispositivo hardware che contiene chiavi crittografiche che richiedono l'attivazione attraverso un secondo fattore di autenticazione.
L'autenticazione viene quindi ottenuta provando il possesso e il controllo della chiave. Questo sistema è basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato II del Regolamento 910/2014.

Appendice D – Usabilità e Accessibilità

Per lo sviluppo dell'interfaccia utente, i fornitori di servizi e i gestori delle identità digitali devono garantire:

- l'usabilità ovvero la facilità d'uso come
    - la presentazione delle informazioni e delle scelte in modo chiaro e conciso, la mancanza di ambiguità e il posizionamento di elementi importanti in aree appropriate
    - la garanzia del funzionamento su diversi dispositivi e browser secondo lo stato dell'arte della tecnologia.
- l'accessibilità per tutelare il diritto di accesso ai servizi informatici e telematici della pubblica amministrazione da parte dei disabili in coerenza con Legge n. 4 del 9 gennaio 2004, aggiornato dal DM 20 marzo 2013, e le indicazioni Web Accessibility Initiative (WAI) del World Wide Web Consortium (W3C).

Al fine di ricondurre a una *user experience* comune per tutti gli utenti, limitandone l'eventuale disorientamento nell'accesso tramite diversi gestori dell'identità digitale, l'interfaccia del percorso di iscrizione (sign up) presso i gestori di identità digitale, nonché del login per l'accesso ai fornitori di servizi, sarà unica per tutti i gestori, fatto salvo lo spazio predisposto per la visualizzazione del proprio logo.

Nella sezione SPID del sito AgID saranno pubblicati tutti gli aggiornamenti e le linee guida relative alle interfacce di autenticazione e gestione della registrazione con le ulteriori indicazioni necessarie per garantire una omogenea *user experience*.