Agenzia per l'Italia Digitale
*Presidenza del Consiglio dei Ministri*

# SPID

## MODALITÀ ATTUATIVE

# Sommario

## Indice delle tabelle

# Normativa e standard di riferimento

[1] CAD – Codice Amministrazione Digitale - D.Lgs. 7 marzo 2005 n. 82 e s.m.i. (aggiornamento 11-11-2013)

[2] Codice in materia di protezione dei dati personali – D.Lgs. 30 giugno 2003 n. 196

[3] DPCM del 29-10-2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014): Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

[5] ISO-IEC 18014 Time-stamping

[6] ISO-IEC 19790:2012 Security requirements for cryptographic modules

[7] ISO-IEC 24760-1 A framework for identity management -- Part 1: Terminology and concept

[8] ISO-IEC 27001 - Information security management

[9] ISO-IEC 29003 Identity proofing

[10] ISO-IEC 29100 Basic privacy requirements

[11] ISO-IEC 29115:2013 Entity authentication assurance framework

[12] ITU-T X.1254 Entity Authentication Framework

[13] ITU-T Recommendation X.1252 (2010) Baseline identity management terms and definitions

[14] NIST 800-63-2 Electronic Authentication Guideline

[15] FIPS PUB 140-2 Security requirements for cryptographic modules

# Terminologia e concetti

## Termini e definizioni

Sono di seguito elencate le definizioni ed i termini utilizzati nella stesura del presente documento. Per i termini definiti dal CAD e dal DPCM si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato anche il termine inglese corrispondente, generalmente usato in letteratura tecnica e negli standard.

**Adesione:** è il primo passaggio del processo di iscrizione, dove una entità aderisce a SPID fornendo tutti i dati e la documentazione necessaria;

**Attributi identificativi:** nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d' identità utilizzato ai fini dell'identificazione;

**Attributi secondari:** il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni;

**Autenticazione multi-fattore:** autenticazione con almeno due fattori di autenticazione indipendenti (ISO-IEC 19790);

**Autenticazione:** disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2);

**Codice identificativo:** il particolare attributo assegnato dal gestore dell'identità' digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID;

**Credenziale:** un insieme di dati presentati come evidenza dell'identità dichiarata/asserita o di un proprio diritto (ITU-T X.1252), in pratica il Titolare/utente si avvale di questo attributo (a singolo o doppio fattore) unitamente al codice identificativo (entrambi rilasciati dal gestore dell'identità digitale) per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi (Amministrazioni e privati) che aderiscono allo SPID;

**Entità:** può essere una persona fisica o un soggetto giuridico;

**Fattore di autenticazione:** elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità (ISO-IEC 19790);

**Fonte Autoritativa:** in generale un repository riconosciuto come sorgente aggiornata ed accurata delle informazioni (ISO-IEC 29003);

**Fornitore di servizi:** il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita;

**Gestori dell'identità digitale:** le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti;

**Gestori di attributi qualificati:** i soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi;

**Giornale di controllo:** consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche;

**Identità digitale:** la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale;

**Iscrizione:** il processo che, partendo dall'iniziale adesione e a seguito delle fasi di dimostrazione e validazione, si completa con la registrazione con esito positivo della nuova identità digitale e con il rilascio delle credenziali. (ISO-IEC 29003);

**OTP:** una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione;

**Protocollo di autenticazione:** sequenza definita di messaggi fra una entità e il verificatore allo scopo di consentire al verificatore di autenticare l'entità;

**Registro SPID:** registro, tenuto dall'Agenzia, accessibile al pubblico, contenente l'elenco dei soggetti abilitati a operare in qualità di gestori dell'identità' digitale, di gestori degli attributi qualificati e di fornitori di servizi;

**Richiedente:** è la persona fisica che effettua l'adesione. Se la persona fisica non è l'entità (v. soggetto giuridico), essa deve avere titolarità o procure per agire per conto dell'entità;

**Salt:** una sequenza casuale di bit utilizzata assieme ad una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti;

**SPID:** il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98;

**Titolare:** è il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v);

**User Agent:** sistema utilizzato dall'utente per l'accesso ai servizi (di solito il browser per la navigazione in rete);

**Verificatore:** il soggetto attore, nel caso SPID il gestore delle identità digitali, che conferma e avvalora le informazioni di identità;

## Abbreviazioni e acronimi

**Agenzia** (anche AgID) – Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali)

**BCP** – Best Current Practice (IETF)

**EAA** Entity Authentication Assurance

**ETSI** – European Telecommunications Standards Institute

**DPCM** - DPCM del 29-10-2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014): Definizione delle Caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

**ICT** Information and Communications Technology

**IdM** Identity Management

**IDP** Identity Provider (il gestore delle identità digitali in ambito SPID)

**IEEE** – Institute of Electrical and Electronics Engineers

**IETF** – Internet Engineering Task Force

**IP** Internet Protocol

**IPV** Identity Proofing and Verification

**IS** International Standard

**ISO/IEC** – International Organization for Standardization/International Electrotechnical Commission

**ITU-T** –International Telecommunication Union, Telecommunication Standardization Sector

**LoA** Level of Assurance

**NIST** - National Institute of Standards and Technology

**PII** Personally Identifiable Information

**SAML** Security Assertion Markup Language

**SSL** Secure Socket Layer

**TCP** Transmission Control Protocol

**TLS** Transport Layer Security

**URL** Uniform Resource Location

# 1 Premessa

Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia, secondo modalità definite nel DPCM, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni o dei soggetti privati che aderiranno al sistema, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati. SPID sarà adottato dalle pubbliche amministrazioni (come da art. 2 comma 2 del CAD), entro i ventiquattro mesi successivi all'accreditamento del primo gestore dell'identità digitale (art. 14 comma 2 del DPCM); inoltre e ai fini dell'erogazione dei propri servizi in rete, le imprese (art. 15 del DPCM), hanno la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti[1].

Il sistema SPID ha lo scopo principale di definire un ambiente sicuro, efficace ed economico per consentire l'accesso, per i cittadini e le imprese, ai servizi offerti da tutte le amministrazioni pubbliche (e dai fornitori di servizi aderenti al sistema) in modalità telematica in coerenza con una strategia che privilegia il digitale per default.

Il modello segue un approccio federato per la fornitura dei servizi di identità digitale in modo da (a) consentire ai cittadini e alle imprese di scegliere autonomamente il gestore delle identità digitale certificato e (b) creare un mercato libero e competitivo che stimoli una concorrenza virtuosa ed un continuo miglioramento delle soluzioni tecnologiche e dei sistemi.

Ai sensi del comma 2-ter dell'art. 64 del CAD [1] SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite nel DPCM [3] e nei regolamenti ivi previsti, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati. Al fine dell'omogeneità del sistema anche nei confronti del Cittadino è necessario che identity provider e service provider seguano gli stessi elementi identificativi sia nelle procedure di riconoscimento ed assegnazione delle credenziali sia per l'accesso ai servizi.

[1] L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

Questa guida descrive le modalità attuative di SPID includendo le fasi di accreditamento e di adesione, il ciclo di vita completo delle identità digitali e credenziali associate, il processo di autenticazione e la necessaria componente di gestione e supervisione.

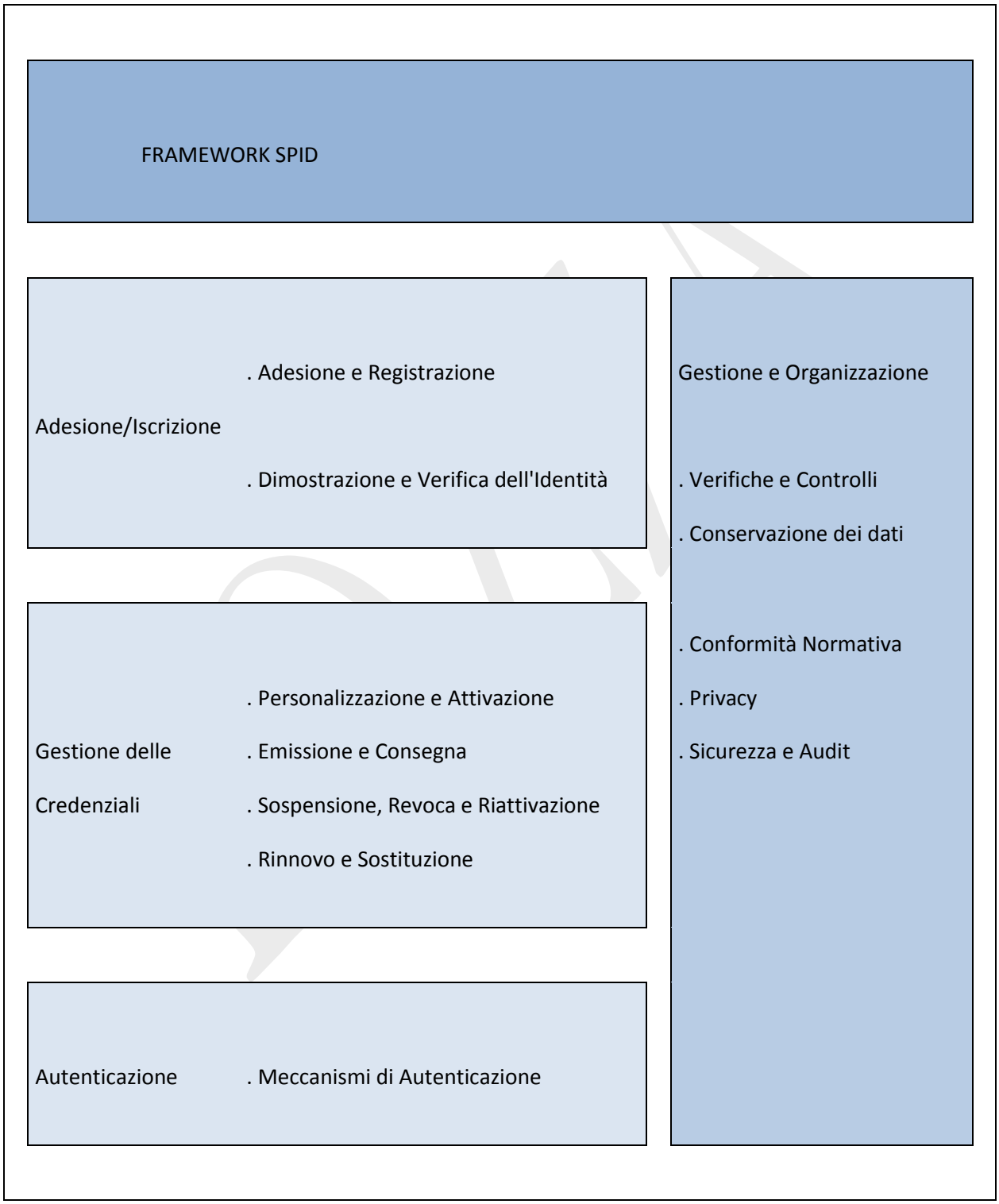



**Tabella 1 - Framework SPID**

# 2 Ambito di applicazione

Il presente documento stabilisce, ai sensi dell'art. 4 comma 2 del DPCM, le modalità attuative per la realizzazione dello SPID.

Il modello SPID prevede la separazione delle funzioni di identificazione (di competenza dei gestori dell'identità digitale) dalle funzioni di attestazione e autenticazione degli attributi qualificati (di competenza dei gestori di attributi qualificati).

Lo SPID è basato su tre livelli di sicurezza di autenticazione informatica, adottati in funzione dei servizi erogati e della tipologia di informazioni rese disponibili:

- livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115) prevede sistemi di autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato adeguato 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.

- livello 2 (corrispondente al LoA3 dell'ISO-IEC 29115) prevede, invece, un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi che possono subire un danno consistente da un utilizzo indebito dell' identità digitale.

- livello 3 (corrispondente al LoA4 dell'ISO-IEC 29115) prevede un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi conformi ai requisiti dell' Allegato 3 della Direttiva 1999/93/CE; 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.

In ambito SPID, i fornitori di servizi (PA e imprese aderenti) che erogano servizi qualificati devono seguire un metodo di gestione iterativo composto da quattro fasi come dallo schema sotto illustrato.

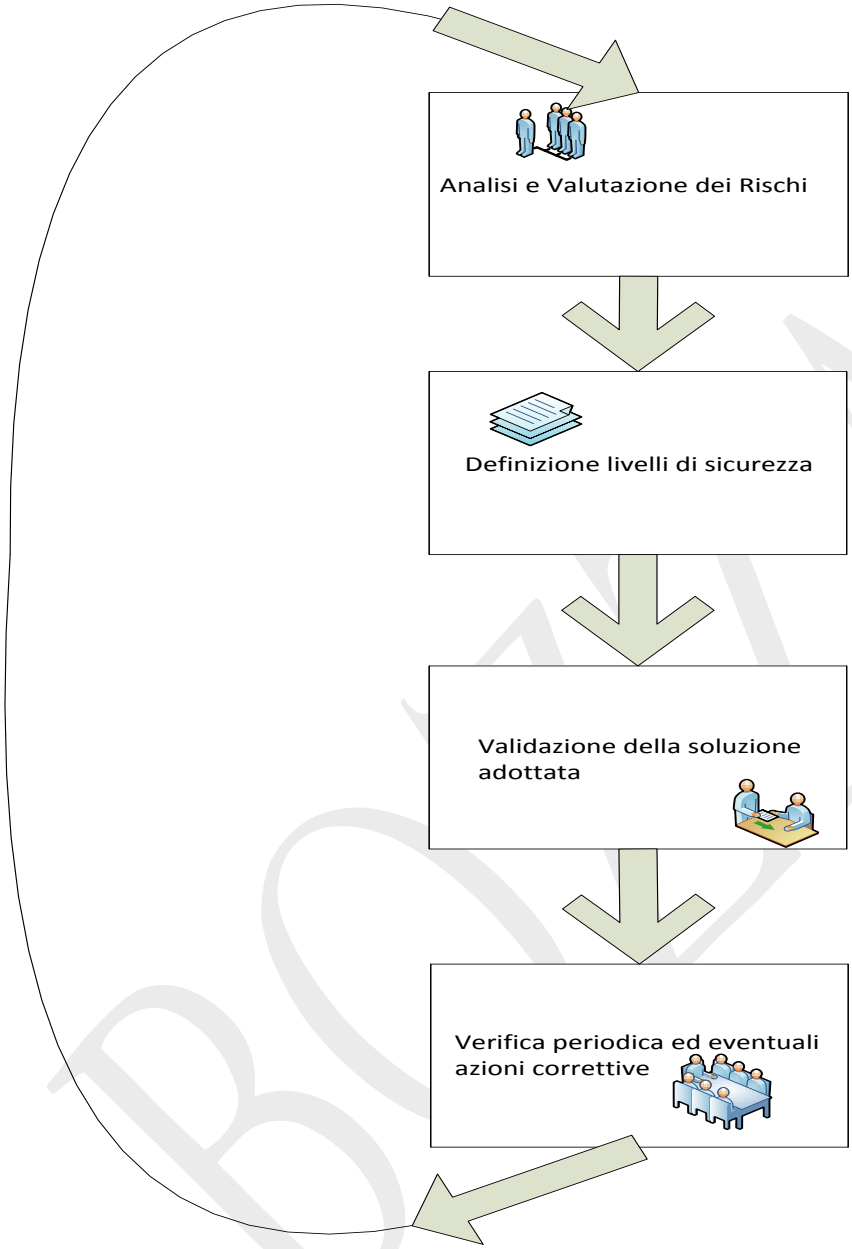



**Figura 1 - SP Flusso di gestione**

In particolare, questo documento fornisce le linee guida e le modalità attuative per la seconda fase allo scopo di definire adeguati livelli di sicurezza di autenticazione informatica e di conseguenza selezionare i sistemi, i servizi e le tecnologie.

Per ciascuno dei tre livelli di sicurezza di autenticazione informatica sono indicati i requisiti e le modalità per:

- la registrazione, dimostrazione e validazione delle identità digitali (IPV Identity proofing and validation);
- credenziali (ad uno o a doppio fattore) usati per l'autenticazione;
- meccanismi di gestione delle credenziali;
- protocolli utilizzati per effettuare l'autenticazione tra il richiedente e il verificatore (gestore delle identità digitali o il gestore degli attributi qualificati);
- meccanismi di asserzione utilizzati per comunicare i risultati dell' autenticazione remota.

Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione Europea dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata nella *Gazzetta Ufficiale* dell'Unione Europea, Serie L, n. 13 del 19 gennaio 2000, è consentito di circolare liberamente nel mercato interno.

## 2.1 Modalità di associazione LoA (livelli di autenticazione informatica SPID)

Il processo di autenticazione è diretto alla verifica dell'identità digitale basandosi sull'attendibilità delle credenziali presentate, ad es. una password, rispondendo alla semplice domanda: "Quanto sono sicuro che tu sei veramente quello che tu affermi di essere ?". In altre parole, quale livello di fiducia può essere assegnato dalla parte (normalmente un fornitore di servizi) in relazione al fatto che le credenziali presentate siano effettivamente nel pieno possesso della persona di cui viene asserita l'identità.

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.

La scelta di un adeguato livello di sicurezza (LoA) deve essere fondamentalmente basata sulle conseguenze derivate da un errore di autenticazione e/o un uso improprio delle credenziali; livelli di sicurezza (LoA) più alti saranno associati a quei sistemi/applicazioni/sistemi che comportano conseguenze ed impatti più significativi (come il trattamento di dati sensibili o dati relativi a reddito o patrimonio) mentre richieste a carattere informativo, e di basso contenuto, possono essere associate a livelli più bassi.

La metodologia suggerita dall'Agenzia, prevede l'identificazione dei rischi per ogni specifico sistema/applicazione/servizio e l'associazione ai livelli di sicurezza previsti in ambito SPID, ovviamente l'assegnazione del potenziale impatto (basso, moderato, alto) di questi rischi dipende dallo specifico contesto e dalle entità coinvolte da impropria autenticazione.

Il livello di assegnazione SPID è determinato dal livello più alto di una qualsiasi categoria di potenziale impatto, ad esempio se cinque categorie di potenziale impatto sono a livello 1 ed una sola è a livello 2 allora deve essere scelto il livello di sicurezza 2 di SPID.

La tabella seguente fornisce una sintesi delle associazioni impatti potenziali – rischio – livello di sicurezza SPID.

| | **Impatto potenziale massimo di eventi per ogni livello di sicurezza SPID** | | |
|---|---|---|---|
| **Impatto causato da un errore di autenticazione** | **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 | Basso | Moderato | Alto |
| Potenziale danno per rilascio di informazioni sensibili | 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 | N/A | Basso | Moderato/Alto |

**Tabella 2 - 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. |

**Tabella 3 - Definizione valore impatto**

Ulteriori considerazioni possono essere fatte in relazione alla classificazione dei dati secondo lo schema riportato in tabella :

| **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 | Livello 1 è adeguato per utenti sono iscritti ad un sito ma senza la possibilità di eseguire operazioni dispositive. | Esempio 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 di cui sono soggetti, o per utenti che per motivazioni professionali possono accedere ad 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. |

**Tabella 4 - 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.

# 3 Accreditamenti – Convenzioni - Adesioni

L'Agenzia gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni.

L'Agenzia cura l'aggiornamento del registro SPID e vigila sull'operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate.

L'Agenzia stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità. A tali convenzioni i gestori dell'identità digitale e i gestori degli attributi qualificati sono tenuti ad aderire.

Tutti i fornitori di servizi, che hanno aderito allo SPID stipulando una convenzione con l'Agenzia osservano gli obblighi indicati all'art. 13 del DPCM [3].

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

Possono aderire allo SPID come fornitori di servizi anche i soggetti privati che soddisfano quanto indicato all'art. 15 comma 1 del DPCM [3] .

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 come da art. 6 comma 4 e 5 del DPCM [3] .

## 3.1 Gestori dell'Identità Digitale

I soggetti che rispettano i requisiti indicati all'art.10 comma 3 del DPCM [3] presentano domanda di accreditamento all'Agenzia .

La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

Il termine di novanta giorni, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità dell'Agenzia o che essa non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

Ai sensi dell'art. 6 comma 2 del DPCM [3] , l'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello, i criteri per la valutazione dei sistemi di autenticazione informatica e la loro assegnazione al relativo livello di sicurezza SPID.

Come da art. 6 comma 3 del DPCM [3] i gestori dell'identità digitale devono adottare soluzioni di autenticazione informatica che non richiedono ai fornitori di servizi di dotarsi di dispositivi, fissi o mobili, proprietari.

A seguito dell'accoglimento della richiesta, l'Agenzia stipula apposita convenzione e dispone l'iscrizione del richiedente nel registro SPID, consultabile in via telematica.

Il soggetto accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche Amministrazioni.

Il gestore dell'identità digitale deve rispettare tutti gli obblighi previsti nella convenzione stipulata con l'Agenzia anche ai sensi dall'art. 11 del DPCM [3] .

L'Agenzia procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la permanenza della sussistenza dei requisiti previsti dal DPCM [3]. Se, all'esito dei controlli, accerta la mancanza dei requisiti richiesti per l'iscrizione nel registro SPID, decorso il termine fissato per consentire il ripristino degli stessi, l'Agenzia, con provvedimento motivato notificato all'interessato, può adottare le azioni previste dall'art. 12 comma 4.

La tabella seguente sintetizza tutti i passaggi necessari:

| |
|---|
| I soggetti che rispettano i requisiti indicati all'art.10 comma 3 del DPCM [3] presentano domanda di accreditamento[2] all'Agenzia . |
| (A) Requisiti soddisfatti: domanda di accreditamento accolta. |
| (B) L'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello SPID (ai sensi dell'art. 6 comma 2 del DPCM [3] ) |

[2] Documentazione per accreditamento (attualmente disponibile in bozza sul sito AGID) http://www.agid.gov.it/sites/default/files/circolari/bozza_documentazione_per_accreditamento_idp_20141020_v.0.3.pdf

| |
|---|
| (C) I gestori dell'identità digitale devono adottare soluzioni di autenticazione informatica che non richiedono ai fornitori di servizi di dotarsi di dispositivi, fissi o mobili, proprietari (anche ai sensi dell'art. 6 comma 3 del DPCM [3]). |
| L'Agenzia, se soddisfatte le condizioni (A), (B) e (C), stipula apposita convenzione e dispone l'iscrizione[3] del richiedente nel registro SPID. |
| L'Agenzia svolge controlli volti ad accertare la permanenza della sussistenza dei requisiti previsti dal DPCM [3] e se, all'esito dei controlli, accerta la mancanza dei requisiti richiesti per l'iscrizione nel registro SPID, decorso il termine fissato per consentire il ripristino degli stessi, l'Agenzia, con provvedimento motivato notificato all'interessato, può adottare le azioni previste dall'art. 12 comma 4. |

**Tabella 5 - Flusso per accreditamento**

## 3.2 Fornitori di servizi – PA

I fornitori di servizi che aderiscono allo SPID stipulano una convenzione con l'Agenzia osservano gli obblighi indicati all'art. 13 del DPCM [3] .

L'adesione allo SPID da parte delle pubbliche amministrazioni in qualità di fornitori di servizi è regolato come indicato all'art. 14 del DPCM [3] .

[3] Deve essere prevista ricezione del certificato assicurativo in luogo dell'impegno a stipulare polizza (v. schema di polizza presentato con la documentazione per l'iscrizione).

## 3.3 Fornitori di servizi - privati

I fornitori di servizi che aderiscono allo SPID stipulano una convenzione con l'Agenzia osservano gli obblighi indicati all'art. 13 del DPCM [3] .

L'adesione allo SPID da parte di soggetti privati fornitori di servizi è vincolato a quanto indicato all'art. 15 del DPCM [3] .

## 3.4 Gestori di Attributi Qualificati

I soggetti che hanno il potere, in base alle norme vigenti, di attestare gli attributi qualificati si accreditano presentando domanda all'Agenzia e indicano i dati che intendono rendere disponibili nello SPID.

L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui sopra comporta la cancellazione dal registro di gestore di attributi qualificati gestito dall'Agenzia.

Ai soggetti che hanno il potere di attestare gli attributi qualificati ed hanno sede stabile in altri Stati membri dell'Unione europea si applicano le norme di recepimento della direttiva 1999/93/CE.

La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

Il termine di novanta giorni, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità dell'Agenzia o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

A seguito dell'accoglimento della domanda, l'Agenzia dispone l'iscrizione del richiedente in un apposito registro. L'Agenzia ha il compito di gestire il registro, accessibile da parte dei fornitori di servizi, con le tipologie di dati resi disponibili da ciascun gestore di attributi qualificati.

Il soggetto accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche Amministrazioni.

Il gestore di attributi qualificati che attestano e rilasciano attributi qualificati è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

a. sull'esattezza e sulla completezza delle informazioni necessarie alla verifica dell'attributo qualificato;
b. sull'adempimento degli obblighi a suo carico (custodia e adozione di tutte le misure organizzative e tecniche idonee ad evitare danno a terzi).

Il gestore di attributi qualificati che attesta e rilascia attributi qualificati è responsabile, nei confronti dei terzi che facciano affidamento sull'attributo stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione dell'attributo qualificato, salvo che provi d'aver agito senza colpa.

L'Agenzia svolge funzioni di vigilanza e controllo sull'attività dei gestori di attributi qualificati.

Su richiesta degli interessati, sono accreditati di diritto i seguenti gestori di attributi qualificati:

a. il Ministero dello sviluppo economico in relazione ai dati contenuti nell'indice nazionale degli indirizzi PEC delle imprese e dei professionisti di cui all'art. 6-bis del CAD;
b. i consigli, gli ordini e i collegi delle professioni regolamentate relativamente all'attestazione dell'iscrizione agli albi professionali;
c. le camere di commercio, industria, artigianato e agricoltura per l'attestazione delle cariche e degli incarichi societari iscritti nel registro delle imprese;
d. l'Agenzia in relazione ai dati contenuti nell'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi di cui all'art. 57-bis del CAD.

# 4 Identità Digitali e Credenziali

L'adesione ed iscrizione al sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (SPID) , può essere suddivisa nei seguenti processi:

- richiesta e accettazione
- dimostrazione dell'identità
- esame e verifica dell'identità
- emissione della identità digitale e credenziali
- conservazione e registrazione dei documenti

Fermo restando la responsabilità del gestore di identità digitale, in linea generale, questi cinque processi possono essere condotti interamente da una singola organizzazione o possono consistere di una molteplicità di rapporti e funzionalità fornite da diverse organizzazioni.

Nei paragrafi che seguono sarà fornita una descrizione puntuale di questi processi anche in relazione ai livelli di sicurezza, previsti in ambito SPID, di autenticazione informatica (LoA: level of assurance) associati all'identità digitale ed al fatto che l'entità richiedente può essere già in possesso di documenti digitali di identità (ad es. TS-CNS o carte ad esse conformi, altra identità digitale SPID o di validi sistemi informatici preesistenti) o di firma elettronica qualificata o digitale.

A completamento dei processi sopra elencati, deve essere prevista la gestione del ciclo di vita delle identità digitali e delle credenziali.

## 4.1 Processo di adesione/iscrizione

Il processo di richiesta di nuova identità digitale SPID include in primis la compilazione di un modulo di adesione che contiene tutte le informazioni necessarie e sufficienti per l'identificazione dell'entità richiedente all'interno del contesto in cui saranno successivamente utilizzate le credenziali associate all'identità digitale.

Nella richiesta di adesione/iscrizione sono contenuti sia i dati relativi all'identità del richiedente (attributi identificativi) che le informazioni (attributi secondari) che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali ed il sottoscrittore della identità digitale.

Sono considerate obbligatorie per le persone fisiche le seguenti informazioni:

| |
|---|
| Cognome e Nome |
| Sesso, data e luogo di nascita |
| Codice fiscale |
| Indirizzo di residenza |
| Estremi del documento di riconoscimento presentato per l'identificazione, ove presente, quali tipo, numero, ente emittente e data di rilascio e validità dello stesso |
| Gli attributi secondari così come definiti all'art. 1 comma d) del DPCM [3] per semplificare i processi di comunicazione tra il gestore dell'identità digitale ed il sottoscrittore del servizio. |

Sono considerate obbligatorie per le persone giuridiche le seguenti informazioni:

| |
|---|
| Denominazione/Ragione Sociale |
| Codice fiscale o P.IVA (se uguale al codice fiscale) |
| Indirizzo sede legale |
| Certificazione con indicazione Amministratori e/o rappresentanti legale (in alternativa atto notarile di procura legale) e data di rilascio e validità dello stesso |
| Copia ed estremi del documento di identità utilizzato dalla persona fisica |
| Gli attributi secondari così come definiti all'art. 1 comma d) del DPCM [3] per semplificare i processi di comunicazione tra il gestore dell'identità digitale ed il sottoscrittore del servizio. |

Il richiedente può fornire un altro nome (pseudonimo) che sarà inserito in un apposito campo del record associato all'identità digitale (questo campo, nel caso in cui non venisse fornito alcun ulteriore nome dal richiedente, sarà valorizzato con nome e cognome del richiedente stesso).

Come condizione minima per gli attributi secondari dovranno essere forniti almeno un indirizzo di posta elettronica ed un recapito di telefonia mobile che dovranno essere entrambi certificati dal gestore di identità digitale, ad esempio (a) inviando una mail all'indirizzo di posta elettronica dichiarato, con il link ad una url per la verifica e certificazione e (b) inviando un SMS al numero di cellulare con un codice numerico di controllo che deve essere riportato nel SMS di risposta.

L'entità richiedente assume la responsabilità, a norma della legislazioni vigente, delle informazioni richieste e ne è resa esplicitamente consapevole[4] prima di poter avviare il processo di iscrizione a SPID.

## 4.2 Dimostrazione dell'identità

Il processo della dimostrazione dell'identità consiste nell'acquisizione e accertamento di informazioni sufficienti ad identificare un'entità per uno specifico o inteso livello di sicurezza di autenticazione informatica in ambito SPID.

Ai sensi dell'art. 7 del DPCM [3], le identità digitali sono rilasciate, a domanda dell'interessato, dal gestore dell'identità digitale e la richiesta di adesione avviene nei modi seguenti:

1. Identificazione tramite esibizione a vista e acquisizione del modulo di adesione firmato:
    - se il soggetto richiedente è una persone fisica, di un valido documento d'identità (v. Appendice B) ; in questo caso gli attributi identificativi consistono di nome, cognome, luogo e data di nascita, estremi documenti di identità e codice fiscale.
    - se il soggetto richiedente è una persona giuridica, della procura attestante i poteri di rappresentanza; in questo caso gli attributi identificativi consistono di ragione o denominazione sociale, codice fiscale/partita iva.
2. Identificazione informatica (compilando, e sottoscrivendo elettronicamente, i moduli di adesione informatici posti a disposizione in rete dal gestore dell'identità digitale) nel caso in cui:
    a) il richiedente già possiede documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui TS-CNS, CNS o carte ad essa conformi;
    b) il richiedente è già in possesso di una identità digitale SPID di livello di sicurezza pari o superiore a quello oggetto della richiesta;
    c) il richiedente dispone di identificazione informatica fornita da sistemi informatici preesistenti all'introduzione dello SPID che risultino aver adottato, a seguito di apposita istruttoria dell'Agenzia, regole di identificazione informatica caratterizzate da livelli di sicurezza uguali o superiori a quelli definiti nel DPCM [3] .

[4] chiunque renda dichiarazioni mendaci è punibile ai sensi del codice penale e delle leggi speciali in materia (art. 76 del DPR 445/2000)

In questo caso il nuovo gestore delle identità digitali, considera che la fase di identificazione sia stata correttamente espletata dal gestore che ha precedentemente rilasciato un documento digitale di identità.

3. acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o digitale. 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.

Per l'acquisizione dei dati, e successiva validazione, dell'entità richiedente nei casi previsti al punto 2 e 3, il gestore di identità digitale si comporterà come un Service Provider nei confronti di un precedente Identity Provider (altro gestore di identità SPID, il gestore della CNS o gestore di identità con sistemi preesistenti ma equipollenti o superiori) o del fornitore di firma elettronica qualificata o digitale.

La tabella seguente illustra i requisiti minimi a cura del gestore delle identità digitali, e con l'ausilio di personale qualificato, che devono essere garantiti per soddisfare la corretta e sicura attuazione del processo.

| Livello di garanzia | Requisiti |
|---|---|
| Per tutti i livelli SPID | 1) rendere esplicitamente consapevole il richiedente del fatto che chiunque renda dichiarazioni mendaci è punibile ai sensi del codice penale e delle leggi speciali in materia (art. 76 del DPR 445/2000) |
| | 2) Assicurarsi che il richiedente sia consapevole dei termini e condizioni associati all'utilizzo del servizio di identità digitale. |
| | 3) Assicurarsi che il richiedente sia consapevole delle raccomandazioni e precauzioni da adottare per l'uso delle identità digitale. |
| | 4) Acquisire tutti i dati rilevanti di identità necessari alla dimostrazione di identità. |

**Tabella 6 - Requisiti minimi per acquisizione dati**

**Solo nel caso di richiesta di identità digitale con livello 1 e 2** di sicurezza di autenticazione informatica, l'identificazione della persona fisica può essere effettuata dal gestore dell'identità digitale in modalità remota. In questo caso sono richiesti, da parte del richiedente, il possesso di un PC collegato in rete, una webcam ad esso collegata e un sistema audio PC funzionante.

Il soggetto autorizzato e qualificato che effettua l'identificazione verifica l'identità del richiedente tramite il riscontro con documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile del Titolare, firma autografa del Titolare e di timbro, rilasciato da un'Amministrazione dello Stato e della tessera sanitaria/codice fiscale.

I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati come da art. 7 comma 8 e 9 del DPCM.

Per garantire qualità e sicurezza di tutto il processo, nel caso di identificazione remota devono essere abbinati rigorosi criteri di applicazione nelle fasi di esame e verifica delle identità e la consegna delle credenziali deve essere effettuata con modalità e strumenti che assicurino che la consegna sia effettuata al legittimo destinatario con criteri di riservatezza, salvaguardando il contenuto.

In ogni caso, *sia per l'identificazione remota che per quella di persona*, se i documenti utilizzati dal richiedente risultano carenti delle caratteristiche elencate, deve esserne esclusa l'ammissibilità ed il processo di iscrizione deve essere sospeso o bloccato fino alla esibizione di documenti validi ed integri.

In **Appendice B** è riportato un elenco di documenti d'identità secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445.

## 4.3 Esame e verifica delle identità

Questo è il processo di controllo delle informazioni confrontando i dati forniti con informazioni precedentemente convalidate ed il legame con il soggetto richiedente.

Sia il processo di dimostrazione dell'identità che il processo di verifica sono eseguiti allo scopo di ottenere un garantito livello di sicurezza dell'identità del soggetto richiedente prima di procedere alla registrazione come specifica entità.

La verifica dell'identità differisce dalla dimostrazione dell'identità in quanto implica la convalida delle informazioni di identità attraverso sorgenti addizionali - fonti autoritative, in particolare utilizzando prioritariamente i servizi di cui all'articolo 4, comma 1, lettera c) del DPCM [3] (v. convenzioni dell'Agenzia) 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.

Nelle more del completamento del progetto Anagrafe Nazionale della Popolazione Residente (ANPR), i gestori dell'identità digitale ed i gestori degli attributi qualificati, per le sole finalità di verifica dell'esattezza dei dati personali del titolare dell'identità digitale, usufruiscono del servizio di verifica del codice fiscale e dei dati anagrafici ad esso strettamente correlati fornito, in cooperazione applicativa, dall'Agenzia delle Entrate.

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 |

**Tabella 7 - 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 il titolare dell'identità dichiarata e (3) che il richiedente non può successivamente disconoscere la registrazione.

La tabella seguente rappresenta i requisiti per il livello di garanzia (in questo caso è lo stesso per tutti i livelli SPID) in relazione alle prove identità e alla verifica di una persona fisica (v. sottoscrizione cittadino).

| Livello di garanzia | Requisiti |
|---|---|
| Per il livello 1 SPID | 1) Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata (per il livello 1 è previsto anche identificazione remota via webcam)<br><br>2) Le evidenze sono tutte valide ed emesse correttamente in accordo a quanto riportato da fonti autoritative (articolo 4, comma 1, lettera c del DPCM o, in assenza di convenzioni dell'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)<br><br>3) E' verificata l'esistenza, attraverso le fonti autoritative, dell'esistenza dell'identità dichiarata e che non è intervenuto decesso.<br><br>4) Il richiedente viene identificato usando le informazioni ottenute dalla fonti autoritative: Agenzie delle Entrate, ANPR ecc. |
| Per il livello 2 SPID | 1) Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata. (per il livello 2 è previsto anche identificazione remota via webcam)<br><br>2) Le evidenze sono tutte valide ed emesse correttamente in accordo a quanto riportato da fonti autoritative (articolo 4, comma 1, lettera c del DPCM o, in assenza di convenzioni dell'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)<br><br>3) E' verificata l'esistenza, attraverso le fonti autoritative, dell'esistenza dell'identità dichiarata e che non è intervenuto decesso.<br><br>4) Il richiedente viene identificato usando le informazioni ottenute dalla fonti autoritative: Agenzie delle Entrate, ANPR ecc.<br><br>5) Con specifico riferimento al Furto d'Identità: deve essere previsto la consultazione della Gestione dell'Archivio Centrale Informatizzato |
| Per il livello 3 SPID | 1) Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata. (in questo caso l'identificazione deve essere effettuata |

| | |
|---|---|
| | esclusivamente di persona)<br><br>2) Le evidenze sono tutte valide ed emesse correttamente in accordo a quanto riportato da fonti autoritative (articolo 4, comma 1, lettera c del DPCM o, in assenza di convenzioni dell'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)<br><br>3) E' verificata l'esistenza, attraverso le fonti autoritative, dell'esistenza dell'identità dichiarata e che non è intervenuto decesso.<br><br>4) Il richiedente viene identificato usando le informazioni ottenute dalla fonti autoritative: Agenzie delle Entrate, ANPR ecc.<br><br>5) Con specifico riferimento al Furto d'Identità: deve essere previsto la consultazione della Gestione dell'Archivio Centrale Informatizzato[5] |

**Tabella 8 -Requisiti da soddisfare/Livelli di sicurezza SPID (persona fisica)**

La tabella seguente rappresenta i requisiti per il livello di garanzia (anche in questo caso è lo stesso per tutti i livelli SPID) in relazione alle prove identità e alla verifica di una persona giuridica (v. sottoscrizione imprese).

| Livello di garanzia | Requisiti |
|---|---|
| Per tutti i livelli SPID | 1) L'esistenza della persona giuridica è basato su evidenze riconosciute dal sistema delle imprese in ambito nazionale.<br><br>2) Le evidenze sono tutte valide ed emesse correttamente in accordo a quanto riportato da (fonti autoritative)*. |

[5] La titolarità del Sistema di prevenzione è assegnata al Ministero dell'economia e delle finanze, mentre la realizzazione e la gestione dell'Archivio centrale sono affidati a Consap, con rapporto disciplinato da apposita Convenzione del 22 luglio 2013.

| | |
|---|---|
| | 3) E' verificata l'esistenza, attraverso le fonti autoritative, dell'identità dichiarata ed il suo stato giuridico è noto.<br><br>4) La fase successiva è l'associazione di una persona fisica, amministratore o rappresentante legale, all'impresa-persona giuridica. Questo richiede un ulteriore esame come indicato nella tabella precedente per l'identificazione di una persona fisica. |

**Tabella 9 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)**

In generale sono necessari un set di dati, prove e verifiche per le persone fisiche e un set di dati, prove e verifiche per le persone giuridiche; quando una persona fisica rappresenta una persona giuridica è necessario una combinazione di questi due insiemi di dati con altre informazioni (ad es. procura legale, visura camerale) relative alla natura di tale rappresentazione.

## 4.4 Conservazione e registrazione dei documenti

Questo processo completa la fase di iscrizione di una entità al sistema pubblico per la gestione dell'identità SPID; i documenti includono tutte le informazioni e la documentazione che è stata raccolta (e può essere conservata), le informazioni relative al processo di verifica, i risultati di queste procedure ed altri dati pertinenti.

I gestori dell'identità digitale, al fine di poter documentare la corretta attribuzione della stessa, conservano:

1. nel caso di identificazione tramite esibizione a vista:
    a. copia per immagine di tutta la documentazione esibita (documento d'identità per persone fisiche, procura per persone giuridiche) *e nel caso di identificazione remota via webcam tutti i dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico*
    b. modulo di adesione cartaceo/firmato *o modulo di adesione informatico sottoscritto digitalmente* (*ad es. con firme qualificate valide solo per la sessione in corso o per un periodo limitato*).
2. nel caso di identificazione informatica
    a. log della transazione

*b.* modulo di adesione informatico sottoscritto elettronicamente *o digitalmente (ad es. con firme qualificate valide solo per la sessione in corso o per un periodo limitato)*

3. nel caso di firma elettronica qualificata o digitale

   a. modulo di adesione allo SPID sottoscritto digitalmente

oltre a tutti i documenti e dati utilizzati per l'associazione e la verifica degli attributi.

La decisione viene quindi resa e registrata per accettare, rifiutare o segnalare l'iscrizione per ulteriori controlli o approfondimenti.

Tutta la documentazione inerente al processo di adesione deve essere conservata e trattata come indicato all'art. 7 comma 8 e 9 del DPCM.

## 4.5 Emissione della identità digitale

L'identità digitale è composta da un identificativo e dalle credenziali.

L'identificativo deve essere univoco nel dominio del gestore dell'identità digitale e in ambito SPID.

Allo scopo il gestore dell'identità digitale dovrà definire, nell'ambito del proprio dominio, un <**account-ID**> composto dall'indirizzo di posta elettronica dichiarato dal titolare dell'identità digitale (o in alternativa un nuovo[6] indirizzo di posta elettronica rilasciato dal gestore delle identità digitali).

All' <**account-ID**> deve essere associato con relazione biunivoca, un identificatore univoco ID-SPID composto nel modo seguente:

<**ID-SPID**> = <**cod_IdP**><**numero unico**><**suffisso**>

dove

<**ID-SPID**>: è un codice composto da 3 lettere

<**numero unico**>: è un numero composto da 12 cifre

<**suffisso**> : campo libero alfanumerico di 4 caratteri *(da utilizzare come campo di controllo o per sviluppi futuri)*

[6] In questo caso il gestore delle identità digitali deve garantire l'inoltro automatico di tutte le mail ricevute su questo nuovo indirizzo, all'indirizzo di posta elettronica dichiarato dall'entità richiedente.

La fase di gestione delle credenziali comprende tutti i processi relativi alla gestione del ciclo di vita delle credenziali, o mezzi usati per la loro produzione.

Questa fase può comprendere i seguenti processi:

1. creazione delle credenziali
2. emissione delle credenziali o dei mezzi usati per la loro produzione
3. attivazione delle credenziali o dei mezzi usati per la loro produzione
4. conservazione, revoca e/o distruzione delle credenziali o mezzi usati per la loro produzione
5. rinnovo e/o sostituzione delle credenziali o mezzi usati per la loro produzione
6. conservazione dei documenti

Qualcuno dei processi sopra elencati può essere influenzato dal fatto che le credenziali siano rese operative attraverso l'ausilio di un dispositivo hardware.

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 |

**Tabella 10 - Minacce/Processo di emissione**

### 4.5.1 Creazione/produzione delle credenziali

Il processo di creazione delle credenziali comprende tutte le attività necessarie a creare, per la prima volta, una credenziale o i mezzi per la sua produzione.

In alcuni casi le credenziali, o i mezzi usati per loro produzione, richiedono una fase di pre-elaborazione (come personalizzazioni dell'identità) prima della loro emissione.

In questi casi la personalizzazione può avere differenti formati in relazione alla tipologia di credenziale da emettere, per 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 dell'entità 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 in modo da 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 necessarie al successivo supporto per la generazione della firma digitale. 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 l'entità per la quale viene emessa. Come tale associazione viene ottenuta e con quale legame di affidamento tra credenziale ed entità dipende essenzialmente dal livello di sicurezza, previsti in ambito SPID, di autenticazione informatica (LoA: level of assurance) associato all'identità digitale. Ad esempio, in uno scenario online il legame entità richiedente e identificativo può essere realizzato al primo utilizzo con un "codice iniziale" durante la sessione di attivazione su un canale di comunicazione protetto. In alternativa, il codice di attivazione può essere richiesto alla fine del processo di associazione entità richiedente – identificativo.

Per le credenziali composte da un singolo fattore (ad es. password) e non generate in modo completamente casuale, si raccomanda l'adozione di policy come da best practices e la garanzia di un adeguato valore di entropia informativa associata alla credenziale *(in generale è considerato ottimale un valore di entropia non inferiore a 30 ma questo valore può variare in relazione alla durata della password e per specifici contesti applicativi/servizi).*

In particolare in relazione al tipo della password si raccomanda di adottare le seguenti regole di complessità:

- lunghezza minima di otto caratteri
- uso di caratteri maiuscoli e minuscoli
- inclusione di uno o più caratteri numerici
- inclusione di almeno un carattere speciali ad es #, $,% ecc.
- non deve contenere più di due caratteri identici consecutivi

E vietare, o almeno dissuadere dall'uso di formati comuni (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.)

Le password devono avere una durata massima ( 90 giorni in caso di trattamento di dati sensibili o giudiziari e comunque 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) ed in particolare per quanto indicato 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.

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 con l'ausilio di un dispositivo fisico, l'invio di un SMS, liste-tabelle predefinite o applicazioni mobile per smartphone; 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.

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 conformi ai requisiti dell' Allegato 3 della Direttiva 1999/93/CE.

In generale per le credenziali a doppio fattore viene normalmente utilizzato un 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).

- di tipo software: le informazioni necessarie risiedono direttamente nel computer dell'utente, 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 e 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 verificatore 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.

### 4.5.2 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. |

**Tabella 11 - 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, il consenso 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. |
| Phising o pharming | L'utente viene ingannato e crede che l'aggressore sia il fornitore di servizi o di identità (sito civetta). | DNS re-reouting. Una password viene rivelata ad un sito civetta che simula l'originale. |
| Ingegneria sociale | L'aggressore stabilisce un livello di fiducia 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 verificatore online e prova ad indovinare il token valido. | Attacchi online basati su dizionari o password note. |

**Tabella 12 - 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. |
| Phising 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. |

**Tabella 13 - 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.

### 4.5.3 Consegna delle credenziali

Anche in questo caso, la complessità del processo dipende dal livello di sicurezza , previsti in ambito SPID, di autenticazione informatica (LoA: level of assurance) associati all'identità digitale.

Per alti livelli di sicurezza deve essere previsto una "consegna di persona" del dispositivo hardware (ad es. smart card, token ecc.) che contiene le credenziali, per livelli più bassi può essere sufficiente inviare una password o PIN direttamente all'indirizzo fisico (via posta raccomandata) o al domicilio elettronico (posta elettronica, PEC).

Il gestore delle identità digitali è tenuto a garantire:

1. che il Titolare sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali;

2. che il Titolare sia informato in modo compiuto e chiaro sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;

3. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196.

### 4.5.4 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 fortemente 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 previsto 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 sua validità è stata temporaneamente annullata.

## 4.6 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 ed alle applicazioni autorizzate.

Questi file non devono mai contenere le password in chiaro; allo scopo possono essere usate tecniche, come da standard internazionali ed approvate dall'Agenzia, di crittografia o algoritmi di salt e hashing (una sequenza casuale di bit viene utilizzata assieme ad una password come input a una funzione di hash unidirezionale).

In questo modo nei file delle credenziali viene conservato l'output della funzione di crittografia o di hash applicata alla password e, di conseguenza, si ottiene una buona protezione da eventuali attacchi o furti di password.

A livello 2 e 3 SPID, vale tutto quanto indicato a livello 1 con i necessari allineamenti e conformità agli standard ed alla normativa vigente per i moduli crittografici e di sicurezza software/hardware (v. ISO 19790 [6] e FIPS 140-2 [15]).

## 4.7 Gestione del ciclo di vita dell'identità digitale

### 4.7.1 Gestione attributi

Il titolare dell'identità digitale può aggiornare, assumendone la responsabilità a norma della legislazioni vigente, i seguenti attributi identificativi:

a. Per le persone fisiche:
   - indirizzo di residenza
   - estremi del documento di riconoscimento (e nuova scadenza)
   - pseudonimo
b. Per le persone giuridiche:
   - indirizzo sede legale
   - codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
   - persona fisica (amministratore o rappresentante legale della società)

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

In una logica che privilegia la strategia digitale per default, le modalità operative per gli aggiornamenti devono essere rese possibili attraverso un'area web dedicata del gestore delle identità digitali seguendo criteri di autenticazione basati sulle credenziali in possesso del titolare.

A valle del processo di acquisizione, il gestore delle identità digitali deve seguire le fasi di esame e verifica in relazione al livello SPID associato all'identità digitale e come descritto nel precedente par. 4.3.

Il record aggiornato e associato all'identità digitale sarà effettivo solo a validazione completata con successo.

La richiesta di aggiornamento e l'effettivo aggiornamento devono essere notificati al titolare dell'identità digitale utilizzando un attributo secondario funzionale alle comunicazioni (ad es. l'indirizzo di posta elettronica se non è stato modificato durante la sessione di aggiornamento).

Il gestore delle identità digitale deve pure prevedere un servizio di help desk telefonico e di assistenza presso i centri presenti nel territorio.

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.).

### 4.7.2 Cancellazione/Revoca

Ai sensi dell'art. 8, comma 3 e art. 9 del DPCM, il gestore dell'identità digitale 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

I casi indicati ai punti 1 e 4 sono trattati al paragrafo 4.8.1 relativo alla sospensione/ revoca delle credenziali.

Per i casi previsti ai punti 2 e 3, il gestore delle identità digitali utilizza i servizi messi a disposizione dalle convenzioni di cui all'art. 4, comma 1, lettera c) del DPCM [3] .

In assenza di servizi equivalenti messi a disposizione dalle convenzioni, sarà cura del soggetto titolare (eredi o procuratore, amministrazione, società subentrante) presentare formalmente tutta la documentazione necessaria all'accertamento per la cessata sussistenza dei presupposti per l'esistenza della credenziale e il gestore dell'identità, in possesso di questa documentazione, dovrà procedere tempestivamente alla revoca e cancellazione.

Nel caso di cancellazione/revoca di una identità digitale primaria (una identità utilizzata per richiedere successivamente altre identità digitali dallo stesso o altro gestore di identità digitali) devono essere

previsti meccanismi di revoca automatica di tutte le identità digitali derivate in modo da garantire l'assenza di identità digitali "orfane" .

## 4.8 Gestione del ciclo di vita delle credenziali

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:

- il fatto che la credenziale è stata creata
- l'identificativo della credenziale
- l'entità per la quale è stata emessa
- lo stato della credenziale

Opportuna documentazione e registrazione sarà mantenuta per ogni processo (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) incluso nella fase 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

### 4.8.1 Sospensione/Revoca

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

La revoca è necessaria nei casi seguenti:

1. smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria)
2. scadenza (per decorrenza contrattuale o validità del documento d'identità)
3. per un periodo di inattività superiore a 24 mesi
4. utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto
5. una differente credenziale è stata emessa in sostituzione della credenziale in questione (ad es. per upgrade tecnologici)

In particolare, per i casi previsti ai punti 2, 3 e 5 il gestore dell'identità digitale revoca automaticamente la credenziale ma devono essere previsti meccanismi con il quale il gestore comunica, con congruo avviso (almeno 30 giorni prima e successivamente 10 giorni, 5 giorni e il giorno precedente la revoca

definitiva), la causa e data della revoca al titolare dell'identità digitale utilizzando l'indirizzo di posta elettronica ed il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Nei casi previsti ai punti 1 e 4, anche a seguito di segnalazioni come da art. 8 comma 4 del DPCM l'utente richiede la sospensione immediata dell''identità digitale al gestore del servizio.

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 titolare dell'identità digitale.

Il gestore dell'identità digitale sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Durante questo periodo possono verificarsi due condizioni:

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 definitivamente revocata

In assenza di queste condizioni, l'identità digitale sarà automaticamente ripristinata scaduto il periodo di 30 giorni dalla data/ora/minuti della richiesta.

Si noti esplicitamente 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.

### 4.8.2 Scadenza/Re-attivazione/Re-emissione

Per rinnovo si intende il processo che estende il ciclo di vita delle credenziali, invece per sostituzione si intende un processo in cui viene emessa una nuova credenziale, o mezzo usato per produrla, associata ad un'entità per sostituire una credenziale emessa precedentemente e che risulta revocata.

# 5 Autenticazione

Nella fase di autenticazione, il titolare dell'identità digitale usa le proprie credenziali assegnate dal gestore dell'identità digitale per asserire la propria identità . Il processo di autenticazione è interessato esclusivamente con l'istituzione (o meno) di fiducia nella richiesta di identità e non tiene in alcun conto o ha relazioni con le specifiche azioni che il fornitore dei servizi (o meglio quella componente del fornitore dei servizi che può aver richiesto una autenticazione dell'identità per scopi diversi come ad esempio controllo accessi, gestione amministrativa, decisione autorizzativa ecc.) può scegliere di prendere sulla base della richiesta effettuata.

## 5.1 Validazione delle credenziali

In generale, Il processo di autenticazione include l'uso di un protocollo per dimostrare il possesso e/o il controllo di una credenziale in modo da garantire e instaurare fiducia nella richiesta di identità.

Per il livello 1 SPID di autenticazione informatica associati all'identità digitale, può essere sufficiente l'uso di un di un solo fattore di autenticazione, normalmente una password.

I livelli 2 e 3 di SPID sono basati su tecniche di autenticazione a doppio fattore , basate almeno su due cose indipendenti che una persona è (parametri biometrici), possiede (ad es. smart card, token) o conosce (ad es. password, PIN), in modo da garantire maggiore sicurezza ed aumentare, di conseguenza, la garanzia sull'identità digitale.

Lo scenario di attuazione SPID fa riferimento al modello federato delle identità digitali definito dalle specifiche SAML emesse dal consorzio OASIS.

In questo contesto, in conformità con le disposizioni del DPCM [3], gli attori previsti sono i seguenti:

- *i titolari dell'identità digitale* identificati nei soggetti che accedono ai servizi telematici, erogati da un fornitore di servizi, fornendo la propria identità digitale;
- *i gestori dell'identità digitale* costituiti dalle persone giuridiche che creano, rendono disponibili e gestiscono gli attributi necessari al fine di dimostrare l'identità digitale dei soggetti operanti in rete;
- *i gestore di attributi qualificati* rappresentati dagli enti aventi per legge l'obbligo di certificare il possesso e la validità di attributi qualificati, abilitazioni professionali, poteri di rappresentanza o altri attributi dei soggetti operanti in rete.

- *i fornitori di servizi* rappresentati dai soggetti privati o dalle pubbliche amministrazioni che erogano servizi in rete per cui la cui fruizione è richiesta l'identificazione e l'autenticazione degli utenti;

Le relazioni tra i suddetti attori si evidenziano nelle interazioni necessarie al completamento delle attività che, a partire da una richiesta avanzata da un soggetto titolare di un identità digitale, portano all' autorizzazione o al diniego della fruizione di un servizio telematico, messo a disposizione da un fornitore di servizi. Tali interazioni determinano la produzione di certificazioni da parte delle entità di certificazione, ovvero *gestori delle Identità digitali* o dei *gestori di attributi qualificati*, e l'utilizzo delle stesse da parte dei *fornitori di servizi*.

La figura sotto riportata illustra i passaggi previsti:

- il soggetto *titolare dell'identità digitale* richiede l'accesso ad un servizio collegandosi telematicamente al sito o al portale del *fornitore dei servizi*;

- il *fornitore dei servizi* rimanda il soggetto *titolare dell'identità digitale* presso il proprio *gestore dell'identità digitale* richiedendone l'autenticazione con specifico livello SPID associato al servizio richiesto;

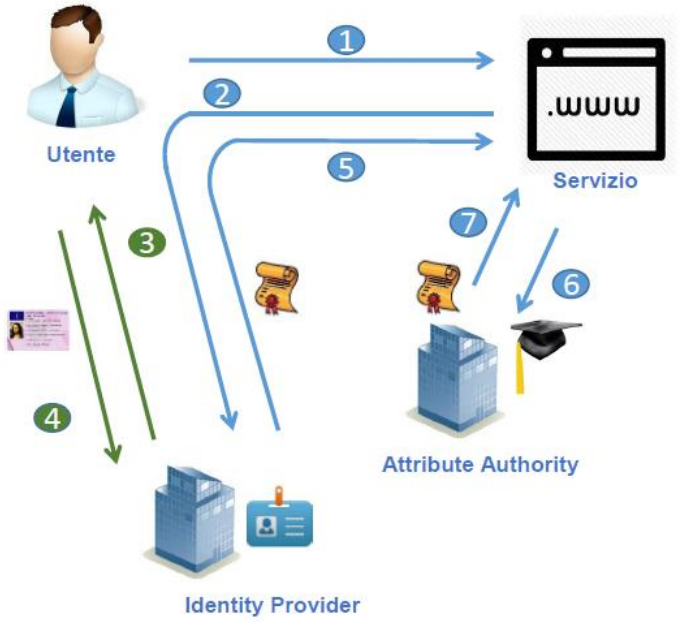
- *il gestore dell'identità digitale* verifica l'identità del soggetto sulla base di credenziali da lui accettate ed esibite dal soggetto. Se la verifica ha esito positivo viene emessa a favore dell'erogatore del servizio una certificazione ( asserzione di autenticazione SAML) di autenticazione e rimanda il soggetto presso il *fornitore dei servizi*;

- il *fornitore dei servizi* pur avendo adesso conferma dell'identità dell'utente può avere la necessità di verificare ulteriori attributi qualificati eventualmente presenti nel profilo utente e richiesti dalle policy di sicurezza che regolano l'accesso al servizio. In questo caso:

  a. individuati i *gestori di attributi qualificati* in grado di attestare la validità degli attributi necessari inoltra agli stessi un richiesta di attestazione degli stessi presentando i riferimenti dell'identità digitale per la quale si richiede la verifica;

  b. il risultato della richiesta è l'emissione di una certificazione ( asserzione di attributo SAML) emessa a favore del fornitore dei servizi;

- Il *fornitore dei servizi* raccolte tutte le certificazioni (asserzioni SAML) di identità e eventualmente di attributi qualificati presenti nel profilo necessarie per l'applicazione delle policy di sicurezza relative al profilo utente del soggetto che richiede l'erogazione può verificarne la sussistenza e decidere se soddisfare o rigettare la richiesta di servizio avanzata.

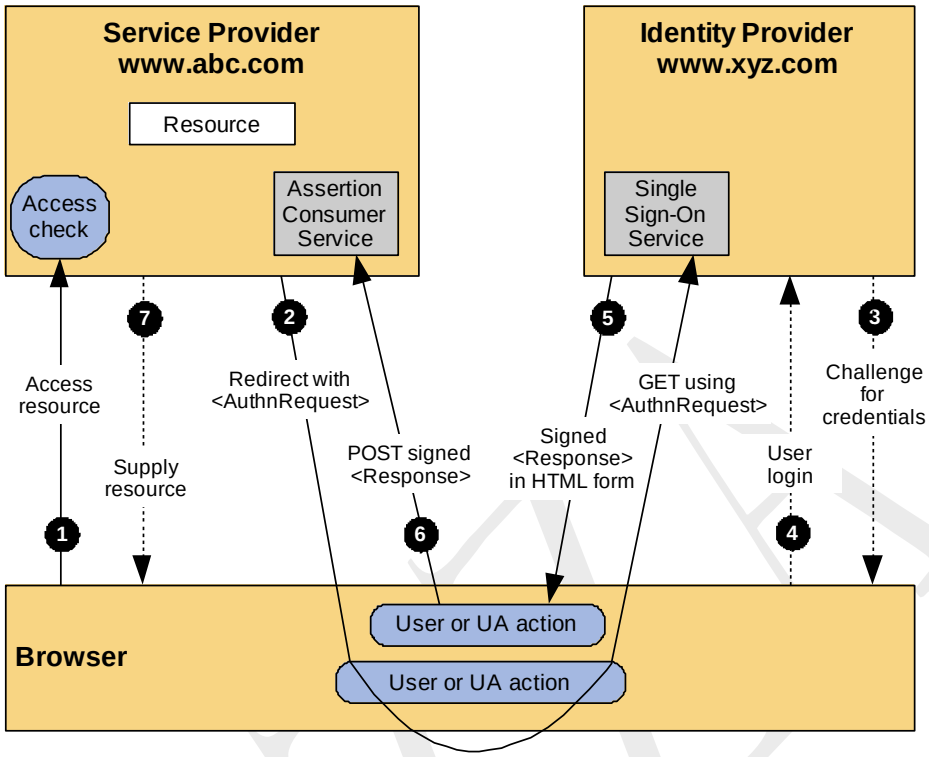



1. Richiesta di servizio
2. Inoltro verso Identity provider
3. Richiesta credenziali
4. Verifica credenziali
5. Rendirizzamento verso il service provider con asserzione di autenticazione
6. Richiesta attributi
7. Risposta contenente certificazione attributi

In particolare, le modalità di funzionamento del *gestore delle identità digitali,* per semplicità *Identity Provider*, sono quelle previste da SAML v2 per il profilo "*Web Browser SSO*".

Per SPID, cfr.documento regole tecniche, è prevista la modalità "*SP-Initiated"*: nelle versioni "*Redirect/POST binding*" e "*POST/POST binding*", in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un *fornitore di servizi*, indicato anche con il termine tecnico di *Service Provider*, il quale a sua volta si rivolge opportunamente all'autorità di certificazione d'identità in modalità "pull". La richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da un *Service Provider* all'*Identity Provider* usando il binding HTTP Redirect o il binding HTTP POST.

La relativa risposta SAML (basata sul costrutto <Response>) può invece essere inviata dall'*Identity Provider* al *Service Provider* solo tramite il binding HTTP POST.




***SSO SP-Initiated Redirect/POST binding***

L'elenco dei gestori delle identità digitali riconosciuti in SPID è pubblicato sul Registro SPID, accessibile telematicamente ai fornitori di servizio secondo le modalità espresse nelle regole tecniche SPID.

I soggetti titolari delle identità digitali dovranno indicare ai fornitori di servizio il gestore dell'identità digitale cui vogliono fare riferimento per la fase di autenticazione, indicando il codice identificativo dell'identità digitale o scegliendo da un elenco contenente i gestori delle identità digitali riconosciuti in SPID proposto dal fornitore dei servizi ai soggetti che fanno richiesta di erogazione di servizio.

I gestori dei servizi dovranno rendere noto ai gestori delle identità gli attributi che dovranno essere certificati a seguito dell'autenticazione dei soggetti richiedenti i servizi. Tali attributi dovranno essere i minimi necessari alla verifica dei profili utente associati ai servizi e potranno variare da servizio a servizio.

I gestori dell'identità al momento dell'autenticazione devono chiedere e ottenere dai titolari delle identità digitali esplicita autorizzazione alla trasmissione delle informazioni contenute negli attributi di cui viene richiesta certificazione da parte dell'erogatore dei servizi.

## 5.2 Conservazione dei documenti

Il monitoraggio e la tracciatura degli eventi nella fase di autenticazione è necessaria per diversi motivi come ad es . la corretta fornitura del servizio, conformità alla normativa di sicurezza, obblighi di legge.

Considerato che nel caso SPID sono coinvolte persone (fisiche o giuridiche), le informazioni contenute possono includere dati sensibili e devono essere trattate nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

# 6 Criteri per la valutazione dei sistemi di Autenticazione informatica per ogni livello di sicurezza SPID

ai sensi dell'art. 6, comma 2 del DPCM [3] l'Agenzia definisce i criteri per la valutazione dei sistemi di autenticazione informatica e la loro assegnazione al relativo livello di sicurezza.

Per il primo livello SPID (corrispondente a LoA2 dell'ISO 29115 [11]), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica ad un solo fattore, quali ad esempio una password.

Per il secondo livello SPID (corrispondente a LoA3 dell'ISO 29115 [11]), il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori non necessariamente basati su certificati digitali, ad esempio alla password può essere combinato un OTP (attraverso un out of band token come un SMS inviato ad un cellulare, attraverso un applicazione mobile o un dispositivo fisico).

Per il terzo livello SPID (corrispondente a LoA4 dell'ISO 29115 [11]), 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 conformi ai requisiti dell' Allegato 3 della Direttiva 1999/93/CE, ad esempio adottando meccanismi di autenticazione a livello di trasporto (alla connessione con l'IdP, il browser dell'utente, opportunamente configurato, accede al token, previo inserimento di qualcosa che l'utente conosce o che è, e abilita l'handshake previsto dal protocollo TLS 1.2 per l'invio del proprio certificato X.509).

In allegato C viene riportata una tassonomia completa dei tipi di token ed uno schema per individuare il livello di sicurezza di autenticazione informatica SPID nel caso di utilizzo multi-token.

Per tutti i livelli SPID, lo scambio delle asserzioni tra le parti avviene utilizzando il protocollo SAML 2.0.

In questo documento ulteriori e precise indicazioni sono fornite nelle sezioni relative alla modalità di associazione LoA (livelli di autenticazione informatica SPID), nei processi descritti per le identità digitali e credenziali e nella sezione di autenticazione e validazione delle credenziali.

L'Agenzia valuta e autorizza l'uso degli strumenti e delle tecnologie di autenticazione informatica consentiti per ciascun livello SPID.

I gestori delle identità digitali rendono pubbliche le decisioni dell'Agenzia con le modalità indicate dalla stessa.

In particolare per quanto riguarda la verifica del soggetto richiedente , l'Agenzia (come da art. 7, comma 3 del DPCM [3]) definisce le modalità con le quali la verifica dell'identità è effettuata secondo i più alti livelli di controllo disponibili ed in relazione ai livelli di sicurezza (LoA) delle identità digitali.

I fornitori di servizi scelgono il livello di sicurezza necessario per accedere ai propri servizi anche sulla base della metodologia suggerita dall'Agenzia (v. par. 2.1), in particolare per una corretta associazione valutazione dell'impatto causato da un errore di autenticazione e conseguente associazione con adeguato livello di sicurezza SPID.

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.

# 7 Usabilità e Accessibilità

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

- l'usabilità ovvero la facilità d'uso come (1) 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 e (2) 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 e le indicazioni Web Accessibility Initiative (WAI) del World Wide Web Consortium (W3C).

I paragrafi che seguono descrivono le diverse interfacce utente da sviluppare in dipendenza delle differenti fasi e funzionalità dello SPID lato utente finale.

## 7.1 Adesione e iscrizione[7]

Riguarda l'utente e l'IdP, dipende dai differenti meccanismi di identificazione previsti da SPID

## 7.2 Autorizzazione[8]

Riguarda l'utente, il fornitore dei servizi e il gestore delle Identità Digitali

## 7.3 Gestione delle credenziali e degli attributi[9]

Riguarda l'utente e il gestore dell''identità digitali per tutto il ciclo di vita della identità digitale

[7] Interfaccia standard per tutti i gestori, info su campi necessari, logo e chiaramente richiami a vincoli di usabilità e accessibilità; potrebbe anche essere raccomandato l'utilizzo di tecniche CAPTCHA allo scopo di impedire che i bot (un programma che accede alla rete attraverso lo stesso tipo di canali utilizzati dagli utenti umani) utilizzino il servizio di registrazione per creare spam o per violare la sicurezza con operazioni di hacking.

[8] definire due modalità (per il pilota con selezione manuale dell'IdP e quella definitiva con selezione automatica sulla base dell'identità digitale), deve essere omogenea e standard per tutti ma può differire in dipendenza del livello SPID e dei token da utilizzare

[9] fornire indicazioni e vincoli per usabilità e accessibilità, suggerire tecniche CAPTCHA allo scopo di impedire che i bot utilizzino questo servizio per creare spam o per violare la sicurezza con operazioni di hacking.

# 8 Disciplina sull'utilizzo degli elementi identificativi dello SPID

Questo capitolo deve essere completato con specifiche indicazioni per l'utilizzo degli elementi identificativi del sistema SPID (v. manuale di riferimento per il logo SPID).

# 9 Vigilanza 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 indica le migliori pratiche da adottare e favorisce la diffusione della cultura dell'accessibilità con azioni di formazione e informazione sul tema.

L'Agenzia svolge attività di governance, supervisione e procede a verifiche e controlli periodici (o su segnalazione) per quanto riguarda :

- conformità dei sistemi alle regole tecniche ed alle modalità attuative
- all'usabilità ed accessibilità
- corretta esecuzione dei processi di dimostrazione, esame e verifica dell'identità
- gestione del ciclo di vita delle identità digitali
- conservazione dei dati
- conformità normativa
- privacy
- sicurezza e audit

L'Agenzia esercita attività di vigilanza e di controllo al fine di verificare la permanenza della sussistenza dei requisiti previsti dal DPCM [3] e se, all'esito dei controlli, accerta la mancanza dei requisiti richiesti per l'iscrizione nel registro SPID, decorso il termine fissato per consentire il ripristino degli stessi, l'Agenzia, con provvedimento motivato notificato all'interessato, può adottare le azioni previste dall'art. 12 comma 4.

I gestori delle identità digitali si sottopongono, con cadenza almeno biennale, ad una verifica di conformità alle disposizioni vigenti da parte di un organismo di valutazione accreditato ai sensi del Regolamento CE 765/2008 del Parlamento Europeo e del Consiglio del luglio 2008 ed inviano all'Agenzia l'esito della verifica, redatto dall'organismo di valutazione in lingua inglese, entro tre giorni lavorativi dalla sua ricezione.

L'Agenzia può inoltre richiedere ai gestori delle identità digitali:

a. informazioni circa il livello di soddisfazione dei propri clienti;

b. le caratteristiche di eventuali servizi aggiuntivi offerti.

In un'apposita sezione della struttura informativa sono registrate e gestite le informazioni relative a disservizi, segnalazioni e reclami secondo la classificazione riportata 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). |

**Tabella 14 - 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 per 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 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 può disporre l'inibizione dell'esercizio dell'attività svolta dal gestore inadempiente, 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, può adottare le azioni previste dall'art. 12 comma 4 del DPCM.

Nel caso in cui l'Agenzia disponga la revoca dell'accreditamento del gestore dell'identità digitale si applicano le disposizioni relative alle cessazioni ai sensi dell'art. 12 del DPCM.

I gestori delle identità digitali informano tempestivamente l'Agenzia e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali.

I gestori delle identità digitali inviano, con cadenza almeno bimestrale, all'Agenzia i dati statistici relativi all'utilizzo del sistema, metriche quantitative e qualitative che saranno definiti e concordati a valle del primo pilota SPID.

# Appendice A – Privacy e protezione delle informazioni personali di identificazione (PII) / dati personali.

A tutela dei dati personali: tutti i dati, le informazioni e la documentazione (cartacea ed elettronica) relativa all'entità richiedente di cui il gestore delle identità digitali, il gestore degli attributi qualificati e i fornitori di servizi vengono in possesso nell'esercizio delle loro attività tipiche attività (ad es. nel caso del gestore delle identità per le fasi di iscrizione, emissione, gestione, autenticazione e per tutto il ciclo di vita dell'identità) , sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico.

In particolare i dati personali vengono trattati da tutti gli attori nel perimetro SPID in conformità con il Decreto Legislativo 30 giugno 2003, n. 196.

# Appendice B – Documenti di Identità

Il soggetto che effettua l'identificazione verifica l'identità del Titolare tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi
- Tesserino di riconoscimento rilasciato da una Amministrazione dello Stato al proprio dipendente.

# Allegato C - Tassonomia dei tipi di token

In questo documento si considerano i seguenti tipi di token validi 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 verificatore (normalmente l'identity provider) 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 conformi ai requisiti dell' Allegato 3 della Direttiva 1999/93/CE

- 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 conformi ai requisiti dell' Allegato 3 della Direttiva 1999/93/CE.

La tabella seguente riporta lo schema per individuare il corrispondente livello di sicurezza di autenticazione informatica SPID quando viene utilizzata una combinazione multi-token.

| | Token con segreto memorizzato | Token con conoscenza pre-registrata | Token con tabella dei codici/segreti | Token out of band | Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP) | Dispositivo Crittografico a singolo fattore (SF) | Token crittografico software multi-fattore (MF) | Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP) | Dispositivo Crittografico multi-fattore (MF) |
|---|---|---|---|---|---|---|---|---|---|
| Token con segreto memorizzato | Livello 1 SPID | Livello 1 SPID | Livello 2 SPID | Livello 2 SPID | Livello 2 SPID | Livello 2 SPID | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Token con conoscenza pre-registrata | X | NA | NA | NA | NA | Livello 1 SPID | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Token con tabella dei codici/segreti | X | X | NA | NA | NA | Livello 1 SPID | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Token out of band | X | X | X | NA | NA | Livello 1 SPID | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Dispositivo a singolo fattore (SF) del tipo One-Time Password (OTP) | X | X | X | X | NA | Livello 1 SPID | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Dispositivo Crittografico a singolo fattore (SF) | X | X | X | X | X | X | Livello 3 SPID | Livello 2 SPID | Livello 3 SPID |
| Token crittografico software multi-fattore (MF) | X | X | X | X | X | X | Livello 3 SPID | Livello 3 SPID | Livello 3 SPID |
| Dispositivo multi-fattore (MF) del tipo One –Time Password (OTP) | X | X | X | X | X | X | X | Livello 2 SPID | Livello 3 SPID |
| Dispositivo Crittografico multi-fattore (MF) | X | X | X | X | X | X | X | X | Livello 3 SPID |

**Tabella 15 - Schema livello sicurezza SPID / multi-token**